Zebra Enterprise Messaging Service

Version 3.0.24309

Workcloud Communication

Customer Administrator Guide

Terms of Use

Proprietary Statement

Product Improvements

Liability Disclaimer

Limitation of Liability

Contents

Contents

Contents

About This Guide

This guide describes the service and features of the Zebra Enterprise Messaging Service (ZEMS). This guide aims to help customers determine how ZEMS fits into their business practices and define the configuration of the ZEMS service to support their business.

Chapter Descriptions

Topics covered in this guide are as follows:

- About This Guide—Describes the conventions used in this guide.
- ZEMS Features—Describes the service and features of the Zebra Enterprise Messaging Service (ZEMS).
- Using the ZEMS Customer Portal—Describes the features of the ZEMS Customer Administrator Portal.
- Webhook Integrations—Describes how to create incoming and outgoing webhooks to facilitate messaging between ZEMS and third-party applications such as Microsoft Teams, Twilio, and Infobip.
- Configuring PTT Pro Clients for ZEMS—Describes how to configure the PTT Pro for Android and PTT Pro for iOS clients to use ZEMS messaging.
- ZEMS API Endpoints—Describes the API endpoints that customers can use for bulk operations.

Icon Conventions

The documentation set is designed to give the reader more visual clues. The following visual indicators are used throughout the documentation set.

NOTE: The text here indicates information that is supplemental for the user to know and that is not required to complete a task.

IMPORTANT: The text here indicates information that is important for the user to know.

CAUTION: If the precaution is not heeded, the user could receive a minor or moderate injury.

WARNING: If danger is not avoided, the user CAN be seriously injured or killed.

DANGER: If danger is not avoided, the user WILL be seriously injured or killed.

Notational Conventions

The following notational conventions make the content of this document easy to navigate.

- **Bold** text is used to highlight the following:
  - Dialog box, window, and screen names
  - Dropdown list and list box names
  - Checkbox and radio button names
  - Icons on a screen
  - Key names on a keypad
  - Button names on a screen
- Bullets (•) indicate:
  - Action items
  - List of alternatives
  - Lists of required steps that are not necessarily sequential
- Sequential lists (for example, those that describe step-by-step procedures) appear as numbered lists.

Service Information

If you have a problem with your equipment, contact Zebra Global Customer Support for your region. Contact information is available at: zebra.com/support.

When contacting support, please have the following information available:

- Serial number of the unit
- Model number or product name
- Software/firmware type and version number

Zebra responds to calls by email, telephone, or fax within the time limits set forth in support agreements.

If your problem cannot be solved by Zebra Customer Support, you may need to return your equipment for servicing and will be given specific directions. Zebra is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty.

If you purchased your Zebra business product from a Zebra business partner, contact that business partner for support.

Revision History

Change	Date	Description
MN-004513-01 Rev A	May 2022	First version early access.
MN-004513-02 Rev A	June 2022	Internal release.
MN-004513-03 Rev A	September 2022	Added ZEMS Portal and APIs.
MN-004513-04 Rev A	December 2022	Add support for Twilio and SMS messaging.

Change	Date	Description
MN-004513-05 Rev A	March 2023	Add support for IWG and IWG APIs.
MN-004513-06 Rev A	July 2023	Add support for Infobip SMS messaging.
MN-004513-07 Rev A	October 2023	Add support for WhatsApp and urgent messages.
MN-004513-08 Rev A	February, 2024	Add Originate and Receive attributes for group members, and assign users as managers for a site through Profile Manager.
MN-004513-09 Rev A	April, 2024	Rebranded to Workcloud Communication
MN-004513-10 Rev A	May, 2024	Add support for MOTD and manual sync with the PTT Pro Server.
MN-004513-11 Rev A	August, 2024	• Zebra WS50 Android Wearable Computer can receive the announcements sent through the IWG Announcer. • Search functionality within messages in a conversation. • Receive the announcements sent through the IWG Announcer.
MN-004513-12 Rev A	March 2025	Added conversation reporting and masking for PTT Pro for iOS.

ZEMS Features

The Zebra Enterprise Messaging Service (ZEMS) is an add-on service to Workcloud Communication PTT Pro. ZEMS is available upon request, during initial onboarding, or later. Contact the Service Desk to enable ZEMS services.

The ZEMS service provides:

- Basic text messaging from users to users or groups, including the ability to reply.
- Sending audio, video, or image files as an attachment to a message.
- Broadcast messaging enables managers to send a one-way message to users in regions or sites.
- Integration with applications such as Microsoft Teams and messaging services such as Twilio and Infobip through Webhooks.
- IWG endpoints to send announcements and messages from third-party applications.

ZEMS is supported on Workcloud Communication PTT Pro apps and is incorporated seamlessly into the end-user experience. A browser-based ZEMS Web Client is also available for desktop users.

Supported PTT Pro Clients

The Zebra Enterprise Messaging Service (ZEMS) includes text messaging with the ability to send video, audio, and images to one or more contacts and groups. Users with the manager role can send broadcast messages to regions, child regions, and departments (sites).

The following PTT Pro clients support ZEMS messaging:

- PTT Pro for Android version 3.3.10196 or later
- PTT Pro for iOS version 1.0.11088 or later
- ZEMS Web Client version 2.1.22307 or later

NOTE: The PTT Pro PC Client does not support ZEMS.

NOTE: Workcloud Communication PTT Pro clients can use ZEMS messaging or legacy messaging, but not both at the same time.

NOTE: The PTT Pro client versions listed above are required for ZEMS version 2.1.22309 or later.

Messaging

Enable ZEMS messaging in your Workcloud Communication PTT Pro clients using the same method you use to configure other client features. Zebra will provide the required information such as the URL for the ZEMS server and the API key.

After the Workcloud Communication PTT Pro apps are configured with the required information, users can message other users or groups at their site. The Zebra Enterprise Messaging Service Client User Guide describes how to send messages and view received messages.

NOTE:

- The PTT Pro PC Client does not support ZEMS. Use the ZEMS Web Client to send and receive messages on a desktop PC.

- Messages sent through the IWG Messenger API will not be received by ZEMS users. Announcements sent through the IWG Announcer API will operate as normal.

- Zebra WS50 Android Wearable Computer can receive the announcements sent through the IWG Announcer.

Supported Media Types

ZEMS enables clients to include attachments in messages and provides a link to the attachment in the message. All attachments are stored on shared cloud storage.

ZEMS supports the following media types:

- application/msword
- application/vnd.ms-excel
- application/vnd.ms-powerpoint
- application/vnd.openxmlformats-officedocument.presentationml.presentation
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
- application/vnd.openxmlformats-officedocument.wordprocessingml.document
- application/pdf
- application/vcard
- application/vnd.apple.pkpass
- text/vcard
- text/x-vcard
- text/csv
- text/rtf
- text/richtext
- text/calendar
- text/directory
- image/
- audio/
- video/

> 📝 **NOTE:** ZEMS delivers attachments for the supported media types. ZEMS clients may require additional software or apps to open or view the attachments.
>
> • Refer to [Twilio Mime Types](#) for information about the media types supported by Twilio.
>
> • Refer to [Infobip Content Types](#) for information about the media types supported by Infobip. See [Unsupported Mime Types](#) for MIME type support between ZEMS, Infobip, and WhatsApp.

Limitations

ZEMS clients are limited to uploading an attachment of 10 MB. The attachment size limit for Twilio is 5 MB.

Broadcast Messaging

Broadcast messaging provides communication across regions, where a region is a collection of sites (PTT Pro departments). After you define regions and assign sites, you can assign managers to regions. Managers are PTT Pro users with elevated privileges in ZEMS. Managers can send broadcast messages to their regions, sites, and groups.

Regions include the following properties:

• A region can contain one or more regions.

• Managers can be associated with one or more regions.

Regions Example

In this example, an enterprise is divided into East and West regions. Each region has a manager that supervises operations. The East and West regions are further divided into districts, D1 through D4. Each district contains one or more sites, which are departments in the PTT Pro Server.

Figure 1   Regions in a ZEMS Deployment
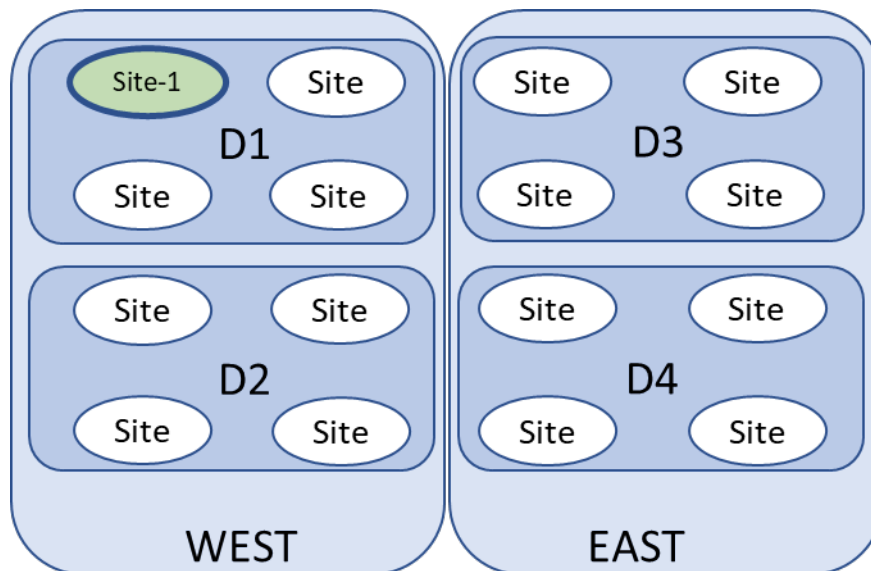
Site-1, highlighted in green, belongs to the West region, but it also belongs to the D1 district (child region). PTT Pro users in Site-1 can receive broadcast messages sent by the manager of Site-1, the D1 child region, or the West region.

Configuration Process

You define regions and sites and assign managers in the ZEMS server.

1. Define the regions. This includes specifying the top-level regions and child regions. A child region may also contain child regions, creating a multi-level hierarchy. To add regions, use one of the following methods:

    - Use the Regions/Sites tab in the ZEMS portal.

    - Use the ZEMS API Region controller.

2. Associate sites (PTT Pro departments) with the regions. Every region that does not have child regions needs to have a site associated with it. To add sites to regions, use one of the following methods:

    - Use the Regions/Sites tab in the ZEMS portal.

    - Use the ZEMS API Region.Sites controller.

3. Assign managers to regions and sites by associating PTT Pro user IDs with the region or site. Every region, child region, and site may have one or more managers and a single PTT Pro user may manage multiple regions. To assign managers to regions and sites, use one of the following methods:

    - Use the Regions/Sites tab in the ZEMS portal to associate managers with sites.

    - Use the Users tab in the ZEMS portal to associate managers with regions or sites.

    - Use the ZEMS API Region.Managers controller to associate managers with regions or sites.

Configuration of the Example Enterprise

The following table illustrates the information necessary to configure the example described in Regions Example. After this information is configured in ZEMS, following the prescribed process, the managers, identified by their PTT Pro user name, can send broadcast messages to their regions.

Table 1   Example ZEMS Enterprise Configuration

Region Level 1	Region Level 2
Name: West	Name: D1
Manager: Leonardo.DaVinci	Manager: Vincent.Van.Gogh
Manager: Rembrandt	Sites: 1 2 3 4
	Name: D2
	Manager: Paul.Gaugin
	Sites: 5 6 7 8
Name: East	Name: D3
Manager: Claude.Monet	Manager: Pablo Picasso
Manager: Rembrandt	Sites: 9 10 11 12
	Name: D4
	Manager: Salvador.Dali
	Sites: 13 14 15 16

> **NOTE:** Regions that do not have child regions must have sites associated with them.

In this example, Leonardo.DaVinci can broadcast messages to the West region, the D1 region, and the underlying sites. Vincent.Van.Gogh can broadcast messages to the D1 region and the underlying sites.

The customer administrator is encouraged to plan out the regions, child regions, and sites as shown in Example ZEMS Enterprise Configuration before beginning the configuration.

PTT Pro for Android Broadcast Message Example

In this example, the user manages both the East and West regions. This user can send a broadcast message to all regions, one region (East or West), or one or more child regions (for example, District 24 and District 13, which are child regions of the East region).

When a manager composes a broadcast message, the top-level regions display.

Figure 2   Regions for a Broadcast Message
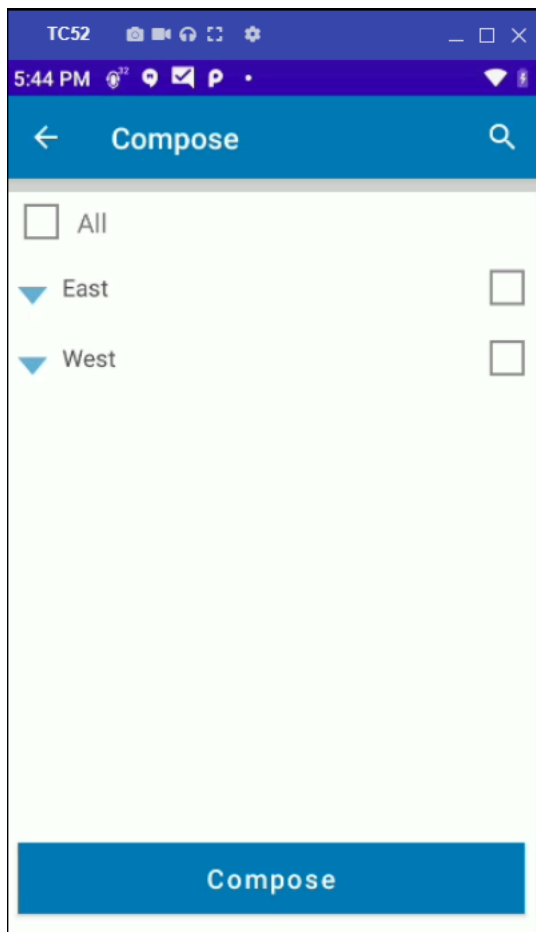
A manager can expand the regions to see the child regions and sites.

Figure 3   PTT Pro Broadcast Screen with Child Regions
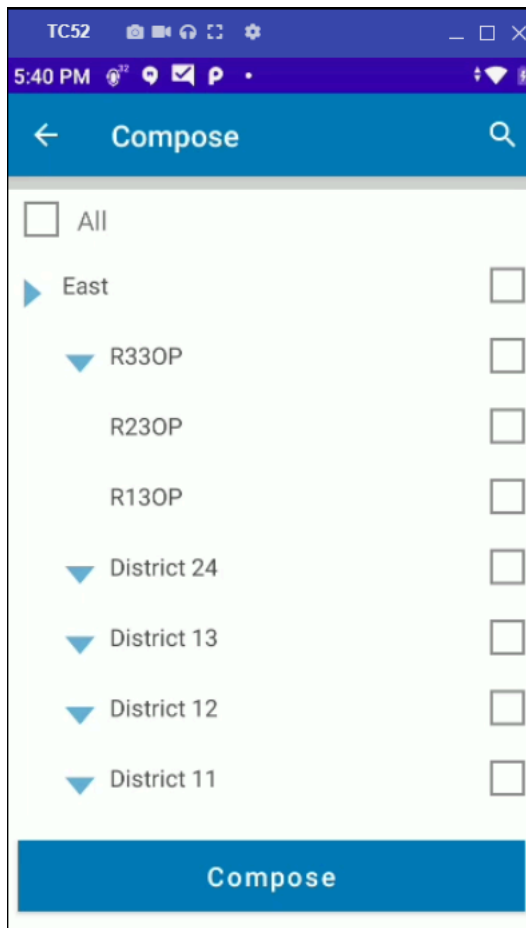
Broadcast Message Expiry

You can set an expiry date for the broadcast message. The message is removed from the system after a refresh or re-login after the message expiration.

- When the toggle is off, the Expiry value is set to 0, meaning the message has no expiration date.

- When the toggle is on, the Expiry value is set to 1 by default, meaning the message expires in one day, and you can increment it to up to 30.

- After sending the message, check the remaining time from the **Sent** tab. For example, if the expiry is set to 5 days, 4 day(s) 23 hour(s) will be the remaining time.

NOTE:

Checking a Broadcast Massage

PTT Pro for Android and Zebra WS50 Android Wearable Computer retain broadcast messages until they expire, enabling you to check messages even if you were offline when they were sent.

Figure 4   Select Set Message Expiry option for the Broadcast Message

Figure 5   Expiry toggle-off

Figure 6   Expiry toggle-on

Figure 7   Check the remaining time

Webhooks

A webhook is a lightweight API that enables external applications to send messages to and receive messages from regions, sites, and groups. Webhooks are defined as incoming or outgoing. An outgoing webhook from ZEMS feeds an incoming webhook of the external application.
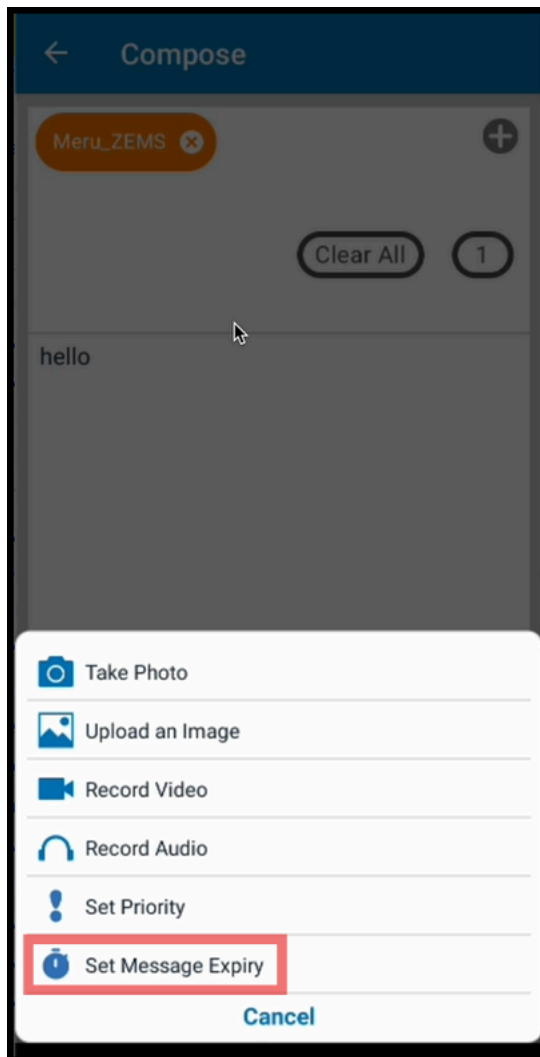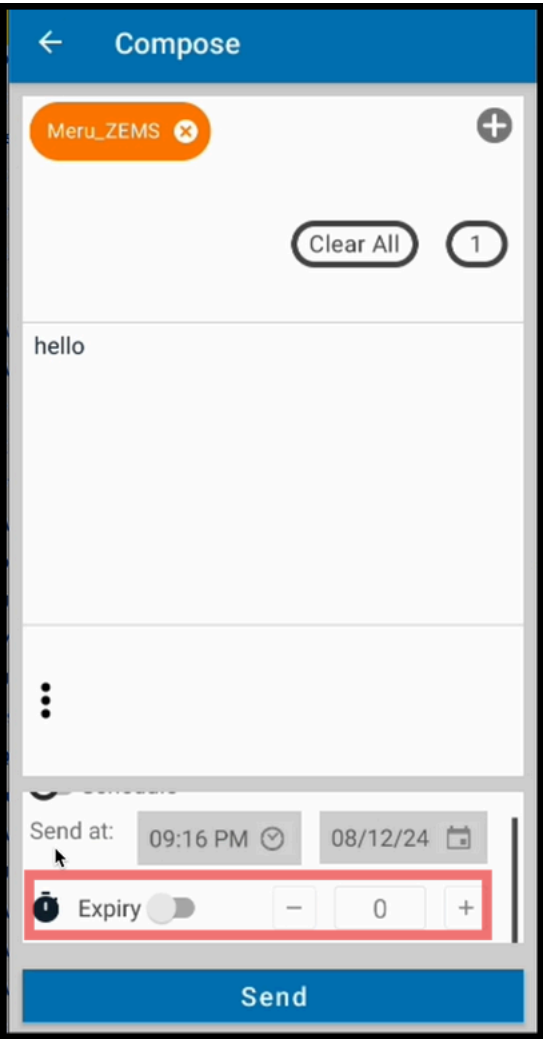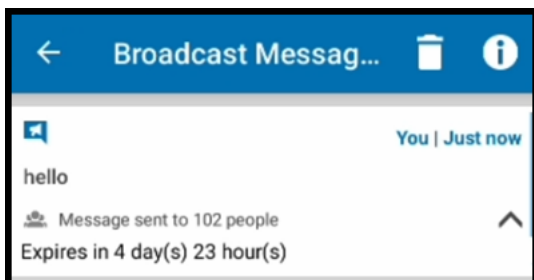
It is not necessary to define two-way communication, that is webhooks in both directions, between ZEMS and an external application.

