Copyright

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2019 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

COPYRIGHTS & TRADEMARKS: For complete copyright and trademark information, go to www.zebra.com/copyright.

WARRANTY: For complete warranty information, go to www.zebra.com/warranty.

END USER LICENSE AGREEMENT: For complete EULA information, go to www.zebra.com/eula.

Terms of Use

- Proprietary Statement
  This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries (Zebra Technologies™). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

- Product Improvements
  Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

- Liability Disclaimer
  Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

- Limitation of Liability
  In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.
Revision History

Changes to the original guide are listed below:

<table>
<thead>
<tr>
<th>Change</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-01 Rev A</td>
<td>5/2017</td>
<td>Initial release.</td>
</tr>
<tr>
<td>-03 Rev A</td>
<td>8/2018</td>
<td>Updates to Announcer API and Messenger API information. Streaming feature renamed Content Sharing. Multiple announcers now available. Announcer mapping no longer required. LMR Gateway renamed to IP Gateway.</td>
</tr>
<tr>
<td>-04 Rev A</td>
<td>12/2018</td>
<td>Updates to Overview chapter, and Media Tab in Using IWG</td>
</tr>
</tbody>
</table>
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copyright</td>
<td>2</td>
</tr>
<tr>
<td>Terms of Use</td>
<td>2</td>
</tr>
<tr>
<td>Revision History</td>
<td>3</td>
</tr>
<tr>
<td>About This Guide</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>Documentation Set</td>
<td>7</td>
</tr>
<tr>
<td>Chapter Descriptions</td>
<td>7</td>
</tr>
<tr>
<td>Notational Conventions</td>
<td>8</td>
</tr>
<tr>
<td>Service Information</td>
<td>8</td>
</tr>
<tr>
<td>Provide Documentation Feedback</td>
<td>8</td>
</tr>
<tr>
<td>Overview</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>9</td>
</tr>
<tr>
<td>Audio Interworking</td>
<td>10</td>
</tr>
<tr>
<td>PTT Express</td>
<td>10</td>
</tr>
<tr>
<td>LMR</td>
<td>10</td>
</tr>
<tr>
<td>PTT Pro Audio</td>
<td>11</td>
</tr>
<tr>
<td>Announcer API</td>
<td>12</td>
</tr>
<tr>
<td>Mapping Audio Endpoints</td>
<td>13</td>
</tr>
<tr>
<td>Endpoint Priority</td>
<td>14</td>
</tr>
<tr>
<td>Text Interworking</td>
<td>14</td>
</tr>
<tr>
<td>PTT Pro Text</td>
<td>14</td>
</tr>
<tr>
<td>Messenger API</td>
<td>15</td>
</tr>
<tr>
<td>Message of the Day (MOTD)</td>
<td>16</td>
</tr>
<tr>
<td>Licensing</td>
<td>17</td>
</tr>
<tr>
<td>Installation and Upgrade</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>18</td>
</tr>
<tr>
<td>Requirements</td>
<td>18</td>
</tr>
<tr>
<td>Installing the IWG Virtual Machine</td>
<td>18</td>
</tr>
<tr>
<td>Restarting the IWG</td>
<td>19</td>
</tr>
</tbody>
</table>
# Table of Contents

Activating the IWG ................................................................. 19  
Activating the IWG Using a Configuration File ................................. 19  
Activating the IWG Using the IWG Management Portal ......................... 21  
Updating the IWG .................................................................. 23  
Check for New Version Online ................................................... 23  
Install Version from File ............................................................ 23  
Change Version to Older Version ................................................... 24  
Uninstall Version .................................................................. 25