Refer to Connectors for information about creating webhooks.

NOTE: ZEMS Web Client users do not receive media files sent through a webhook.

Interworking Gateway

The Interworking Gateway (IWG) allows third-party applications to send audio files and text messages to PTT Pro recipients. A recipient can be a PTT Pro user or a PTT Pro group.

ZEMS supports the IWG APIs:

Announce REST APIs

Allows audio messages to be submitted to ZEMS with a specified IWG endpoint. ZEMS processes the audio message and broadcasts it to the PTT Pro recipient specified by the IWG endpoint. PTT Pro recipients that are unavailable when the audio message is broadcast do not receive the message. Refer to the Workcloud Communication Announcer REST API Developer Guide for details regarding the API.

Messenger REST APIs

Allows text messages, with optional attachments, to be submitted to ZEMS with a specified IWG endpoint. ZEMS processes the message and forwards it to the PTT Pro recipients specified by the IWG endpoint. Refer to the Workcloud Communication Messenger REST API Developer Guide for details regarding the API.

Messages can be sent to recipients using one of two configurations:

- ZEMS messaging enables PTT Pro users to receive messages on ZEMS. Choose this option if you are using ZEMS and IWG.

- PTT Pro messaging enables PTT Pro users to receive messages through PTT Pro messaging. Choose this option if you are not using ZEMS.

ZEMS messaging is the default configuration. You are configured for PTT Pro messaging if you migrate from an IWG environment to ZEMS. Contact Zebra Support if you want to use ZEMS for messaging.

Messaging is only supported from external applications to an IWG endpoint. Messaging in the reverse direction is not supported.

Figure 8   Text and Audio Messages with IWG

Configure IWG to Send Audio or Text Messages

Configure a destination PTT Pro group or PTT Pro user in ZEMS as an IWG endpoint to send an audio or text message from ZEMS to PTT Pro. For the IWG endpoint to reach the destination PTT Pro group or user, ZEMS communicates with the PTT Pro Server using a proxy user.

The PTT Pro server is unaware that the proxy user is not a normal PTT Pro user. The proxy user acts like any other PTT Pro user, but instead of running on a device, it runs on the ZEMS server and forwards communications from the Messenger and Announcer APIs. Proxy users must be configured in PTT Pro as users.

When you add an IWG endpoint, ZEMS adds the proxy user to the PTT Pro server. ZEMS does not support multiple simultaneous transactions for a single IWG endpoint. Only one audio message using that endpoint may occur simultaneously. If an audio communication comes in for an endpoint employed in another audio communication, the second audio communication will fail. A message will fail if a message comes in for an endpoint employed in an audio communication.

IWG Example

In this example, an enterprise owner connects the PTT Pro group Hardware to applications that generate text messages and announcements.

Figure 9 Interworking PTT Pro Audio
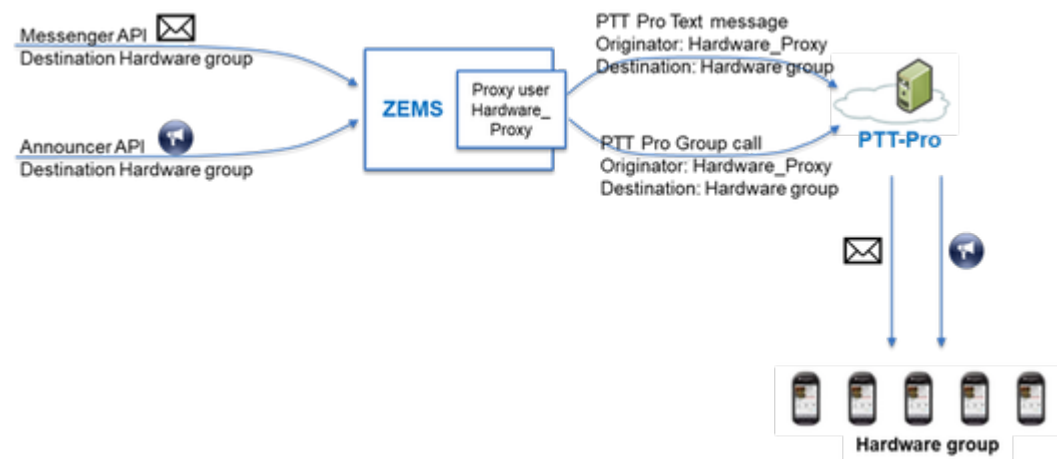
The customer administrator adds an IWG endpoint to ZEMS with the following information:

- The Site (PTT Pro department) includes the Hardware group. The department must exist in the PTT Pro and be synced to ZEMS before it can be used to create an IWG endpoint.

- Target type is Group. A PTT Pro user or a PTT Group are possible target types for the endpoint. The name of the group in this example is Hardware.

- The endpoint name, Hardware, in this example.

- The proxy name of Hardware_Proxy.

When the administrator adds the endpoint, ZEMS performs the following actions:

1. ZEMS adds a user to the PTT Pro Server with the specified proxy name, in this example, Hardware_proxy. If the user already exists in the PTT Pro Server, the IWG uses the existing user.

2. ZEMS adds the user Hardware_Proxy to the Hardware group if it is not already a member of the group.

3. ZEMS adds the PTT_Pro_Hardware endpoint to the IWG with the proxy of Hardware_proxy. As a result of adding Hardware_proxy as the proxy, ZEMS registers with the PTT Pro Server as the user Hardware_proxy.

When the IWG receives an announcement or message intended for the PTT_Pro_Hardware endpoint, the IWG forwards the communication from the Announcer or Messenger to the Hardware group using the proxy user Hardware_Proxy.

> **NOTE:** When an announcement or message is forwarded from the Announcer or Messenger to the Hardware group, the originator is identified by the proxy name, Hardware_proxy, in this example.

The following diagram shows how Sites in ZEMS correspond to departments in the PTT Pro server. When you add an IWG endpoint, the proxy user is added as a PTT Pro user. If the target of the IWG endpoint is a group, as in this example, the proxy user is added as a group member.

Figure 10 Department in PTT Pro and Sites in ZEMS
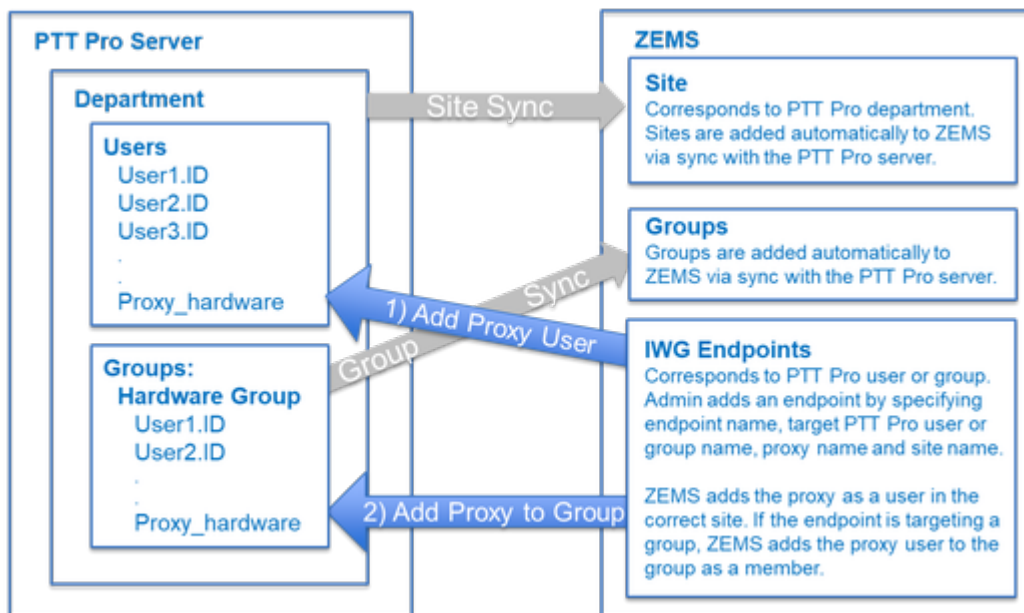
ZEMS Data Synchronization

ZEMS uses the users, groups, and sites (departments) defined in the PTT Pro Server, eliminating the need to configure this information in ZEMS. ZEMS synchronizes data with the PTT Pro Server every 24 hours.

Table 2 ZEMS Synchronization with PTT Pro

Action	Result
New user is configured to use ZEMS.	Department (sites), group, contacts, and message history are synchronized.
Daily sync with PTT Pro	All customer departments (sites), groups, and users are synchronized.

> **NOTE:** A user with super-admin privileges can synchronize data with the PTT Pro Server from the Regions/Sites view.

Group Synchronization with the ZEMS Web Client

If the group membership for a user is modified in the PTT Pro Server, the ZEMS Web Client does not reflect this change until the next daily sync unless the user is also logged into the PTT Pro for Android client.

Using the ZEMS Administrator Portal

The ZEMS Administrator Portal allows an administrator to create the organizational structure, assign managers to regions, monitor messages, and configure webhooks.
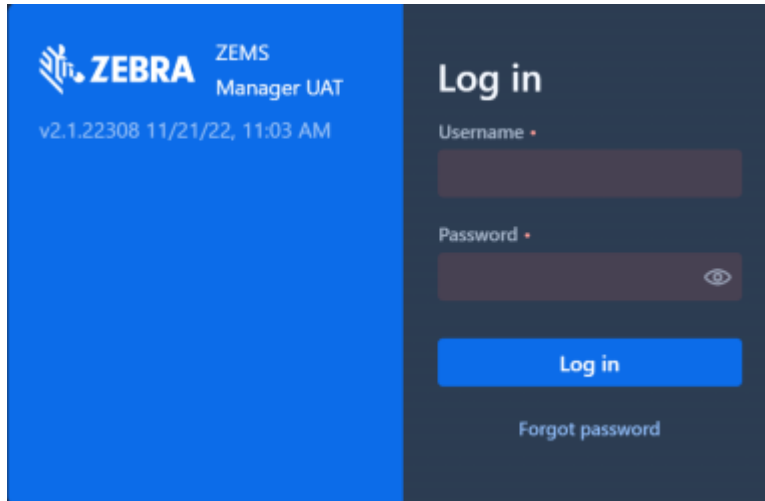
The web-based portal includes these functions:

- Dashboard
- Conversations
- PTT Data
  - Region/Sites
  - Groups
  - Users
- Connectors
  - Incoming Webhooks
  - Outgoing Webhooks
- Twilio Connectors
- Infobip Connectors
- IWG
  - Endpoints
  - Stats
- System
  - Portal Users
  - Events

ZEMS Portal URL

Zebra will provide you with the URL to the ZEMS Administrator Portal. You will also receive a username and password. When you log in for the first time, you will receive an email with a link to update the password.

Figure 11   Customer Administrator Log In Screen
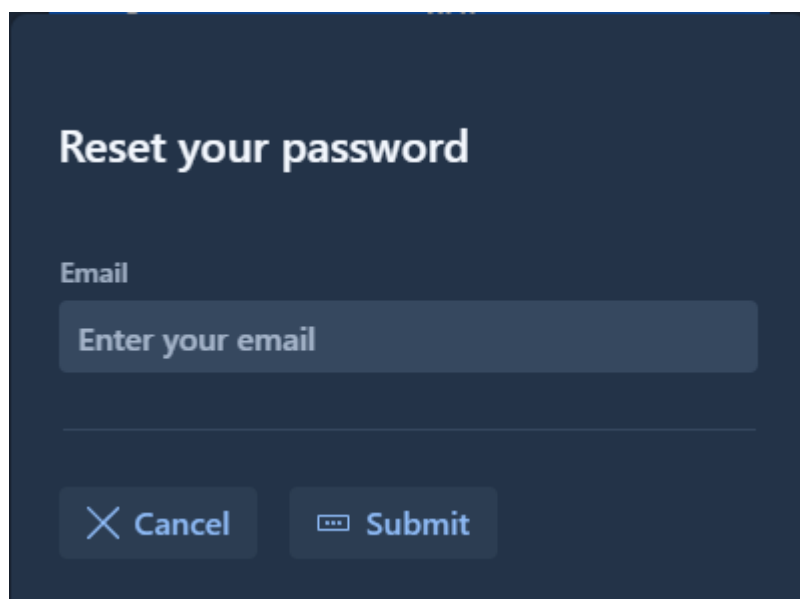
Resetting Your Administration Portal Password

You can reset a password by asking the site Super-Admin to reset the password, or you can use the **Forgot password** link on the portal **Log in** screen.

A portal password must be from 8 to 40 characters long and include one number, one lowercase letter, one uppercase letter, and one of the following special characters: [@#$%!.].

1. Navigate to the portal **Log in** screen.

2. Click the **Forgot password** link.

3. Enter your email address in the **Email** field and click **Submit**.

4. Check your email for a message with a link to reset your password.

Top Toolbar

The toolbar at the top of the ZEMS Administrator Portal is always visible. The toolbar displays the name of the screen and provides access to the Customer Details screen, a link to the Swagger APIs, and the Log Out command.

Figure 12   Top Toolbar with the Sidebar Collapsed
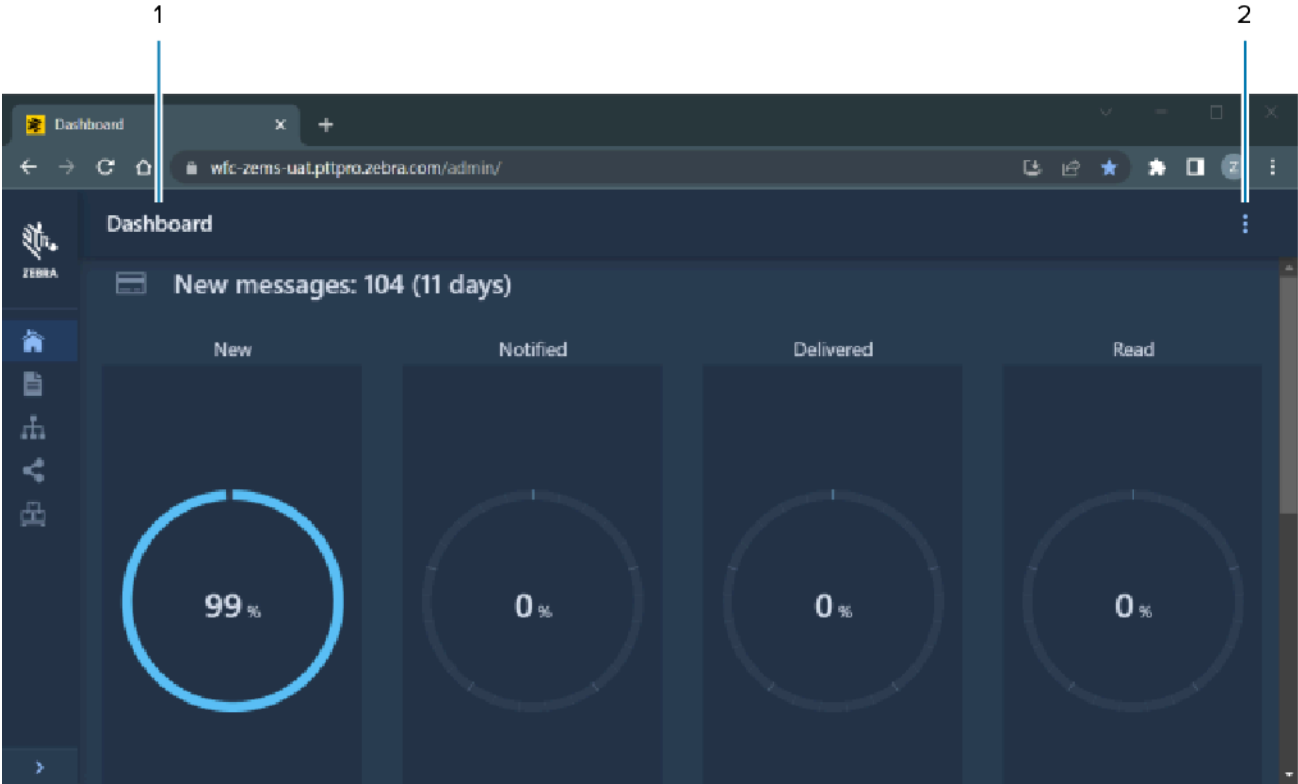
1	Name of the portal screen.
2	Show Menu provides access to: • Customer Details • Name of the logged-in user • Swagger APIs • Log Out

Customer Details

The **Customer Details** screen includes the following information:

ID
  The customer ID number in ZEMS.

Name
> The customer's name in ZEMS.

Created
> The date the customer was created in ZEMS.

Token
> The API key is needed to configure PTT Pro clients and use the ZEMS APIs.

Figure 13   Customer Info Screen
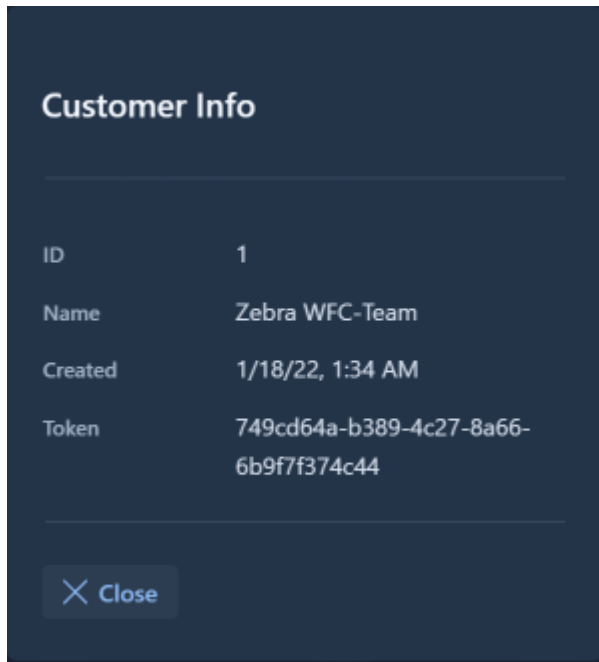
Dashboard

The **Dashboard** provides an overview of message activity using charts and a line graph. It is the initial view of the portal when you log in.

Message Count

The top of the **Dashboard** provides a message count. This count includes the total number of sent messages since your customer account was created in ZEMS.

Figure 14   Message Count on Dashboard

Circle Charts

Circle charts show the status of sent messages: The circle charts show:

New
> Messages that have not been delivered or read and users have not been notified.

Notified
> The intended recipient of the message has been notified.

Delivered
The recipient has downloaded the message.

Read
The recipient has read the message.

Figure 15   Circle Charts Display Message Status
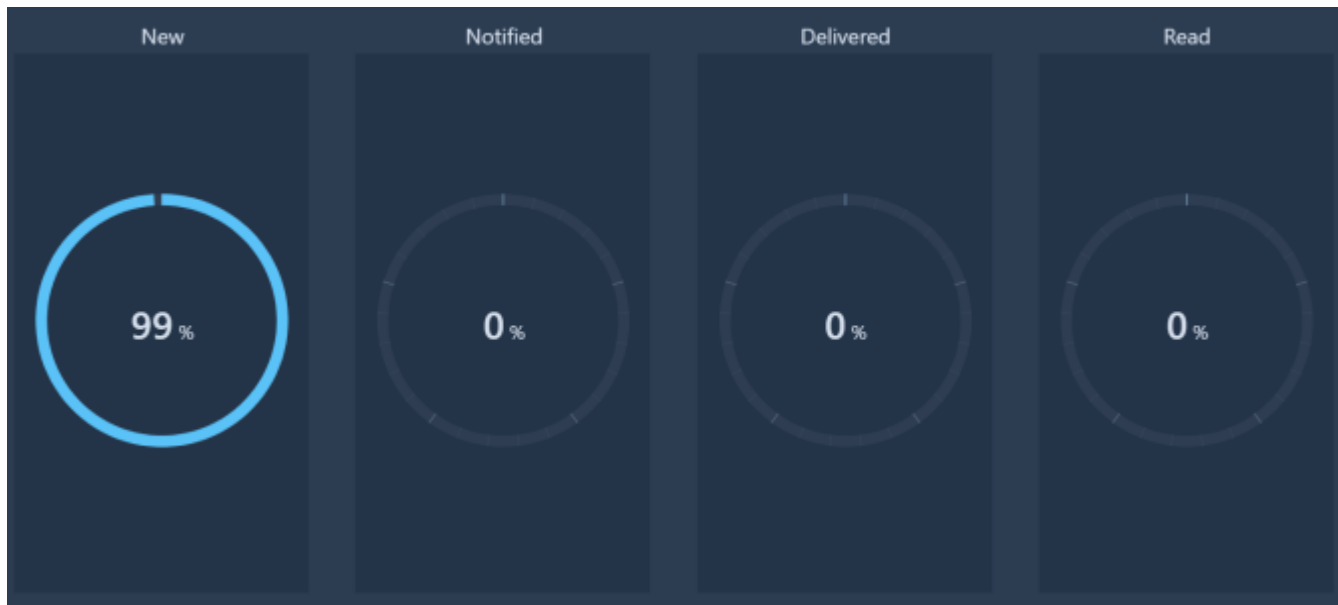
The four charts add up to 100% because each message falls into one of these four states. Partial percentages, such as 0.5%, are not displayed.

Line Graph

The text message line graph shows the message distribution over the last 14 days.

Figure 16   Distribution of Text Messages By Time
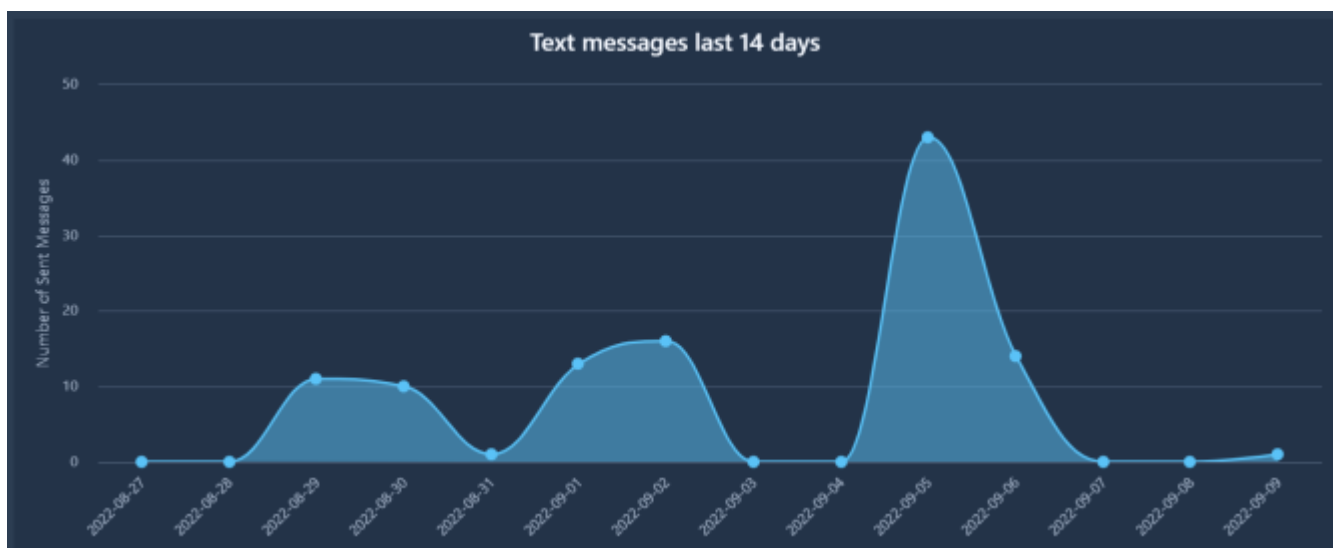
Conversations

The **Conversation** view lists all of your users' conversations. Each conversation consists of one or more messages. Messages get automatically deleted after 30 days. When a conversation has no remaining messages, it is removed.

> **NOTE:** The **Conversations** view is available to users with the Super-Admin role.

Figure 17 Conversation View

1	Conversations view.
2	Filter for conversations: • Internal displays ZEMS messages and PTT calls. • Broadcast displays broadcast messages. • External displays messages from an external source, such as WhatsApp and SMS.

3	Search conversations by username.
4	Refresh to update the Conversation view.
5	A conversation from a PTT call.
6	A conversation from an external source.
7	A conversation from a broadcast message.
8	Total number of conversations. When a conversation is opened, it shows the number of messages within it.

Select a conversation to view the individual messages.

NOTE: The search bar at the top of the messages helps you search text within a conversation.

Figure 18 Messages in a Conversation
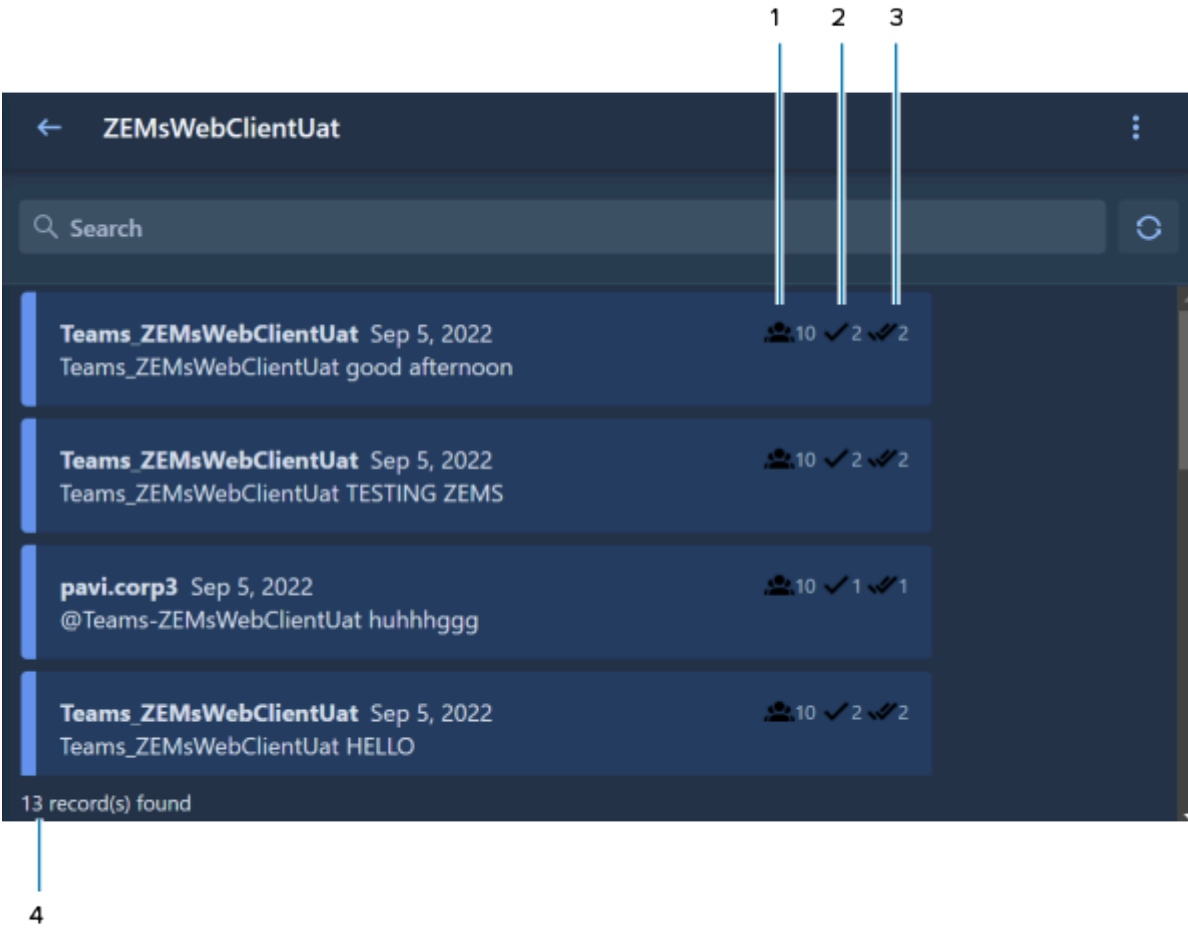
1	Number of message recipients, including offline users.
2	Number of users who have downloaded the message. This includes users that have read the message.

3	Number of users who have read the message.
4	Total number of messages in this conversation.

Select a message to view the message status for each recipient. You can also use the **User Login** and **Status** fields to filter by user or status.

Figure 19   Message Recipients

Prioritized Messages

Users who send messages through the PTT Pro for Android or the ZEMS Web Client can add a priority to messages. The user can assign a priority to one-to-one messages, group messages, and broadcast messages, provided the user is a manager in ZEMS. When you read a message through the **Conversation** view, you can see the priority of the message.

In the following example, a one-to-one message has a priority of urgent. A text label and an icon indicate the priority.

Figure 20   A Message Prioritized as URGENT
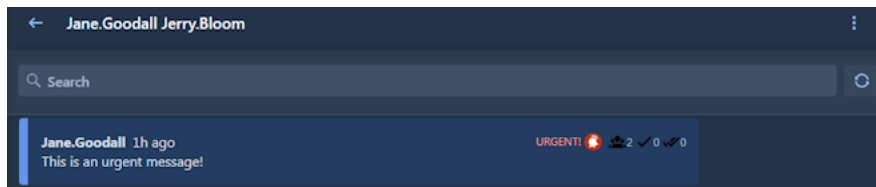
Message Priorities

Table 3   ZEMS Message Priorities

Priority	Description
💬	A normal message.

Table 3   ZEMS Message Priorities (Continued)

Priority	Description
	A message marked as important.
	A message marked as urgent. When a user receives an urgent message, an alert sound occurs every two minutes until the message is marked read. The urgent message alert is repeated for a specified interval. The default interval for PTT Pro for Android is 10 minutes. The default interval for the ZEMS Web Client is 20 minutes.

Conversation Reporting

If you have super-admin privileges, you can download user messages (conversations) and PTT call history from the **Conversations** view in the ZEMS Administrator Portal. This data includes any attachments or media files attached to messages. The conversation data is provided in a CSV file.

The Download Conversations icon appears on the right toolbar, in the yellow circle in the following image.

Figure 21   Download Conversations Icon
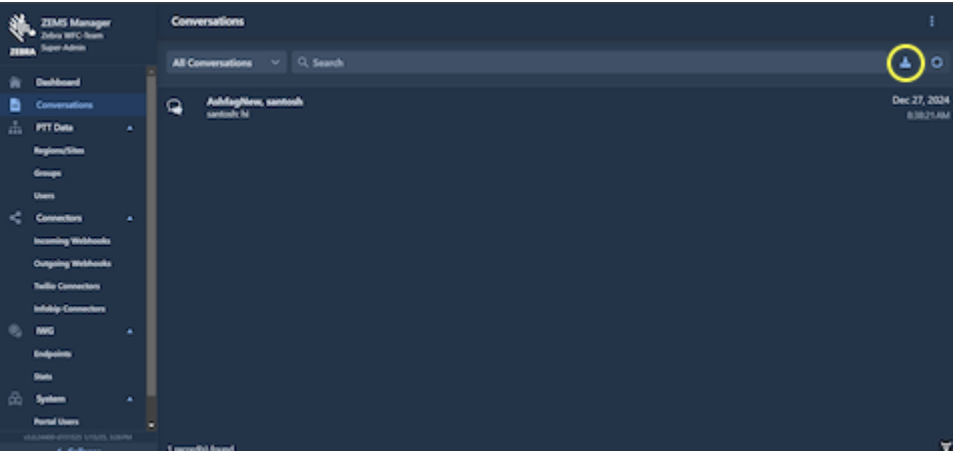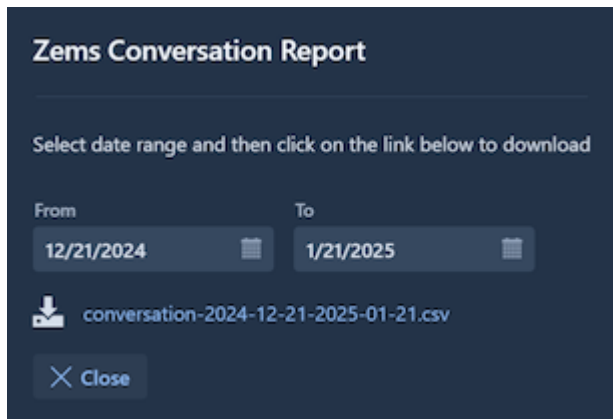
Icon	Description
	Click **Download Conversations**.

When you click **Download Conversations**, select a date range for the report.

NOTE: The Conversation screen removes inactive conversations after 30 days. Active conversations remain until they are inactive for 30 days.

Figure 22   Select a Date Range for the Report

Click the link in the **Zems Conversation Report** dialog to download the report to your local system.

  NOTE: The Conversation report includes a large amount of data and requires time to process. When you click the download link, it takes a few minutes before the report downloads.

Conversation Report Details

The conversation report is provided as a CVS file. Each message is contained within a row, and each column divides the message into parts.

Table 4   Conversation Report Columns

Column Head	Description
Conversation Id	Identifies the conversation within the ZEMS Server.
Message Id	Identifies the message with the conversation.
Body	Contents of the message.
Priority	Priority of the message. The priority is one of three values: • Normal • Important • Urgent
Media URL	URL to media, if any, included with the message. See Media URLs for information about accessing media files.
Expiry in Days	Number of days after which the message expires and is removed from the Conversation screen.
User Login	Login identifier of the user who sent the message.
First Name	First name of the user who sent the message.
Last Name	Last name of the user who sent the message.

Table 4 Conversation Report Columns (Continued)

Column Head	Description
Message History	Status of the message history. The history is one of: • 2 (Delivered) • -1 (Sent) • 0 (Created) • 1 (Notified) • 3 (Read) • 4 (Opened)
Created At	Time when the message was created.
Recipient Information	Describes the type of recipient. The recipient is one of: • User • Group • Site • Region
Conversation Type	The type of conversation. The type is one of: • 0 (Internal) • 1 (Broadcast) • 2 (External)
Site Id	Site where the message originated.
Group Name	If the message recipient was a group, this field provides the group name.

Media URLs

The media URLs in the Conversation Report require authentication to access. You need to request the API token for your tenant from Zebra. After you receive the API token, you can retrieve the media files using `curl`.

The format of the curl command is:

```
curl -H "Apikey: <api-key>" <media-url> -o <output-filename>
```

The `<media-url>` must exactly match the URL in the Conversation Report. In addition, the `<output-filename>` must match the filename with the correct file extension, such as `.jpg` or `.mp4`

The media type appears in the Media URL column as the mime type. For example, the following mime type is `.mp4`.

```
[{"mime":"video/mp4","size":5643,"]
```

.

PTT Data

PTT Data includes three views: **Regions/Sites**, **Groups**, and **Users**. Each view is automatically populated with data from the PTT Pro Server and each view provides ZEMS-specific functions to organize the PTT Pro data to suit your needs.

Regions and Sites PTT Pro Data

Regions/Sites is populated with the departments (sites) from the PTT Pro Server. Use the toolbar and Region/Sites options to create regions and assign managers to regions and sites.

You can complete the following tasks from the **Regions/Sites** view:

- Create regions and assign sites to those regions.

- Assign managers to sites.

- Create and/or associate outgoing webhooks to sites.

- Create and/or associate incoming webhooks to sites.

Figure 23   Region/Sites View
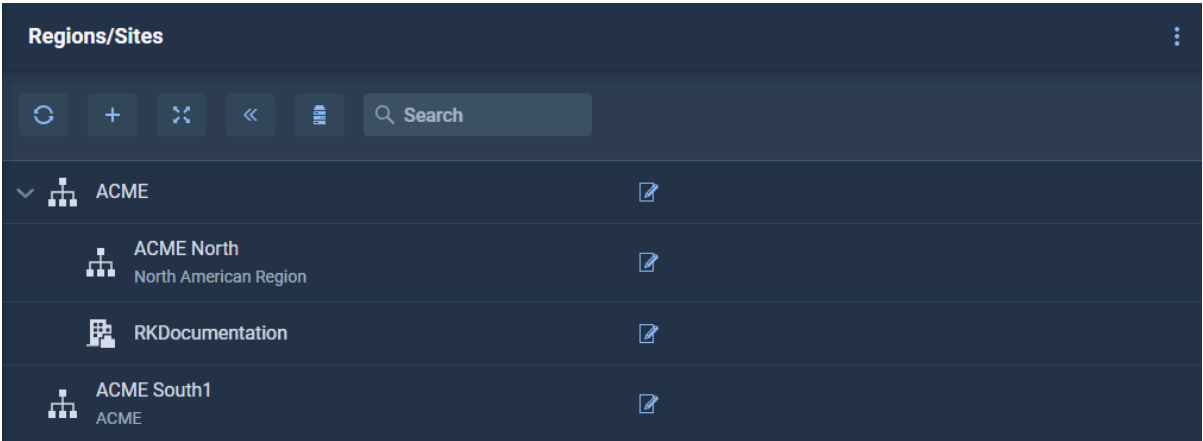
🏢	Identifies a site. A site is a department in the PTT Pro Server.
🔀	Identifies a region. A region can contain sites or additional regions to create a hierarchy.
🔄	Refresh the view.
＋	Add a region.
⤢	Expand all regions.

«	Collapse all regions.
	Sync data with the PTT Pro Server. This option requires Super-Admin privileges.
	Edit a region or site.

Adding a Region

The regions you create are displayed in a tree-like structure. Use the arrow to the left of the region to expand or collapse the region.

1. Click ✚ in the toolbar. The **Add Region** dialog appears.

2. Enter a name in the **Name** field and an optional description in the **Description** field.

3. Click to select a parent region from the Parent Region drop-down menu.

   Select **<top>** to create a top-level region or select a region to create a child region.

4. Select the row with the region to view details for the region and where you can add managers, outgoing webhooks, and incoming webhooks. Refer to Users and Connectors on page 41 for more information.
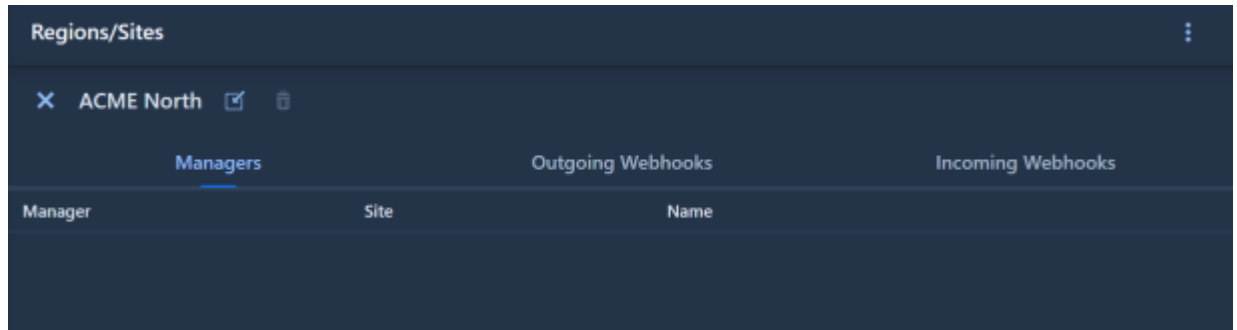
Assigning a Site

After you create one or more regions, you can assign sites to the regions.

1. Locate the site you want to assign. Sites are listed below regions in the **Region/Sites** view.

2. Click the edit button next to the site name.

   The **Update Region** dialog appears.

3. Assign the site by selecting the region from the **Parent Region** drop-down menu.

4. Click **Update region**.

Groups

The **Groups** view displays the department groups created in the Workcloud Communication PTT Pro Management Portal and the Personal and Member groups created by users. Administrators use the Workcloud Communication PTT Pro Management Portal to create or modify groups, including adding or removing users. Users can create and modify Personal and Department groups.

Groups include the Originate and Receive attributes for group members. These attributes are retrieved from the PTT Pro Server. When a user sends a message to a group, the message is received by group members with the Receive attribute set to True. If the message is sent when a user is logged out, the message is added to the conversation when the user logs in.