## Configuration

*Introduction* ........................................................................... 26  
*Configuring the IWG* .......................................................... 26  
IWG Management Portal - Graphical User Interface ......................... 27  
IWG Management Portal - Import Configuration File ..................... 28  
IWG Service Menu - Configuration Options ..................................... 28  
Install New Certificate .................................................................. 29  
Static Configuration File Change ................................................... 30  
Dynamic Configuration File Change ............................................... 31  
Start Stop Restart ................................................................... 32  
Pull Logs .................................................................................... 32  
Change Audio Video Repository Time for Keeping Files .................. 33  
*Configuration File Types* ....................................................... 34  
Dynamic Configuration ................................................................ 34  
Static Configuration .................................................................. 34  
Dynamic and Static Configuration Files ......................................... 34  
Configuration File Parameters .................................................... 35

## Using the IWG Management portal

*Introduction* ........................................................................... 37  
IWG Management Portal ........................................................... 37  
Endpoints .................................................................................... 38  
Endpoint Types ......................................................................... 41  
PTT.Express Endpoint .................................................................. 41  
Announcer Endpoint ................................................................... 41  
Messenger Endpoint ................................................................... 43  
LMR Endpoint ............................................................................ 44  
PTT Pro Endpoints ....................................................................... 45  
Content Sharing .......................................................................... 49  
Call Log ...................................................................................... 49  
Media ......................................................................................... 50  
License ......................................................................................... 51  
Releasing Licenses ...................................................................... 52  
Adding Activation Codes .............................................................. 52  
Administration ............................................................................ 53  
System Log .................................................................................. 54

## Configuration Examples

*Introduction* ........................................................................... 55
### Management Portal Examples
- Connect PTT Express and LMR ................................................................. 55
- Connect PTT Express and Announcer .......................................................... 55
- Static Configuration Example ...................................................................... 56
- Dynamic Configuration Example ............................................................... 56

### IP Gateway Configuration
- IP Gateway Configuration ........................................................................... 58

### Main Utility Menu
- Introduction ................................................................................................. 59
- Change Hostname ......................................................................................... 60
- Change IP Address ....................................................................................... 60
- Change Date and Time .................................................................................. 61
- System Check ............................................................................................... 61
- System Configuration .................................................................................... 62
- System Firewall ............................................................................................ 62
- IWG Service Menu ........................................................................................ 63
- Change Admin Password .............................................................................. 63
  - Password Policy ......................................................................................... 64
- Shutdown or Reboot System ........................................................................... 64
About This Guide

Introduction

This guide provides information about how to install, activate, and operate the Zebra Workforce Connect Interworking Gateway. The administrator should be familiar with Linux and virtual machine operation.

✓ NOTE: Screens and windows pictured in this guide are samples and can differ from actual screens.

Documentation Set

The documentation set for the device is divided into guides that provide information for specific user needs.

- **Administration Guide** - describes how to install, activate, and operate the Interworking Gateway.
- **Announcer REST API Developer’s Guide** - describes how to send an audio file to the WFC Announcer using the WFC Announcer REST API.
- **Messenger REST API Developer’s Guide** - describes how to send text messages to the Workforce Connect Messenger (WFC Messenger) using the WFC Messenger REST API.

Chapter Descriptions

Topics covered in this guide are as follows:

- **Installation and Upgrade**, describes steps you need to install and upgrade the Zebra Workforce Connect Interworking Gateway (IWG).
- **Configuration**, explains how to configure the Zebra Workforce Connect Interworking Gateway (IWG).
- **Using the IWG Management portal**, explains how to use the Zebra Workforce Connect Interworking Gateway (IWG).
- **Configuration Examples**, provides an example of an IWG configuration file.
- **IP Gateway Configuration**, detailed information on the LMR gateway and configuration.
- **Main Utility Menu**, explains how to use the virtual machine Main Service Menu.
Notational Conventions

The following conventions are used in this document:

- **Bold** text is used to highlight the following:
  - Dialog box, window and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - Icons on a screen
  - Key names on a keypad
  - Button names on a screen.

- Bullets (*) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps that are not necessarily sequential.

- Sequential lists (e.g., 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: [www.zebra.com/support](http://www.zebra.com/support).

When contacting support, please have the following information available:

- Licensing information
- Software version.

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.