In a Workcloud Communication Profile Manager environment, the Originate and Receive attributes dynamically change when the user selects a role. When the user selects Workcloud Communication PTT Pro roles, the Originate and Receive attributes are set to True. Unselected Workcloud Communication PTT Pro roles have Originate set to True and Receive set to False. For more information, refer to the Workcloud Communication Profile Manager Administrator Guide.

When the membership of a group is modified, the changes are reflected in ZEMS as follows:

- If the user whose membership was modified is logged into PTT Pro for Android, the change is reflected immediately, including the Originate and Receive attributes.

- If the user is not logged in to the PTT Pro for Android, the change is reflected when the ZEMS server synchronizes with the PTT Pro Server. Go to ZEMS Data Synchronization for more information about synchronization.

NOTE: If you assign a manager to a region or a child region that includes a site, the manager can view the groups and send broadcast messages to the groups of that site.

You can select a group to view the group members and if there are incoming webhooks associated with the group.

Figure 24   Groups View Sorted By Site

1. Use the **Site filter** or the **Group Name** fields to find the group.

2. Click the row with the group name to display the list of users, the values of the Receive and Originate attributes, and incoming webhooks.

Figure 25   Groups View

Users

The Users view lists the department users synchronized from the PTT Pro Server.

The Users view includes the columns listed below. Use the **Site** and **ID** columns to sort users.

- Site

- ID

- User Login/Oauth

- Name

- PTT Pro IDs

- Updated At

Figure 26   Users View

To find a specific user, use the **Site filter** and the **Name filter**. The Site filter lists all of the users in a site when the Name filter matches the filter string against user names.

Select a user to view additional details such as Groups, Managed Sites, and Incoming Webhooks.

Figure 27   User Details
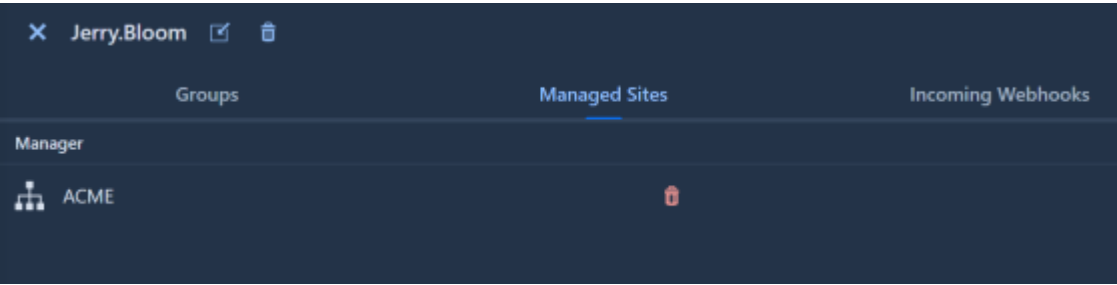
Assigning a User as a Region or Site Manager

A manager can send broadcast messages to their assigned region. If the assigned region contains child regions, the manager can send broadcast messages to those regions as well. You can assign a manager to a region or site.

You can also assign a manager through the **Region/Site** view. This guide describes assigning a manager from the **Users** view.

In a Profile Manager environment, you can assign users as managers to a region or site during user import. Changes are reflected in ZEMS at the next synchronization. For more information, refer Workcloud Communication Profile Manager Administrator Guide.

1. Select a user using the filters on the **User** view.

2. Click the **Managed Sites** column.
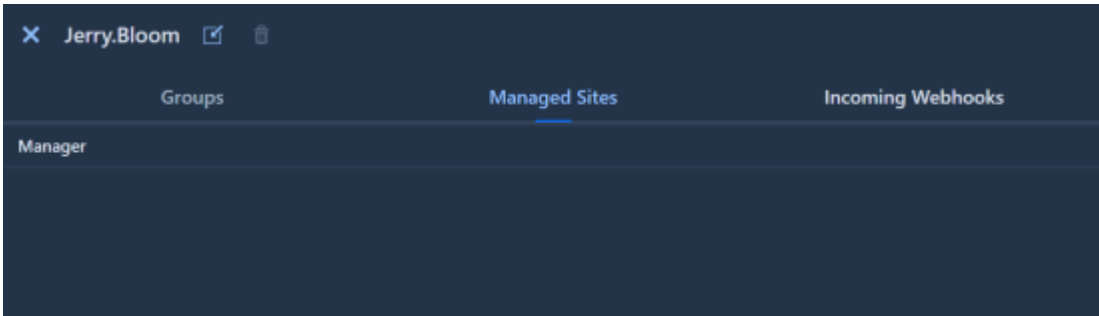
3. Click Add region/site ⧉ to open the **Select Region/Sites** dialog.
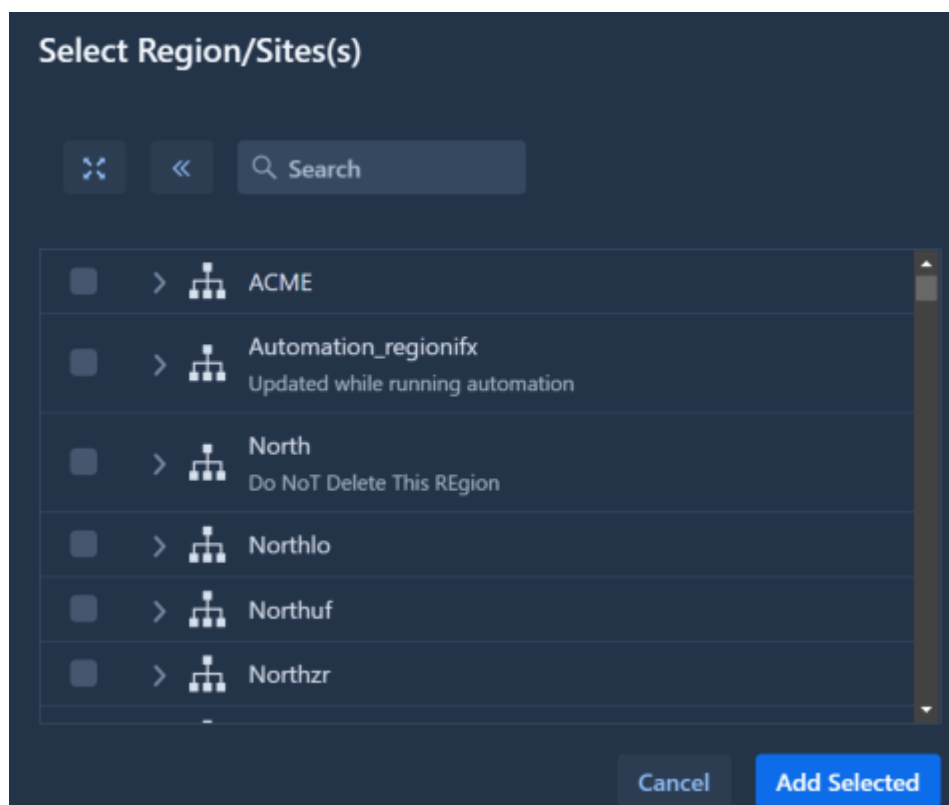
4. Use the Expand All ⤢, Collapse All ≪, or **Search** to select the region or site the user is going to manage.

5. Select the region or site and click **Add Selected**.

The user is listed as a manager for the selected region.

You can verify that the user is assigned the manager role from the **Region/Sites** view. Select the region, and the user is listed under the **Managers** column.

Connectors

Connectors includes the **Incoming Webhooks**, **Outgoing Webhooks**, **Twilio Connectors**, and **Infobip Connectors** screens. You can use these screens to create and manage incoming and outgoing webhooks.

- An incoming webhook allows external applications to send messages through ZEMS.

  You can select **Base Webhook** when creating an incoming webhook. A base webhook allows you to create a single webhook with multiple recipients. The recipients are identified using URL query strings.

- An outgoing webhook provides a method to send ZEMS messages to external applications.

- A Twilio connector creates a secure connection to a Twilio account.

- An Infobip connector creates a secure connection to an Infobip account.

Refer to Creating Webhooks for Microsoft Teams for an example of using webhooks to create a communications connection between Microsoft Teams and a ZEMS region.

Refer to Creating Webhooks for Twilio for an example of using webhooks to create an SMS communications connection with ZEMS.

Refer to Creating a Webhook for Infobip for an example of using a webhook to create an SMS connection with ZEMS.

Types of Incoming Webhooks

Incoming webhooks provide access for external applications to send messages to regions, sites, groups, and users.

You can create two different types of incoming webhooks:

- A webhook that specifies the intended recipient. A separate webhook is needed for each additional recipient.

- A base webhook that enables you to specify one or more recipients when you configure the webhook on the external application. A base webhook must be specified on a region or site. The recipients must be members of the specified region or site according to the following rules:

  - If the base webhook target is a site, you can specify the groups and users of the site as recipients. You cannot specify the site.

  - If the base target is a region, you can specify child regions, sites, groups, or users of the region as recipients. You cannot specify the region.

The recipients of a base webhook are added to the URL when you configure the incoming webhook on the external application. Use standard URL query parameters to specify one or more recipients.

Examples

In this example, the URL identifies the PTT Pro group `Dept-Clothing` as a recipient:

```
https://[ZEMS-URL]/api/v1/service/4Gyruf16k5?group=Dept-Clothing
```
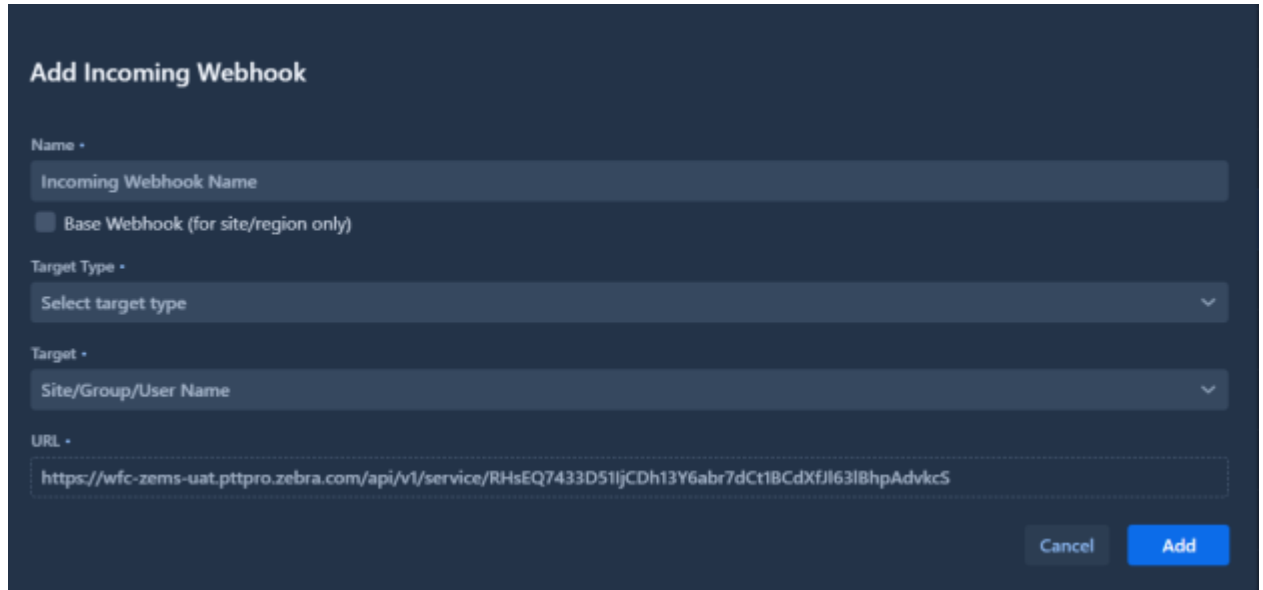
In this example, the URL identifies the PTT Pro group `Dept-Clothing` and the PTT Pro user `Jerry.Bloom` as recipients:

```
https://[ZEMS-URL]/api/v1/service/4Gyruf16k5?group=Dept-Clothing&user=Jerry.Bloom
```

Creating an Incoming Webhook

The **Incoming Webhooks** view allows you to add and delete incoming webhooks and associate them with ZEMS elements. Incoming webhooks can target users, groups, sites, or regions.

1. Click **Add** ➕ to open the **Add Incoming Webhook** dialog.

2. Enter a name in the **Name** field for the incoming webhook.

3. Select **Base Webhook** to optionally create an incoming webhook that accepts URL parameters.

   When selected, the **Target Type** must be a Site or Region.

4. Select the target type from the **Target Type** drop-down menu.

   - USER
   - GROUP
   - SITE
   - REGION

5. Select the target from the **Target** drop-down menu. The target type filters the list of available targets.

6. Click **Add**.

   The URL is automatically generated and cannot be changed.

7. Locate the new webhook in the list of incoming webhooks and click 📋 to copy the URL.

   This URL is used in the outgoing webhook of the external application.

Example

In this example, the target for an incoming webhook is the ACME region shown in the **Region/Sites** view.

Incoming ZEMS Webhook Targets

You need to determine which ZEMS entity will receive the outgoing Teams webhook before you create the ZEMS incoming webhook.

Table 5   Incoming ZEMS Webhook Targets

Target Type	Target Name
User	PTT Pro user name
Group	PTT Pro group name
Site	PTT Pro department name
Region	ZEMS region name

The incoming webhook can also use the Base parameter to send messages to multiple recipients. See About Incoming Webhooks for more information.

Creating an Outgoing Webhook

The **Outgoing Webhooks** view allows you to add and delete outgoing webhooks, as well as to associate a webhook with a region or site.

1. Click ✚ to open the **Add Outgoing Webhook** dialog.

2. Enter a name in the **Name** field for the outgoing webhook.

3. Enter an optional description in the **Description** field.

4. Select a region or site from the **Region/Site** drop-down menu.

5. Enter the URL from the incoming webhook in the **URL** field.

6. Fill in the Message Body Template.

   Refer to Outgoing ZEMS Webhook Message Body Template for information about message body parameters.

7. Click **Add**.

Outgoing ZEMS Webhook Targets

You must determine which ZEMS entity accesses the outgoing ZEMS webhook before creating the ZEMS outgoing webhook.

The available ZEMS entities which can access an outgoing webhook are defined below.

Table 6   Outgoing ZEMS Webhook Targets

Type	Target
Site	PTT Pro department name
Region	ZEMS region name

Outgoing ZEMS Webhook Message Body Template

The Message Body Template for an outgoing ZEMS webhook must be specified when you create the ZEMS outgoing webhook.

The format to specify for Microsoft Teams is:

```
{"type": "message", "text": "your text"}
```

The `text` parameter is a free-form string value with embedded `$variables` that are replaced with actual values from the ZEMS text message. The list of variables that can be embedded inside the text string includes:

- `$BODY` which is the message body from the sender.
- `$SENDER` which is the PTT Pro user login of the sender.
- `$SENDER_NAME` which is the PTT Pro name of the sender.

Example

```
{"type": "message", "text": "$SENDER: $BODY"}
```

NOTE: When using the API, the quotation marks must be escaped using a backward slash (\). This example sent over the API would be `{\"type\": \"message\", \"text\": \"$SENDER: $BODY\"}`.

Using this example Message Body Template and assuming the Microsoft Teams incoming webhook was named `Teams-Channel-ZEMSKDU`, a PTT Pro sender named `cary.grant` sending a message of `3/3/2022 test` to the outgoing webhook would result in the following message body:

```
{"type": "message", "text": "cary.grant: @Teams-Channel-ZEMSKDU 3/3/2022
 test"}
```

This example would appear in the Microsoft Teams channel as `cary.grant: @Teams-Channel-ZEMSKDU 3/3/2022 test`.

Creating a Twilio Connector

The **Twilio Connectors** view enables you to create a connection to Twilio for receiving messages and responding to applications such as SMS and WhatsApp. You must have a Twilio account to enter details in the Add screen to create a Twilio connection.

1. Click ✚ to open the **Add** dialog.

2. Enter a name for the connection in the **Name** field.

3. Enter a description for the connection in the **Description** field. A description is required.

4. Enter the SID from your Twilio account in the **SID** field. The SID is required.

   If you have multiple Twilio accounts, enter the SID for the account you want to use with ZEMS.

5. Enter the token from your Twilio account into the Token field.

6. Enter a default response in the **Default Response** field. A default response is required.

   The default response is returned when a message is sent through the Twilio connector.

Creating an Infobip Connector

The **Infobip Connectors** view enables you to create a connection to Infobip for receiving messages and responding to applications such as SMS and WhatsApp. You must have an Infobip account to enter details in the **Add** screen to create an Infobip connection. Only one Infobip connector can be created.

1. Click ✚ to open the **Add** dialog.

2. Enter a name for the connector in the **Name** field.

46

3. Enter a description for the connection in the **Description** field.

   A description is required.

4. Enter the API Key and the API Base URL from your Infobip account into the **API Key** and **API Base URL** fields.

   The API Key and the API Base URL are required.

5. Optionally, enter a default response in the **Default Response** field.

   The default response is returned when a message is sent through the Infobip connector.

> **NOTE:** You can also specify a default response in your Infobip account.

Changing External User Names to Friendly Names

Users that send messages through a Twilio Connector or an Infobip Connector are added to ZEMS as external users, and their login names are set to a random string. You can change the random string to a recognized name. The new name is used in the Conversation view of the ZEMS Administrator Portal, the ZEMS Web Client, and the Recent view of the Workcloud Communication PTT Pro clients.

1. Select the connector where you want to change the login names:

   - For Twilio, select **Twilio Connectors** and select a Twilio connector.

   - For Infobip, select **Infobip Connectors** and select the Infobip connector.

2. The connector opens and lists the external users who have sent messages.

3. Select the string in the **From** column and enter a recognizable name.

   In the example below, the external user name for a Twilio user is changed to `Friendly Name`.

IWG

Verify that the necessary departments, groups, and users are synced from the PTT Pro Server and present in ZEMS before adding an IWG endpoint. It may take 24 hours for new departments, groups, and users to sync from the PTT Pro Server to ZEMS.

Licensing is not required for IWG endpoints. However, the PTT Pro proxy user uses a PTT Pro user license when it is added to the PTT Pro server.

NOTE: When an IWG endpoint is deleted, the proxy user is not deleted from the PTT Pro Server. You must delete the proxy user manually.

To add IWG endpoints, use one of the following methods:

- Use the **Endpoints** screen to add, delete, and modify IWG endpoints. You can also verify that the proxy exists and is functioning properly.

- Use the ZEMS API IWG.Endpoints controller to add, delete, and modify IWG endpoints. You can also use the API to retrieve and verify endpoint information.

- Use the ZEMS API IWG.Import controller to bulk add IWG endpoints.

Endpoints

The **Endpoints** view lists any existing endpoints. You can use the **Endpoints** view to manage endpoints.

Figure 28   Endpoints View

The Endpoints view includes the following columns:

Site name
Identifies the PTT Pro department where the endpoint was created. Use the menu to filter endpoints by site name.

Name
The proxy name of the endpoint when it was created. Use the menu to filter endpoints by proxy name.

Target

Identifies the recipient of the endpoint. The target can be a PTT Pro user ♟ or a PTT Pro group 👥.

State

Value can be offline, idle, or active.

Status

Reported by the PTT Pro server during registration, announcement, or message through the IWG APIs.

The toolbar in the Endpoint view supports the following actions:

Icon	Description
↻	Refresh the Endpoint view.
✚	Add an IWG endpoint.
✎	Modify an IWG endpoint. This action is visible when you select an endpoint.
▤	Verify or reload an IWG endpoint. This action is visible when you select an endpoint.
♫	Send an audio message to an IWG endpoint. This action is visible when you select an endpoint.
▤	Send a text message with an optional attachment to an endpoint. This action is visible when you select an endpoint.

Adding an IWG Endpoint

When you add an IWG endpoint, the recipient, a PTT Pro user or PTT Pro group, must exist in the PTT Pro Server and synced to ZEMS.

Before adding an IWG endpoint:

- Review the IWG overview and configuration example in Interworking Gateway.

- Ensure that the site you want to add the endpoint to already exists in PTT Pro Server and has been synced to ZEMS. The sync may take up to 24 hours.

- If the target type is a group, ensure that the group already exists in PTT Pro Server and has been synced to ZEMS. The sync may take up to 24 hours.

1. Click **Add** (✚).

2. Click the **Site** drop-down menu and select a site.

   The site specifies where the endpoint is created. The site must exist in the PTT Pro Serverand synced to ZEMS.

3. Enter the name of the proxy user in the PTT Pro Server in the **Proxy** field.

   The PTT Pro proxy user name corresponds to the User Login field in the Workcloud Communication PTT Pro Management Portal. The proxy name must be between three and 25 characters and can include letters, numbers, and periods (.). An example naming convention might be `SiteName.GroupName.Proxy`.

> ✎ **NOTE:** If the proxy user does not exist in the PTT Pro server, it is created.

4. Select USER or GROUP from the **Target Type** drop-down menu.

5. Select the user or group from the **Target** drop-down menu.

   The user or group must already exist in the PTT Pro Server and synced to ZEMS. If the user or group was recently added to the PTT Pro, wait 24 hours to ensure it syncs to the ZEMS server.

Removing an IWG Endpoint

Remove an IWG endpoint when it is no longer needed. Remove the proxy user from the PTT Pro Server if another IWG endpoint does not use the target.

1. Select an endpoint.

2. Click **Update** (✎).

3. Remove the endpoint by clicking **Delete** in the **Update IWG Endpoint** screen.

4. Click **Delete** in the confirmation dialog.

Verifying an IWG Endpoint

Verify an IWG endpoint to ensure the proxy configuration is correct.

1. Select an IWG endpoint.

2. Click **Verify/Reload Endpoint** (🗄).

   The status of the endpoint appears in the **Events** view.

Sending an Announcement to an IWG Endpoint

Send an audio file or an announcement to an IWG endpoint. The announcement will appear as a missed call to recipients who are offline when it is sent.

NOTE: The maximum length of an audio file is 20 seconds, and the maximum file size is 1MB.

Refer to the Workcloud Communication Announcer REST API Developer Guide to send an announcement from a third-party application.

1. Select an IWG endpoint.

2. Click the Audio icon (🎵)

3. Select an audio file in the **Send Audio Announcement** dialog.
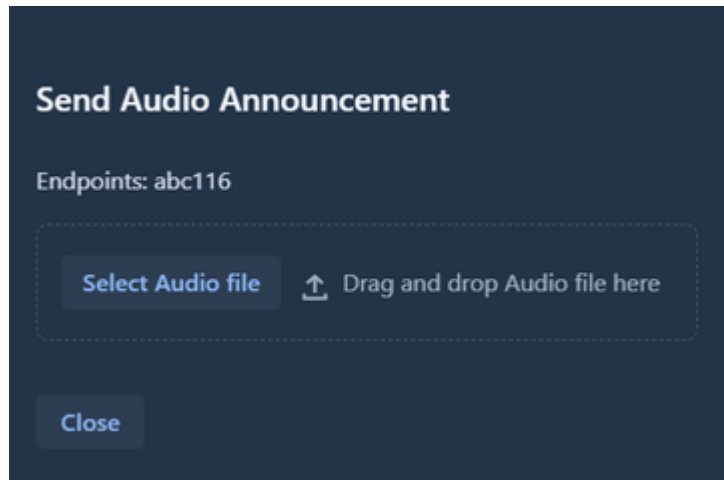
4. Click **Close**. The audio file is processed and sent.

   The announcement is sent as a PTT Pro call. The call ends after the announcement is received.
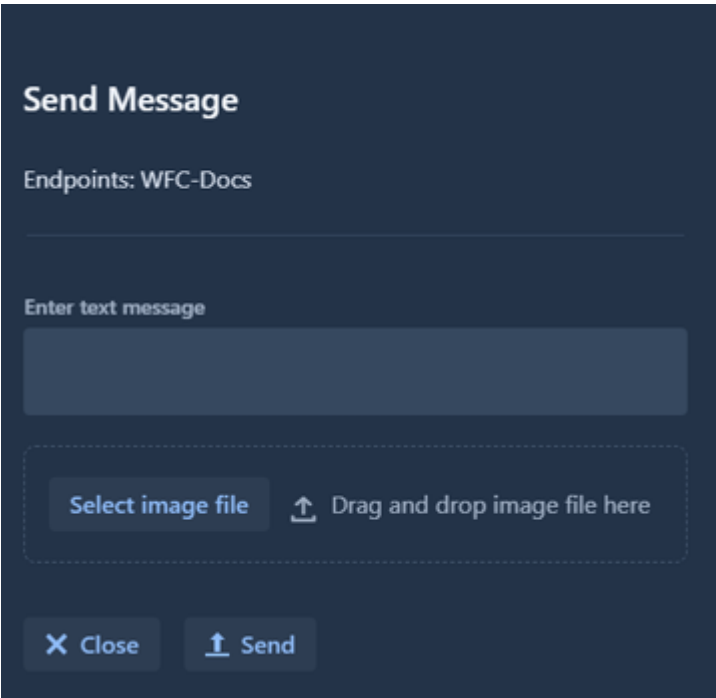
Sending a Text Message to an IWG Endpoint

Send a text message, with an optional image attachment, to an IWG endpoint.

Refer to the Workcloud Communication Messenger REST API Developer Guide to send messages from a third-party application.

1. Select an IWG endpoint.

2. Click **Text Message** (📄).

3. Enter a message in the text box.

4. Optionally, select an image file to include with the message.

5. Click **Send**.

Stats

The **Stats** view lists a summary of all announcer and messenger transactions that occur.

Figure 29   IWG Announcer and Messenger Transactions

The **Stats** view includes the following columns:

Name
> The system-generated name of the event. Use the **Name** menu to filter stats by name.

Value
> The number of transactions.

Timestamp
The time when the statistic was last updated.

System

The **System** view provides access to the **Portal Users** and the **Events** views. You can provide users, with different levels of access, to the portal through Portal Users. The **Events** view lists system events.

Portal Users

Add portal users to help manage your ZEMS data.

The **Add** dialog includes the fields listed below. All fields are required.

Portal User Role
Specify a role for the portal user.

First Name
The first name of the user.

Last Name
The last name of the user.

Login Name
Name the user enters to log in to the portal.

Email
The email address for the user. The email address must be valid because a user can reset their password by email.

Figure 30   Add Portal User

The following roles are available for portal users.

Table 7   Portal User Roles in ZEMS

Role	Description
Super-Admin	• Create, edit, and delete regions and sites • Create, edit, and delete webhooks • Create, edit, and delete IWG endpoints • Send messages and announcements to IWG endpoints • Add, edit, and remove portals users
Admin	• Create, edit, and delete regions and sites • Create, edit, and delete webhooks • Create, edit, and delete IWG endpoints • Send messages and announcements to IWG endpoints
User	• View regions and sites • View webhooks • View IWG endpoints

Events

The **Events** View lists system-level events, such as synchronization with thePTT Pro Server and user-generated events such as sign-in status.

The Events view can be filtered by timestamp, event type, severity, and event source.

Figure 31   Events View

Webhook Integrations

A webhook is a lightweight API that enables external applications to send messages to and receive messages from regions, sites, and groups. Webhooks are defined as incoming or outgoing. An outgoing webhook from ZEMS feeds an incoming webhook of the external application.

Refer to the following sections for instructions on integrating ZEMS with Microsoft Teams, Twilio, or Infobip:

- Creating Webhooks for Microsoft Teams.
- Creating Webhooks for Twilio.
- Creating a Webhook for Infobip.

NOTE: Zebra is not responsible for the procurement, support, or implementation of the third-party services referenced in this section. Please reach out to your sales representative to discuss implementation options.

Refer to Connectors for information about the screens and field descriptions for creating webhooks.

Creating Webhooks for Microsoft Teams

This section describes a validated integration between ZEMS and Microsoft Teams. The validation was tested with Microsoft Teams version 1.5.00.2164. The use of earlier versions of Workcloud Communication PTT Pro or Microsoft Teams cannot be guaranteed to function as described in this document.

Figure 32   Communication Flow Between ZEMS and Microsoft Teams
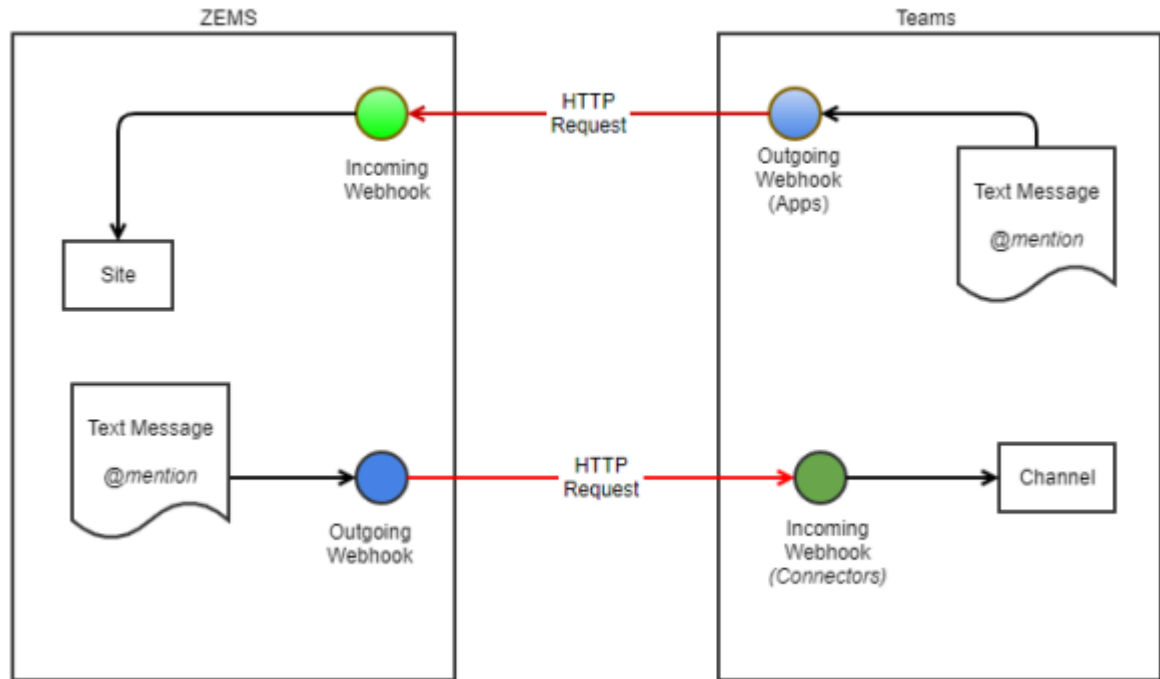
Teams to ZEMS Communication

Configuring communication between ZEMS and Teams involves two steps: creating an incoming ZEMS webhook and creating an outgoing webhook in Teams.

The steps to configure communication between ZEMS and Teams must be performed in this order:

1. Create an incoming ZEMS webhook. A ZEMS webhook URL is generated when the configuration of the incoming ZEMS webhook is complete.

2. Create an outgoing Teams webhook that uses the ZEMS webhook URL. The outgoing Teams webhook is configured for a Team and is valid for all channels within that Team.

Create the Incoming ZEMS Webhook for Teams

Create the incoming ZEMS webhook using the target type and target name. A URL is generated during the creation of the incoming ZEMS webhook This URL must be used when creating the outgoing Teams webhook.

To add an incoming ZEMS webhook, use one of the following methods:

* Use the Incoming Webhooks view to create incoming webhooks targeted to a region, site, group, or user. See Creating an Incoming Webhook.

- Use the Users view to create incoming webhooks targeted to an individual user. See the Users View.

- Use the Groups view to create incoming webhooks targeted to a group. See the Groups View.

- Use the Regions/Sites view to create incoming webhooks to sites or to regions that do not have sites or child regions. See the Regions/Sites View.

- Use the ZEMS API Webhook.Incoming controller to create incoming webhooks targeted to a region, site, group, or user.

Creating the Outgoing Teams Webhook

Create an outgoing webhook in Microsoft Teams and connect it to your incoming ZEMS webhook.
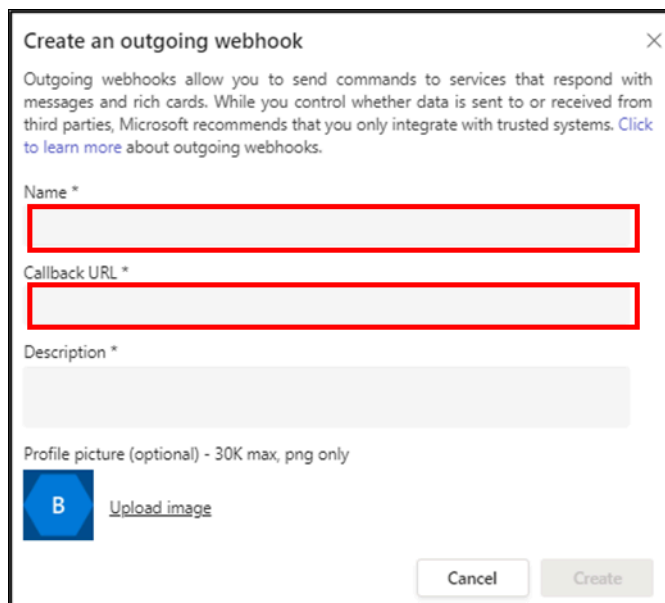
1. Open Teams and click on the ellipses next to the team you want to connect to ZEMS.

2. Select **Manage Team**.
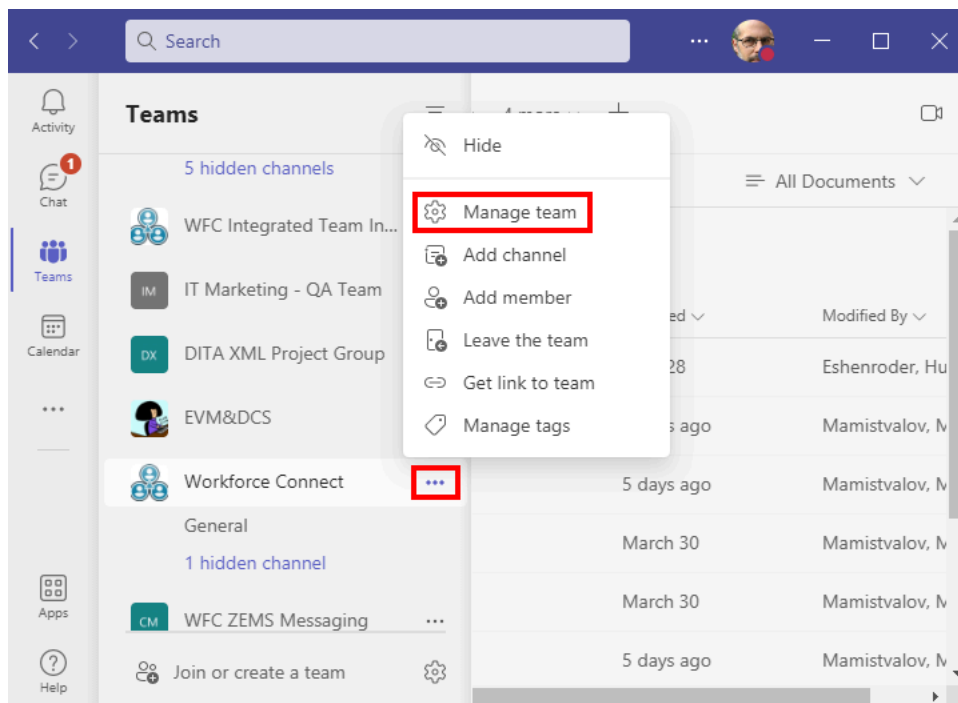
3. Select the **Apps** tab and click on **Create an outgoing webhook**.
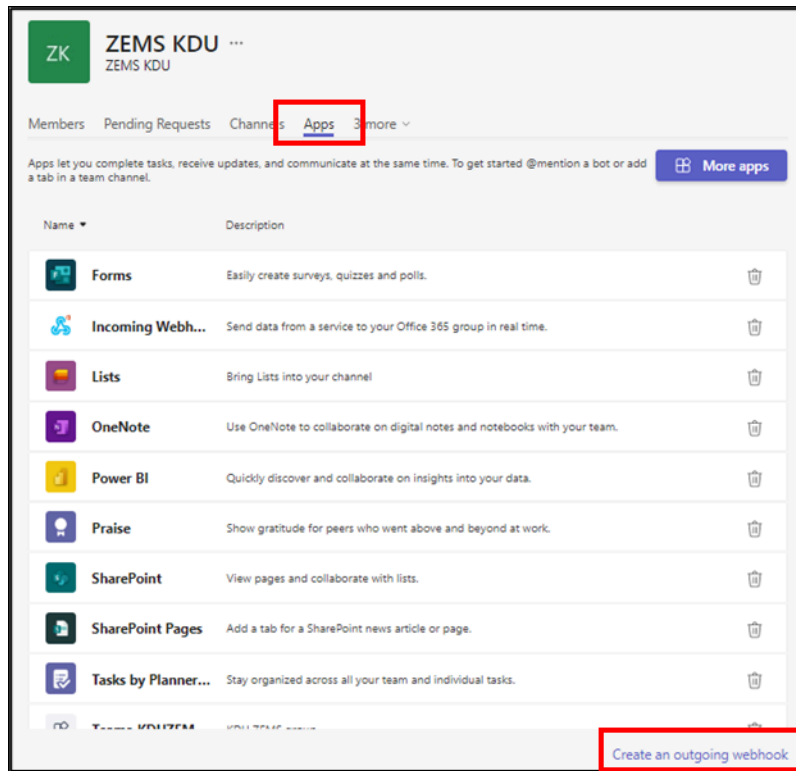
4. Enter a name for the outgoing webhook in the **Name** field. Enter the URL created by ZEMS when you created the incoming webhook in the **Callback URL** field.

The Teams to ZEMS communication is complete. To send a message from Teams to ZEMS, type @, and a list of outgoing webhooks appears.
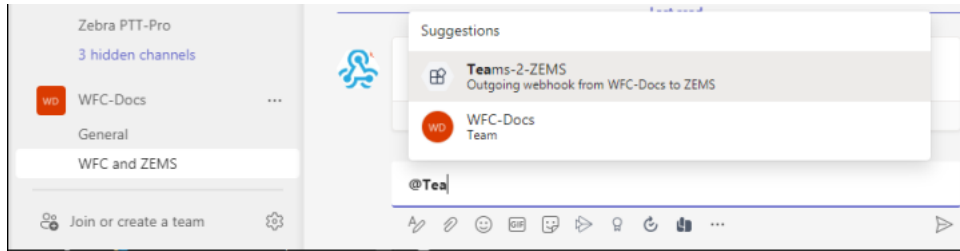
ZEMS to Teams Communication

Configuring communication between ZEMS and Teams requires two steps. First create an incoming webhook in Teams and then create an outgoing webhook in ZEMS.

The steps to configure communication between ZEMS and Teams must be performed in this order:

1. Create an incoming Teams webhook. A Teams webhook URL is generated when you configure the incoming Teams webhook. The incoming Teams webhook is defined on a channel and is only valid for that channel.

2. Create an outgoing ZEMS webhook that uses the incoming Teams webhook URL.
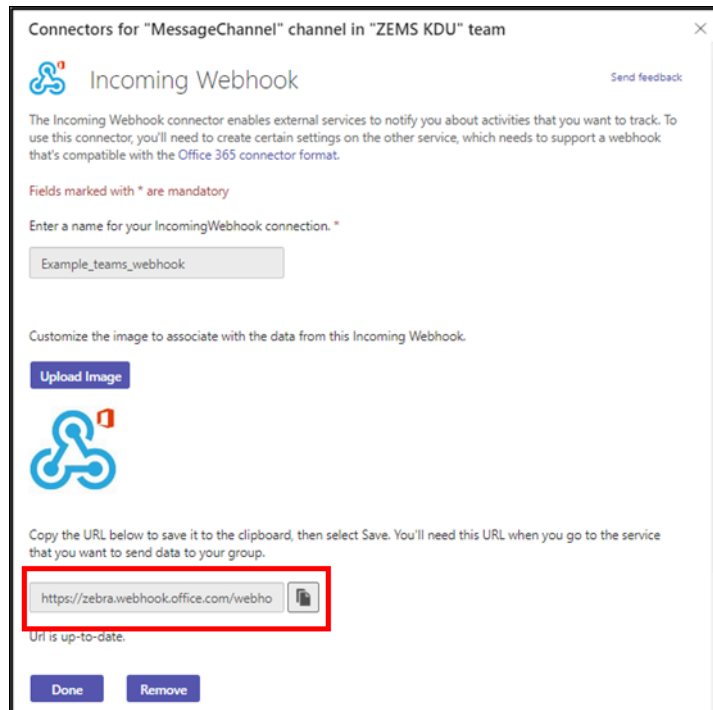
Creating the Incoming Teams Webhook

Create the incoming Microsoft Teams webhook to enable communication from ZEMS to a Teams channel.

1. In the appropriate channel, select the ellipsis and then **Connectors**.

2. Select **Incoming Webhook**.
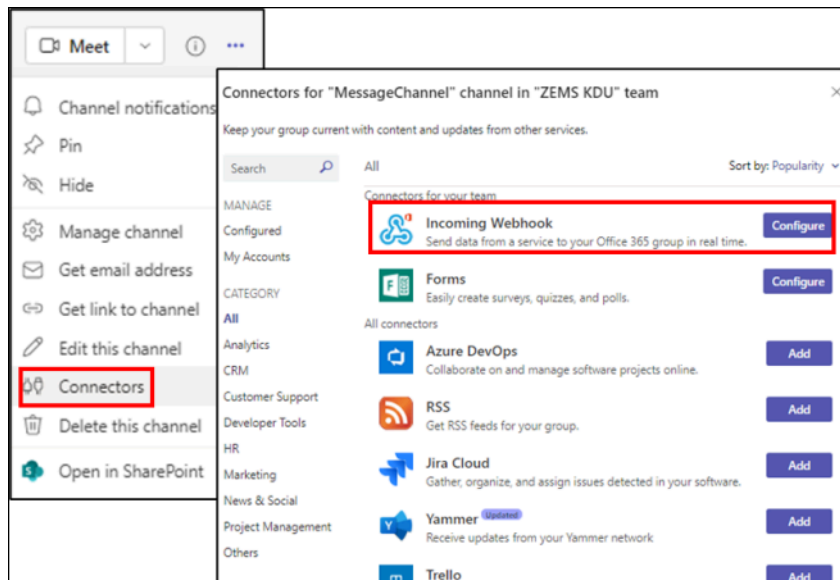
3. Enter a name for your webhook. Save the URL and select **Done**.

Create the Outgoing ZEMS Webhook

Create the outgoing ZEMS webhook using the target name, the Teams incoming webhook URL, and the message body template.

Use one of these methods to add an outgoing ZEMS webhook:

- Use the Outgoing Webhooks view to create an outgoing webhook that originates from regions or sites. See Creating an Outgoing Webhook.

- Use the Regions/Sites view to create an outgoing webhook that originates from a site or region that does not have any sites or child regions. See Regions/Sites View.

- Use the ZEMS API Webhook.Outgoing controller to create outgoing webhooks from regions or sites.

After you create the outgoing ZEMS webhook the ZEMS to Teams communication channel is complete. To send a message from ZEMS to Teams, select a contact, then type @ and a popup list of outgoing webhooks appears. Refer to the Zebra Enterprise Messaging Service Client User Guide for information about sending messages through a webhook.

Creating Webhooks for Twilio

Twilio can be used with ZEMS to provide a communication channel between Workcloud Communication PTT Pro users and external applications or services such as WhatsApp or SMS. This enables enterprise associates to communicate directly with customers using consumer devices.

An example might be a customer sending a text message that they have arrived at a store to pick up purchased items. The difference between the ZEMS integration with Teams is that the ZEMS to Teams and Teams to ZEMS communication channels are independent, ZEMS to Twilio communication depends on Twilio to ZEMS communication to occur first. The reply-path information from the incoming communication is used to send a response back to the customer.

Figure 33   Communication Flow Between ZEMS and Twilio
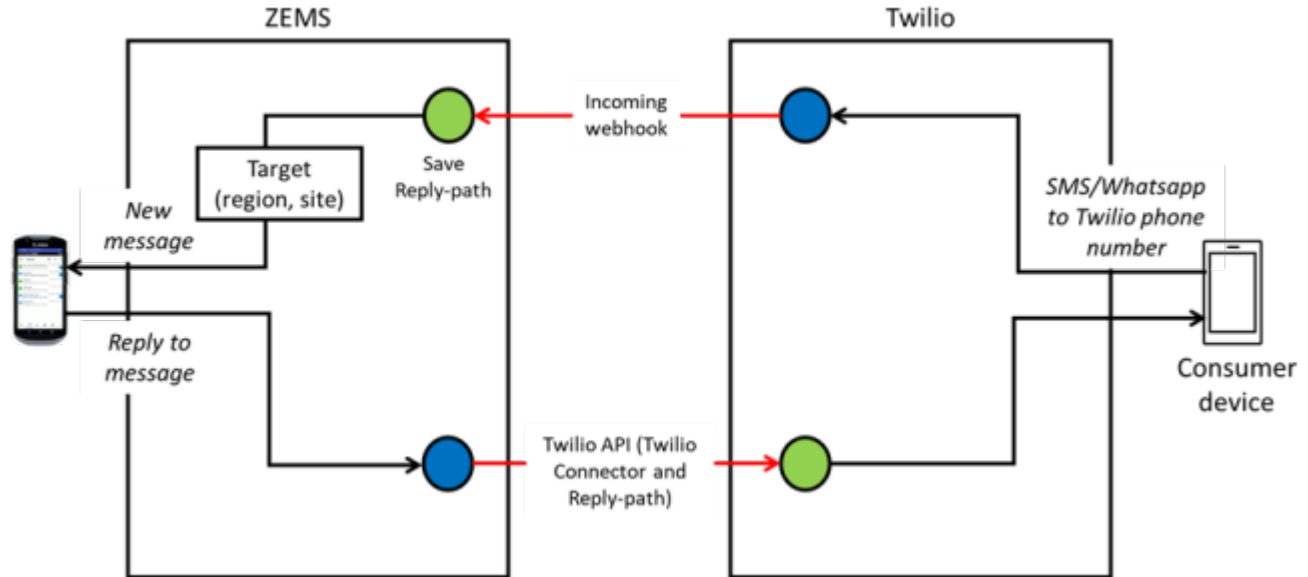
Twilio and ZEMS Communication

Configuring communication between Twilio and ZEMS involves three steps: creating the Twilio connector, creating an incoming ZEMS webhook, and configuring Twilio with the incoming webhook.

The steps to create communication between Twilio and ZEMS must be completed as follows:

1. Create the Twilio Connector as described in Creating a Twilio Connector.

2. Create an incoming ZEMS webhook. A ZEMS webhook URL is generated when the configuration of the incoming ZEMS webhook is complete.

3. Configure the messaging option for the Twilio phone numbers with the incoming ZEMS webhook URL.

Create the Incoming ZEMS Webhook for Twilio

Create the incoming ZEMS webhook using the target type and target name. A URL is generated during the creation of the incoming ZEMS webhook This URL must be used when configuring the phone number in Twilio.

The incoming webhook for Twilio can specify a region, site, group, or user as a target. If the incoming webhook uses the base parameter, then the target must be a region or site. Refer to Types of Incoming Webhooks for more information about the base parameter.

To add an incoming ZEMS webhook, use one of the following methods:

- Use the Incoming Webhooks view to create incoming webhooks targeted to a region, site, group, or user. See Creating an Incoming Webhook.

- Use the Users view to create incoming webhooks targeted to an individual user. See the Users View.

- Use the Groups view to create incoming webhooks targeted to a group. See the Groups View.

- Use the Regions/Sites view to create incoming webhooks to sites or to regions that do not have sites or child regions. See the Regions/Sites View.

- Use the ZEMS API Webhook.Incoming controller to create incoming webhooks targeted to a region, site, group, or user.

Configuring Twilio with the ZEMS Incoming Webhook

Configure a Twilio number with the incoming ZEMS webhook. When you use an incoming webhook with a base parameter, you can use the same incoming webhook for multiple numbers from the same Twilio account. The webhook can target one or more groups and users by using URL query parameters.

1. Open Twilio.com and navigate to **Phone Numbers** > **Manage** > **Active Numbers.**
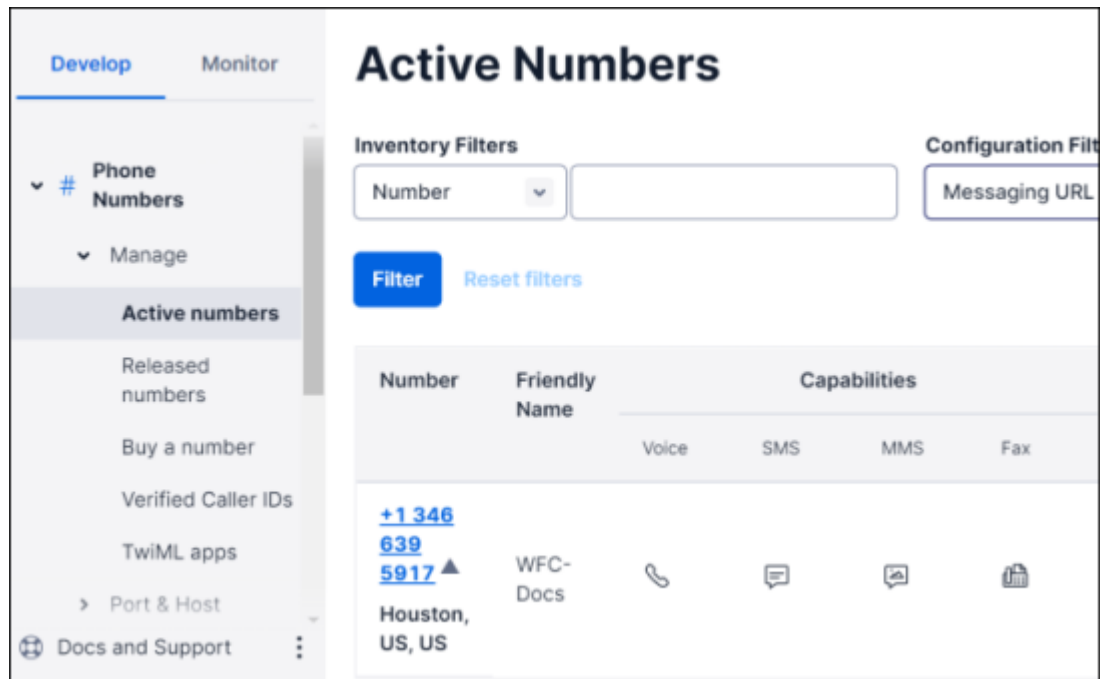
2. Click the Twilio number you want to assign the incoming ZEMS webhook to and scroll down to the **Messaging** section.
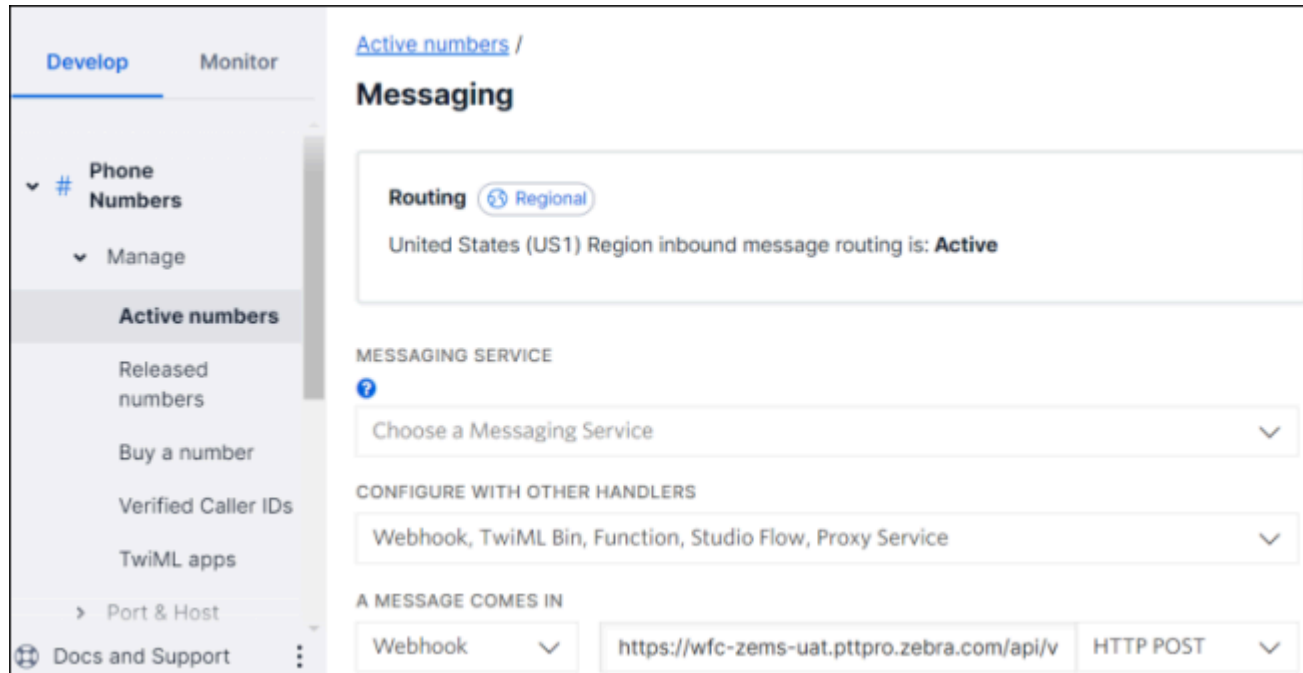
3. Select **Webhook, TwiML Bin, Function, Studio Flow, Proxy Service** from the **CONFIGURE WITH OTHER HANDLERS** drop-down menu.

4. Select **Webhook** from **A MESSAGE COMES IN** drop-down menu.

5. Enter the URL from the incoming ZEMS webhook into the field following **A MESSAGE COMES IN**.

    Add URL query parameters to the URL to specify a site, group, and user targets. Add a **?** character at the end of the URL and use one or more of the following:

    - site=<site name>

    - user=<user name>

    - group=<group name>

    Separate query parameters with the **&** character.

6. Click **Save**.

    Twilio can also be configured with webhooks for WhatsApp. The configuration is similar to the process described above for text messaging. Refer to the [Twilio documentation](#) for more information.

Creating a Webhook for Infobip

Infobip can be used with ZEMS to provide a communication channel between Workcloud Communication PTT Pro users and external applications and services such as WhatsApp and SMS. This enables enterprise associates to communicate directly with customers using consumer devices. An example might be a customer sending a text message indicating that they have arrived at a store to pick up purchased items.

Attachments are not supported for SMS. Additionally, you can only create one Infobip connector for ZEMS.

The Infobip integration with ZEMS differs from Teams integration with ZEMS. While the ZEMS-to-Teams and Teams-to-ZEMS communication channels are independent, the ZEMS-to-Infobip

communication depends on Infobip-to-ZEMS communication occurring first. The reply-path information from the incoming communication is used to send a response back to the customer. Therefore, PTT Pro users cannot send communication to Infobip except as a reply to an incoming message from Infobip.

Figure 34   Communication Flow Between ZEMS and Infobip
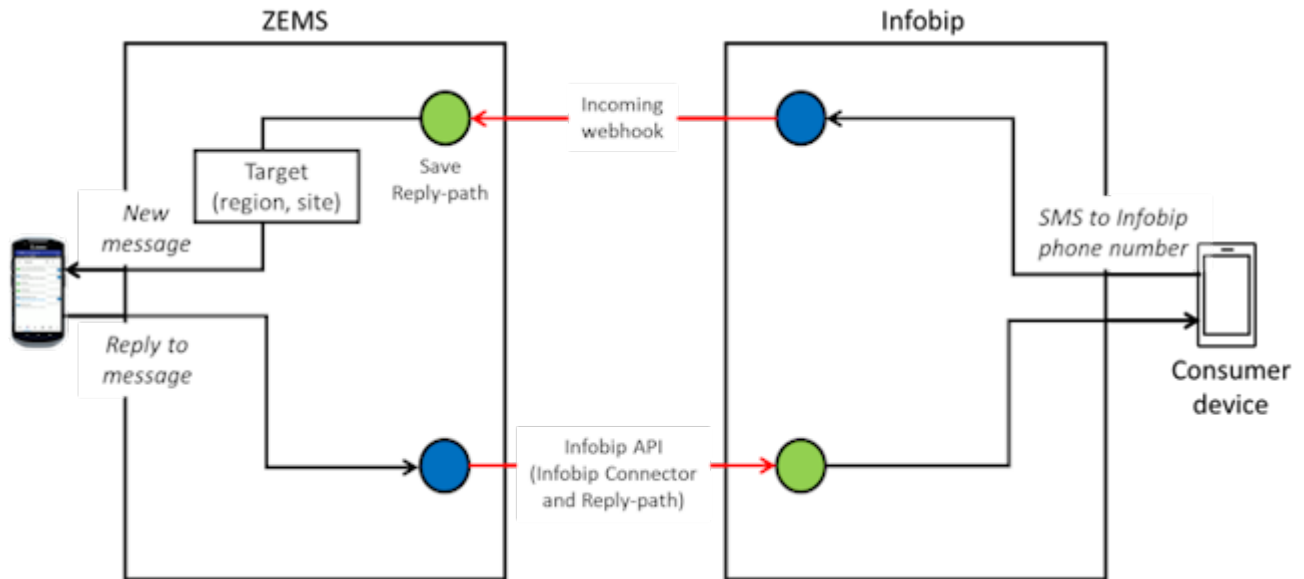
Infobip and ZEMS Communication

Configuring communication between Infobip and ZEMS involves creating the Infobip connector, creating an incoming ZEMS webhook, and configuring Infobip with the incoming webhook.

The steps to create communication between Infobip and ZEMS must be completed in the following order:

1. Create the Infobip Connector as described in Creating an Infobip Connector.

2. Create an incoming ZEMS webhook. A ZEMS webhook URL is generated when you complete the configuration of the incoming ZEMS webhook.

3. Configure the messaging option for the Infobip phone numbers with the incoming ZEMS webhook URL.

> **NOTE:** When a message is sent with an attachment, the recipient will receive two messages. One message contains the message text and the second message contains the attachment.

Create the Incoming ZEMS Webhook for Infobip

Configure an Infobip number with the incoming ZEMS webhook. Use an incoming webhook with a base parameter so that you can use the same incoming webhook for multiple numbers from the same Infobip account. The webhook can target one or more groups and users by using URL query parameters.

The incoming webhook for Infobip can specify a region, site, group, or user as a target. If the incoming webhook uses the base parameter, then the target must be a region or site. Refer to Types of Incoming Webhooks for more information about the base parameter.

To add an incoming ZEMS webhook, use one of the following methods:

- Use the Incoming Webhooks view to create incoming webhooks targeted to a region, site, group, or user. See Creating an Incoming Webhook.

- Use the Users view to create incoming webhooks targeted to an individual user. See the Users View.

- Use the Groups view to create incoming webhooks targeted to a group. See the Groups View.

- Use the Regions/Sites view to create incoming webhooks to sites or to regions that do not have sites or child regions. See the Regions/Sites View.

- Use the ZEMS API Webhook.Incoming controller to create incoming webhooks targeted to a region, site, group, or user.

## Configuring Infobip with the ZEMS Incoming Webhook

Configure an Infobip number with the incoming ZEMS webhook. Use an incoming webhook with a base parameter so that you can use the same incoming webhook for multiple numbers from the same Infobip account. The webhook can target one or more groups and users using URL query parameters.

1. Open Infobip.com and navigate to **Channels and Number** > **SMS**.
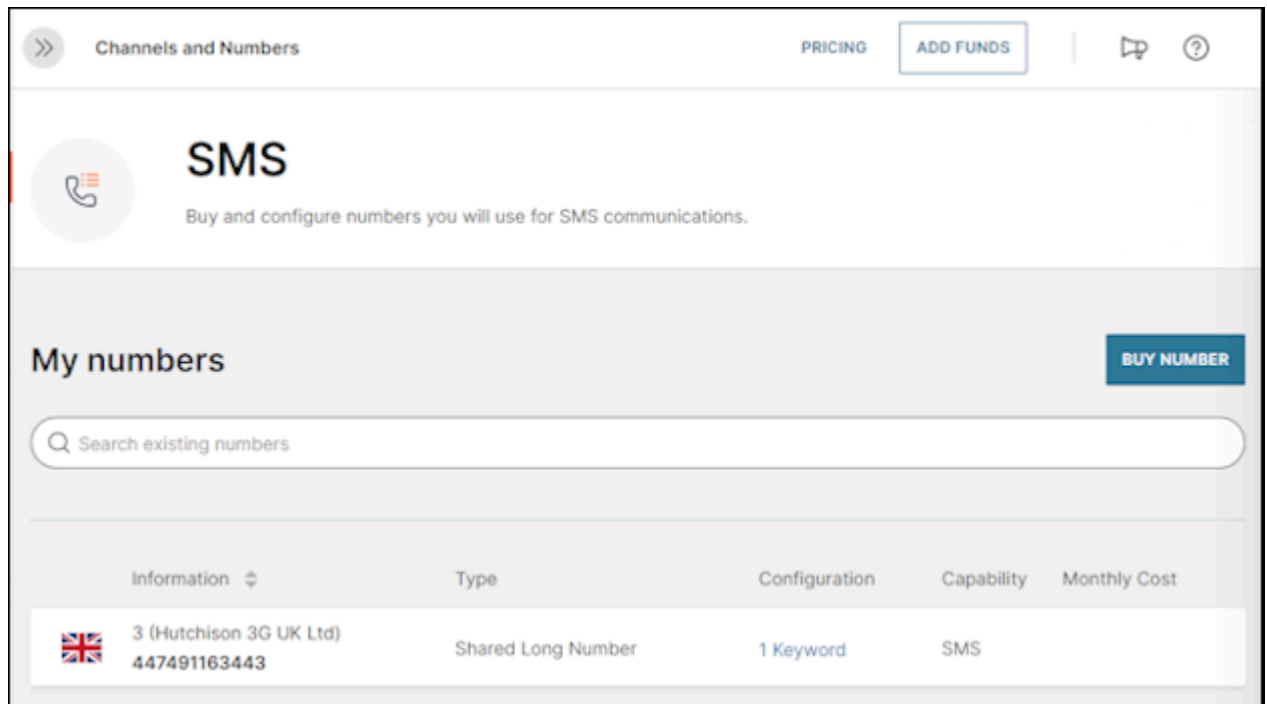
2. Click the Infobip number you want to assign the incoming ZEMS webhook to and click **Add Keyword**.

3. Configure the **Add keyword** dialog with the following information:

   - Set **Forwarding** to Forward to HTTP.
   - Set **Method** to POST.
   - Set **Format** to JSON.
   - Enter the URL from the ZEMS incoming webhook in the **URL** field.

4. Optionally, if you created a base incoming webhook, configure it with these parameters:

   - Add `?` at the end of the URL to specify targets.
   - `site` = PTT Pro department or ZEMS site
   - `user` = PTT Pro user name
   - `group` = PTT Pro group

   Separate query parameters with &. Refer to Types of Incoming Webhooks for more information about webhook parameters.

5. Click **Save**.

Infobip can also be configured with webhooks for WhatsApp. The configuration is similar to the previous process described for text messaging. Refer to the Infobip documentation for more information.

Unsupported MIME Types

The following table lists MIME types that are not supported between WhatsApp and ZEMS.

Table 8 Unsupported MIME Types Between ZEMS and WhatsApp

Type	MIME Type	WhatsApp to PTT Pro	PTT Pro to WhatsApp	Comment
STICKER	image/webp	Not Supported	Not Supported	Supported by Infobip but not supported by ZEMS.
IMAGE	image/gif	Not Supported	Not Supported	Supported by Infobip but not supported by ZEMS.
AUDIO	All formats	Not Tested	Supported	Requires a dedicated WhatsApp business number.
VIDEO	All formats	Not Tested	Supported	Requires a dedicated WhatsApp business number.
DOCUMENT-MS-WORD (.doc)	application/vnd.ms-word	Not Supported	Not Supported	
DOCUMENT-MS-WORD (doc.x)	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Not Tested	Supported	Requires a dedicated WhatsApp business number.
DOCUMENT- MS-EXCEL (.xls)	application/vnd.ms-excel	Not Supported	Not Supported	
DOCUMENT- MS-EXCEL (.xlsx)	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Not Tested	Supported	Requires a dedicated WhatsApp business number.
DOCUMENT- MS-PPT (.ppt)	application/vnd.ms-powerpoint	Not Supported	Not Supported	
DOCUMENT- MS-PPT (.pptx)	application/vnd.openxmlformats-officedocument.presentationml.presentation	Not Tested	Supported	Requires a dedicated WhatsApp business number.
DOCUMENT-TXT	text/plain	Not Supported	Not Supported	
Location		Not Supported	Not Supported	Supported by Infobip but not supported by ZEMS.
Contact-Vcard		Not Supported	Not Supported	Supported by Infobip but not supported by ZEMS.

Configuring PTT Pro Clients for ZEMS

PTT Pro for Android, PTT Pro for iOS, and the ZEMS Web Client require configuration to use ZEMS messaging. The Workcloud Communication PTT Pro clients require the URL to the ZEMS server and the API key while the web client requires OAuth2 for authorization and access.

ZEMS Configuration Parameters for PTT Pro for Android

PTT Pro for Android uses JSON parameters to configure clients for ZEMS.

A sample JSON configuration might appear as follows:

```
{
    "zemsServerURL":"https://serverurl:port",
    "zemsServerApiKey":"thisisyourAPIKey",
}
```

Table 9   JSON Configuration Parameters

Parameter	Description	Type	Default Value	Configurable Values	Configurable using Provisioning Manager
zemsServerUL	URL to the ZEMS server.	String	N/A	valid URL	Yes
zemsServerApiKey	API token required to authorize with the ZEMS server.	String	N/A	valid Token	Yes
zemsSentStatusViewEnable	Shows the sent status view when enabled.	Boolean	true	true false	Yes
zemsUserCountViewEnable	Shows the user count view when enabled.	Boolean	false	true false	Yes

Troubleshooting

The message `Error connecting to ZEMS Service`, indicates a configuration error.

Figure 35   ZEMS Connection Error in Snackbar
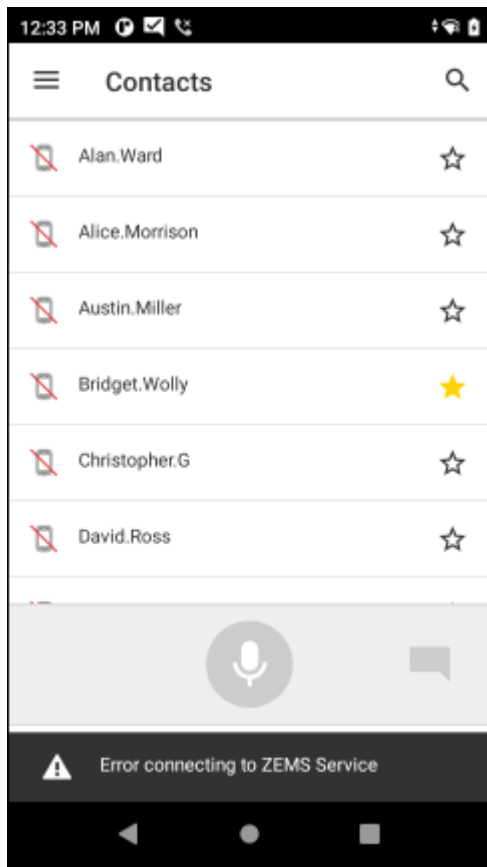
cause this error:

- The PTT Pro user is not yet synchronized with ZEMS.

- The ZEMS configuration is incorrect or PTT Pro cannot connect to the ZEMS server.

ZEMS Configuration Parameters for PTT Pro for iOS

Customer administrators can install and configure PTT Pro for iOS using Mobile Device Management (MDM) software. PTT Pro for iOS supports standard iOS device management features.

For more information about iOS device management features, refer to:

- [Managed AppConfig Sample](#)

- [AppConfig](#)

Refer to the Workcloud Communication PTT Pro Installation Guide for information regarding the managed app configuration XML files for iOS.

XML Configuration File for ZEMS

The following XML provides the XML values for an `iOS_mdm_specfile.xml` for ZEMS. These parameters might be part of a larger configuration file for PTT Pro for iOS.

```
<boolean keyName="zemsEnabled">
```

69

```
            </boolean>
            <string keyName="zemsServerURL">
            </string>
            <string keyName="zemsServerApiKey">
            </string>
```

Table 10   Key Value Pairs for ZEMS

keyName	Type	Description
zemsEnabled	Boolean	Enables ZEMS for the PTT Pro for iOS client. When enabled, legacy messaging is disabled.
zemsServerURL	String	URL used by the client app to access the ZEMS server.
zemsServerApiKey	String	Authorization token is required for the client app to access the ZEMS server.

Masking ZEMS Login Parameters

On the PTT Pro for iOS login screen, you can mask the ZEMS URL and ZEMS API key. You can mask either parameter or both. The parameters for masking these fields can be applied through a Provisioning Manager token that is scanned by the device or deployed in the XML of the device configuration.

Table 11   Mask ZEMS Parameters

Parameter	Description	Type	Default	Configurable Values
maskZemsServerURL	When true, masks the URL for the ZEMS Server on the login screen.	Boolean	false	true false
maskZemsServerApiKey	When true, masks the ZEMS Server API key on the login screen.	Boolean	false	true false

JSON Example

In the following example, the parameters are true and the URL and API key would be masked on the PTT Pro for iOS login screen.

```
{
"zemsEnabled" : true,
"maskZemsServerURL" : true,
"maskZemsServerApiKey" : true,
"zemsServerURL" : "<server_url",
"zemsServerApiKey" : "<api_key>"
}
```

Device Examples

Figure 36   Unmasked ZEMS Parameters
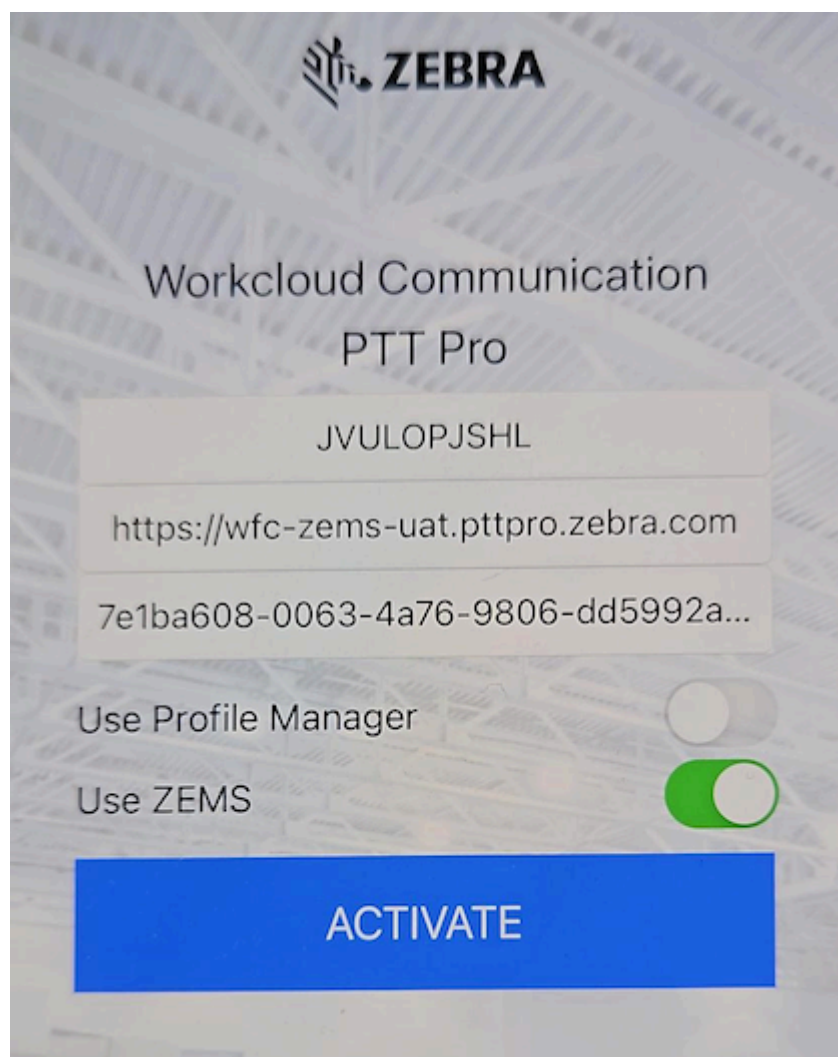
Figure 37   Masked ZEMS Parameters
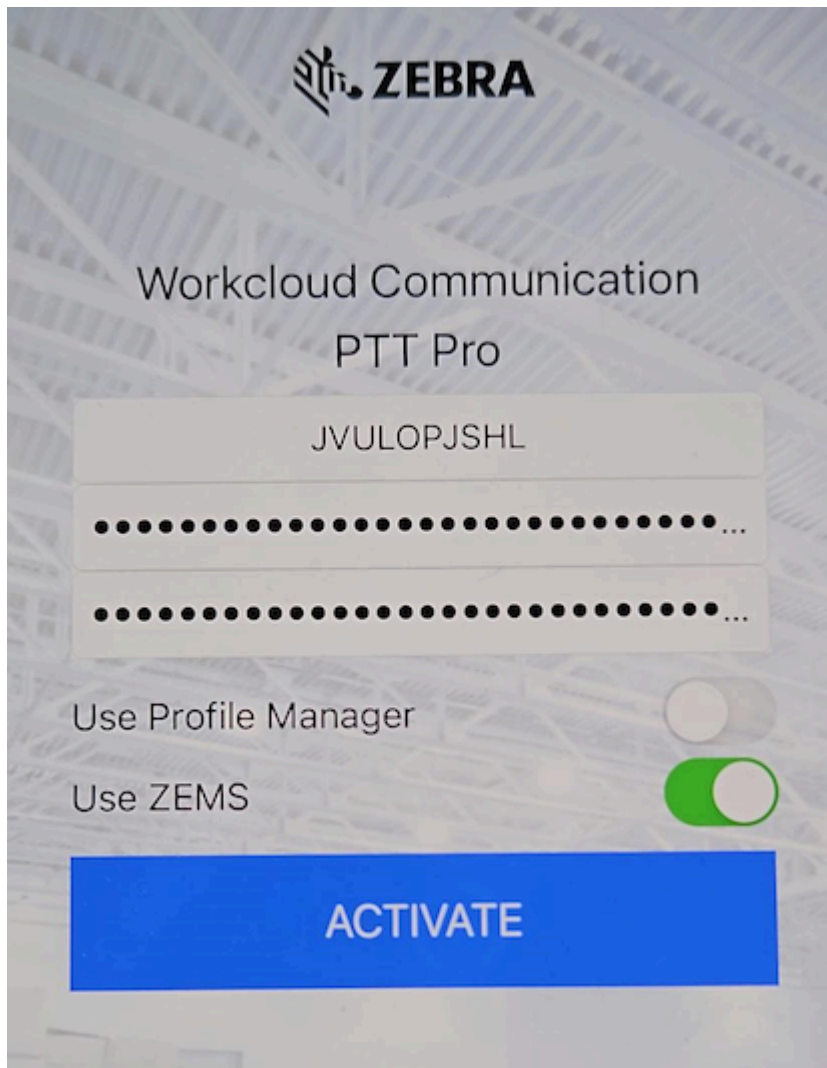
ZEMS Configuration for the Web Client

The ZEMS Web Client requires the customer to provide an OAuth2 domain to authorize PTT Pro users who access ZEMS using the web client. The ZEMS and PTT Pro Server must be configured to use OAuth2. After the PTT Pro Server is configured to use OAuth2, users must enter their OAuth2 credentials to log in to PTT Pro for Android or PTT Pro for iOS.

Refer to Configuring OAuth2 Authentication for information about configuring AD/ADFS for the ZEMS Web Client.

OAuth2 Parameters

The ZEMS server uses the following OAuth2 parameters:

client_id
    The OAuth2 client ID identifies the ZEMS Web Client. This parameter is also used by the Workcloud Communication PTT Pro clients.

access_url
> The OAuth2 access URL is used by the ZEMS Web Client to obtain a Grant Token. This parameter is also used by the Workcloud Communication PTT Pro clients.

oauth_url
> The OAuth2 authorization URL is used by the ZEMS Web Client to authorize and obtain an Access Token and a Refresh Token. This parameter is also used by the Workcloud Communication PTT Pro clients.

logout_url
> The OAuth2 logout_url is used to log out of the ZEMS Web Client. This parameter is not used by the Workcloud Communication PTT Pro clients.

Configuring OAuth2 Authentication

An OAuth2 authentication server must be configured with a callback URI pointing to the public URI of the Web Client service. The callback URI must be of the form `https://{ZEMS_URL}/client/redirect`, where `ZEMS_URL` is the URL of the ZEMS server.

Refer to the [AD/ADFS Integration Guide for PTT Pro and Profile Manager](#) for more information about configuring OAuth2 for PTT Pro for Android.

1. In the ADFS server, right-click on **Application Group** and select **Properties**.
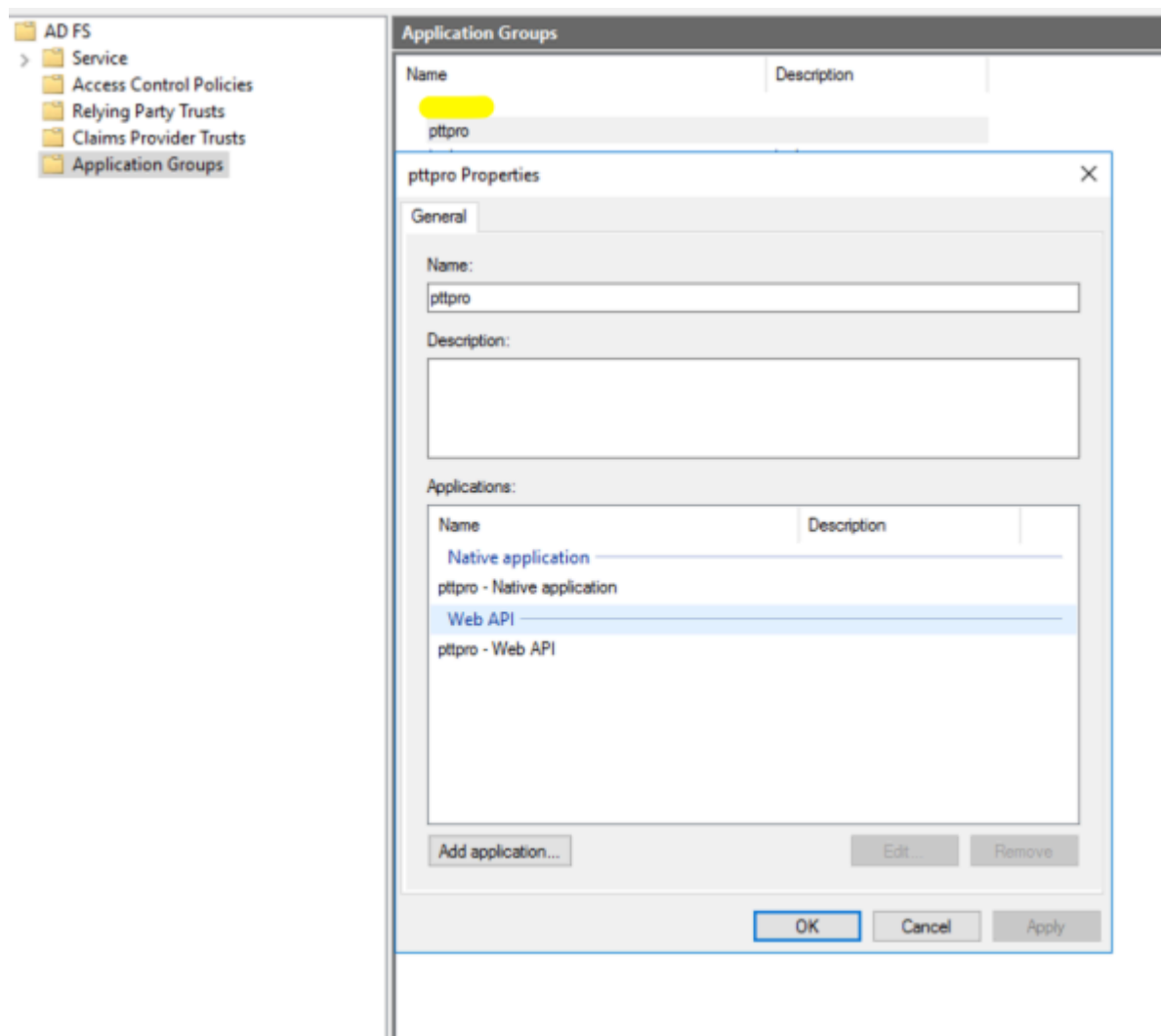
2. Select the Native application and click **Edit**.
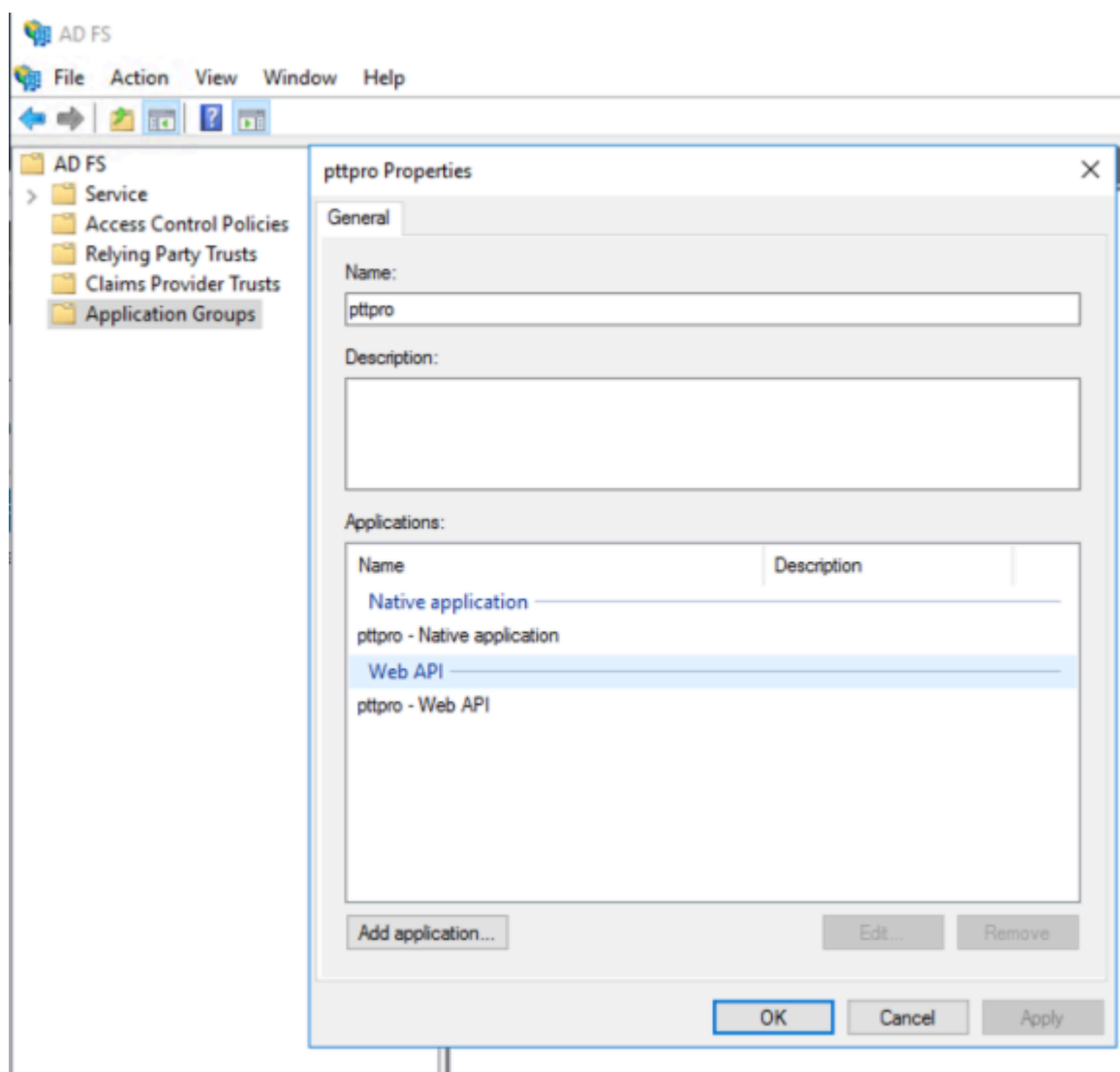
3. Enter the redirect URI to the **Redirect URI** field.

   The redirect URI must be of the form `https://{ZEMS_URL}/client/redirect`, where `ZEMS_URL` is the URL of the ZEMS server.
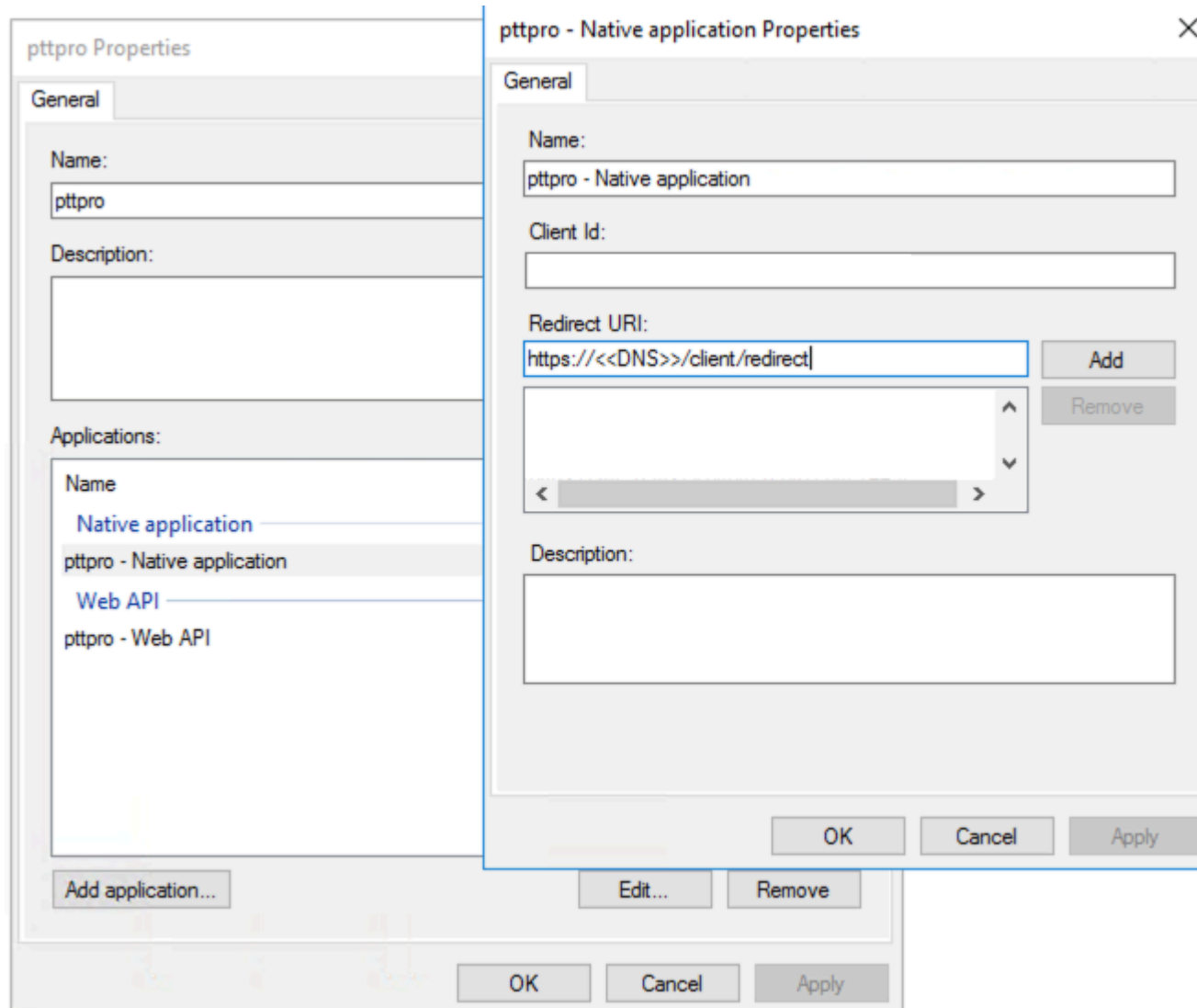
4. Click **OK** to close the **Native application Properties** dialog and **OK** to close the Application Group dialog.

ZEMS API Endpoints

The ZEMS APIs provide a way to view and manage regions and webhooks programmatically.

The Swagger URL provides access to the API endpoints and can be used to experiment with the methods of each endpoint. When you execute a method on the Swagger page, a curl command example is displayed and can be used to create additional API calls.

You can access the Swagger page from the Show Menu in Top Toolbar. Your API key is available from the **Customer Details** screen, which is also accessed from the **Show** Menu.

> **NOTE:** The `System.Alarms` and `System.Customer` endpoints are visible on the Swagger page but are not intended for customer use.

Authenticate to Use Swagger

You must authenticate with your API key to execute the ZEMS endpoint methods using the Swagger page.

1. Click **Authorize** at the top of the Swagger page to open the **Available authorizations** dialog.

2. Enter the API key, or token, in the Value field.

   The API key is shown on the **Customer Details** screen.

3. Click **Authorize** .

4. Enter your user name and password in the **username** and **password** fields and click **Authorize**.

   The Authorize button shows a closed lock.

IWG Communication Endpoint

Use the IWG.Communication endpoint to retrieve a list of endpoints, send an announcement (audio message), or send a text message with an optional image.

The IWG.Communication endpoint includes the following methods:

Method	Description
`GET /iwg/api/v1/list`	Retrieves a list of all IWG endpoints.
`POST /iwg/api/v1/announcement`	Sends an audio file to the specified IWG endpoint.
`POST /iwg/api/v1/message`	Sends a text message to the specified IWG endpoint. An optional image can also be sent with the message.

Refer to the Workcloud Communication Messenger REST API Developer Guide Guide and the Workcloud Communication Announcer REST API Developer Guide for more information regarding these endpoints.

IWG Endpoints

Use the IWG.Endpoints to add, delete, and verify IWG endpoints.

The IWG.Endpoints includes the following methods:

Method	Description
`DELETE /iwg/api/v1/endpoints`	Deletes multiple endpoints. Specify each endpoint by its name.
`DELETE /iwg/api/v1/endpoints/{eid}`	Deletes endpoints identified by their endpoint name, site name, target type, target name, and proxy name.
`GET /iwg/api/v1/endpoints`	Retrieves all of the endpoints for the specified site.
`GET /iwg/api/v1/endpoints/{eid}`	Retrieves endpoints identified by their endpoint name, site name, target type, target name, and proxy name.
`PATCH /iwg/api/v1/endpoints`	Verifies the endpoints. Specify each endpoint by its name.
`POST /iwg/api/v1/endpoints`	Creates an endpoint. This method requires the endpoint name, site name, target type, target name, and proxy name.

IWG Import Endpoint

Use the IWG.Import endpoint to bulk create endpoints.

The IWG.Import endpoint includes the following methods:

Method	Description
`GET /iwg/api/v1/import/template`	Downloads a CSV template for specifying endpoints to import.
`POST /iwg/api/v1/import/csv`	Imports a CSV that specifies multiple IWG endpoints. ZEMS creates the endpoints using the enclosed data, which must include the site name, endpoint name, proxy name, and target name for each endpoint. **NOTE:** The Contact parameter is a Boolean value: FALSE for a group target type and TRUE for a user target type.

Region Endpoint

Use the Region endpoint to manage regions.

The Region endpoint includes the following methods:

Method	Description
`POST /api/v1/region`	Add or update a region and, optionally, its children. The region is added as a top-level region if a parent region is not specified.
`GET /api/v1/region`	Returns a hierarchical list of all regions.
`GET /api/v1/region/nodes`	Returns a hierarchical list of all regions but includes additional information such as the number of registered users in each region.
`GET /api/v1/region/{regionName}`	Returns the specified region and any child regions.
`DELETE /api/v1/region/{regionName}`	Deletes the specified region. This also deletes any child regions and removes any associated managers or sites.

Region Example

This example creates a top-level Region named East, which has a child region named District3. District3 has two sites named Site4 and Site5.

The Swagger parameters for this example:

```
[
  {
    "name": "East"
    "description": "Eastern Region",
    "children": [
      {"name": "District3",
       "description": "Chicago",
       "children": [
          {"name": "Site4"},
```

```
            {"name": "Site5"}
        ]
      }
    ]
  }
]
```

The curl command for this example:

```
curl -X 'POST' \
    'https://<ZEMS_URL>/api/v1/region' \
    -H 'accept: application/json' \
    -H 'ApiKey: <ZEMS_API_KEY>' \
    -H 'authorization: Bearer <TOKEN>' \
    -H 'Content-Type: application/json' \
    -d '[ { "name": "East", "description": "Eastern Region", \
        "children": [ {"name": "District3", "description": "Chicago", \
        "children": [ {"name": "Site4"}, {"name": "Site5"} ] } ] } ]'
```

Region Managers Endpoint

Use the Region.Manager endpoint to add, remove, and retrieve a list of region and site managers.

The Region.Managers endpoint includes the following methods:

Method	Description
POST /api/v1/region/managers/{regionName}	Add a manager to a region or site. The manager must be a valid PTT Pro user.
GET POST /api/v1/region/managers/{regionName}	Returns all managers for the specified region. This method does not return managers for child regions.
GET /api/v1/region/managers/{regionName}/{managerName}	Returns the region manager specified by the region and manager name. This method does not return managers for child regions.
DELETE /api/v1/region/managers/{regionName}/{managerName}	Removes the region manager from the specified region.

Region Managers Example

This example adds a manager named Ernest Shackleton to the East region.

```
curl -X 'POST' \
 'https://<ZEMS_URL>/api/v1/region/managers/East?user=Ernest.Shackleton' \
 -H 'accept: application/json' \
 -H 'ApiKey: <ZEMS_API_KEY>' \
 -H 'authorization: Bearer <TOKEN>' \
 -d ''
```

Region Sites Endpoint

Use the Region.Sites endpoint to manage sites.

The Region.Sites endpoint includes the following methods:

Method	Description
POST /api/v1/region/sites/{regionName}	Add one or more sites to a region. If a site previously belonged to a different region, it will be reassigned to this region. Multiple sites must be separated by commas.
GET /api/v1/region/sites/{regionName}	Returns all sites. If a region is specified, returns the sites from that region. This method does not return sites for child regions.
GET /api/v1/region/sites/{regionName}/{siteName}	Returns a single site specified by the region and site name.
DELETE /api/v1/region/sites/{regionName}/{siteName}	Deletes the site specified by the region and site name.

Sites Parameters

Regions that do not contain child regions must have sites. A response from an API call for a site returns the following parameters:

Table 12   Site Parameters in API Responses

Parameter	Example	Description
"id"	1020	Internal ID of the site.
"customer_id"	1	ZEMS customer ID.
"parent"	393	Parent region ID.
"deleted"	true	This site was deleted from the PTT Pro server and then removed from ZEMS.
"part"	0	Randomly assigned number when a new site is added to the database.
"name"	"R13OP"	Site name.
"description"	"Lincolshire, IL"	Site description.
"created_at"	1637688569	Timestamp when the site was created.
"updated_at"	1637714700	Timestamp when the site was last updated.

Region Sites Example

This example adds two sites to the District3 region.

```
curl -X 'POST' \
 'https://<ZEMS_URL>/api/v1/region/sites/District3' \
 -H 'accept: application/json' \
 -H 'ApiKey: <ZEMS_API_KEY>' \
 -H 'authorization: Bearer <TOKEN>' \
 -H 'Content-Type: application/json' \
```

```
-d 'Site1,Site2'
```

Incoming Webhook Endpoint

Use the Webhook.Incoming endpoint to manage webhooks intended for ZEMS users, groups, sites, or regions.

The Webhooks.Incoming endpoint includes the following methods:

Method	Description
POST /api/v1/connector/app	Creates an incoming webhook and returns the `appId`and URL parameters. The `appId` is used by this endpoint to display or delete the webhook. The URL parameter is required for the outgoing webhook on the external application. When `base` is true, the target must be a region or site.
GET /api/v1/connector/app	Returns all incoming webhooks.
GET /api/v1/connector/app/{appId}	Returns the incoming webhook specified by the `appId`.
DELETE /app/v1/connector/app/{appId}	Removes the incoming webhook specified by the `appId`.

When you create an incoming webhook, the method requires that the target is identified.

Target	Value	Description
User	0	User name as specified in the PTT Pro server.
Group	1	Group name as specified in the PTT Pro server.
Site	2	Department name as specified in the PTT Pro server.
Region	3	Region name as defined in ZEMS.

Outgoing Webhook Endpoint

Use the Webhook.Outgoing to create a webhook that sends a message to an external application.

The Webhook.Outgoing includes the following methods:

Method	Description
POST /api/v1/connector/webhook	Creates an outgoing webhook that returns a `whId` parameter to display or delete this webhook.
GET /api/v1/connector/webhook	Returns a list of all of the outgoing webhooks.
GET /api/v1/connector/webhook/whId}	Returns the outgoing webhook specified by the `whId`.

Method	Description
`DELETE /api/v1/connector/webhook/{whId}`	Delete the outgoing webhook specified by the `whId`.

When you create an outgoing webhook, the request requires the following parameters:

Parameter	Required	Value	Description
body	Yes	Refer to the Message Body Template for the parameters of the message body.	Describes the message format.
headers	No	NA	Not required for a webhook to Microsoft Teams.
method	No	NA	Not required for a webhook to Microsoft Teams.
url	Yes	Valid URL	URL generated when creating the incoming webhook from the external application. Must include `https://`.
description	No	Alphanumeric text	Enter a description of the outgoing webhook.
name	Yes	Alphanumeric text	Unique name for this webhook.
site	Yes	Alphanumeric text	Must match the region or site name.

Outgoing Webhook Example

This example adds an outgoing webhook from Site4 to an incoming Microsoft Teams webhook.

```
curl -X 'POST' \
  'https://<ZEMS_URL>/api/v1/connector/webhook' \
  -H 'accept: application/json' \
  -H 'ApiKey: <ZEMS_API_KEY>' \
  -H 'authorization: Bearer <TOKEN>' \
  -H 'Content-Type: application/json' \
  -d '{ "body": "{\"type\": \"message\", \"text\": \"$SENDER: $BODY\"}", \
      "description": "an example webhook", "name": "OutgoingSiteWebhook", \
      "site": "Site4", "url": "<TEAMS_INCOMING_WEBHOOK_URL" }'
```

Message of the Day (MOTD) Endpoint

PTT Pro users on WS50 can now receive MOTD (Message of The Day) voice messages with a prerecorded announcement to a user or a group of users. The MOTD endpoint enables users to send short text or audio messages as broadcast messages. Messages are sent using the Google Cloud Pub/Sub messaging service. MOTD notifications have a 64-character limit, notificaitons with more characters will be truncated.

Use the following endpoints for MOTD.

Method	Description
`POST api/v1/register/user`	Register the user with the device type of `DeviceTypeAndroidWearable(300)` to receive message notifications.

Method	Description
`GET /api/v1/client/message/recent`	Retrieve the most recent messages from the user.
`POST /api/v1/signout/user`	Sign out the user and de-register the push ID.

MOTD Example

This example registers a user to receive notifications from the GCP Pub/Sub service.

```
curl -X 'POST' \
'https://<ZEMS_URL>/api/v1/register/user' \
-H 'accept: application/json' \
-H 'ApiKey: <ZEMS_API_KEY>' \
-H 'Content-Type: application/json' \
-d '{
"device_push": {
  "device_id": "",
  "device_type": 300,
  "push_id": "",
  "push_route": ""
},
"password": "",
"server": "",
"settings": "",
"userlogin": ""
}'
```

This example retrieves the three most recent messages from the user.

```
curl -X 'POST' \ 'https://<ZEMS_URL>/api/v1/client/message/recent?
numberOfMessage=3 \
-H 'accept: application/json' \
-H 'ApiKey: <ZEMS_API_KEY>' \
-H 'authorization: Bearer <TOKEN>' \
-H 'Content-Type: application/json' \
```

This example signs out the user and de-registers the push ID. This command is called by a client when the user signs out.

```
curl -X 'POST' \ 'https://<ZEMS_URL/api/v1/signout/user ' \
-H 'accept: application/json' \
-H 'ApiKey: <ZEMS_API_KEY>' \
-H 'authorization: Bearer <TOKEN>' \
-H 'Content-Type: application/json' \
-d '{
"device_id": "",
"device_type": 300,
"push_id": "",
"push_route": ""
}'
```