Provide Documentation Feedback

If you have comments, questions, or suggestions about this guide, send an email to EVM-Techdocs@zebra.com.
Introduction

The Zebra Workforce Connect Interworking Gateway provides interworking among the following services, allowing connectivity between work groups using different communication products.

- **PTT Express** - A server-less Push-to-Talk service supporting 32 channels.
- **PTT Pro Audio** - A server-based Push-to-Talk service supporting individual and group audio communications.
- **PTT Pro Text** - A server-based Push-to-Talk service supporting individual and group text communications.
- **Land Mobile Radio (LMR)** - A server-less wireless communication system using dedicated radio devices.

**Figure 1** PTT Technologies Interworking

The IWG also supports interworking via APIs:

- **Announcer API** - A service allowing third party applications to submit audio files for broadcasting to selected destinations via the published API.
- **Messenger API** - A service allowing third party applications to submit text messages to specific PTT Pro individuals or groups via the published API. The Messenger API also allows administrators to upload audio or video content to the IWG and send the URL for the content to specific PTT Pro individuals or groups.
Audio Interworking

Audio interworking requires that audio services are defined as endpoints on the IWG. The PTT Express, LMR, and PTT Pro endpoints can be mapped to other endpoints, enabling communications between them. See Mapping Audio Endpoints on page 13.

PTT Express

PTT Express supports 32 multi-cast channels on a single multi-cast IP address. When a PTT Express channel is defined in the IWG as a PTT Express endpoint, the IWG can broadcast and listen to that PTT Express channel. Mapping other endpoints to a PTT Express endpoint allows the IWG to send audio between the PTT Express channel and other endpoints mapped to the PTT Express endpoint.

PTT Express endpoints follow the defined PTT Express protocol for handling conflict resolution. See Endpoint Priority on page 14.

LMR

Land mobile radios are two-way radios which broadcast on radio frequencies reserved for this purpose. The radios in an enterprise are tuned to a specific two-way radio channel so that the necessary workgroups can communicate.

In order for the IWG to communicate with LMR two-way radios, additional equipment is required.

- An IP Gateway - the IP Gateway converts signals between analog audio on the LMRs to digital packetized audio on an IP network, and vice versa.
- An LMR Donor Radio - Interfaces between the IP Gateway and the 2-way radio channel.
The IWG routes audio between the IP Gateway and any other endpoints mapped to the LMR endpoint. The IWG uses RTP to communicate with the IP Gateway.

When adding an LMR endpoint in the IWG, specify the remote IP address, port of the IP Gateway, and the port of the IWG. The IP Gateway also needs to be configured with the remote IP address and port of the IWG.

**PTT Pro Audio**

PTT Pro is a Push To Talk system supporting group and individual communications for both audio and text messaging. It supports several advanced features including late join and priority override. PTT Pro is supported via an app on the end user device which communicates with server infrastructure.

The PTT Pro Audio endpoint is only valid for audio communications. To use text, add a PTT Pro Text endpoint. If one PTT Pro destination user or group needs to communicate via both text and audio, add that user/group twice – once as a PTT Pro Audio endpoint, and once as a PTT Pro Text endpoint.

In order to reach a PTT Pro user, the IWG must also communicate with the PTT Pro server. In order to do that, the IWG uses a proxy user, or a proxy client.

Proxy clients must be configured in PTT Pro as users, and have an associated PTT Pro user client running on the IWG.

The PTT Pro server is not aware that the proxy client is not being used as a normal PTT Pro user. The proxy client acts like any other PTT Pro user, but instead of running on a device, it runs on the IWG and forwards communications between the PTT Pro server and any other endpoints mapped to the PTT Pro endpoint.

In the below example, the enterprise owner desires to connect the PTT Pro group Hardware to other IWG endpoints (for example, a PTT Express group).

To enable this example, the following steps are followed:

1. A PTT Pro user called Hardware_proxy is added to the PTT Pro server.
2. Hardware_proxy is added to the group Hardware in the PTT Pro server.
3. A PTT Pro Audio endpoint called PTT_Pro_Hardware is added to the IWG, specifying the Hardware group as the target PTT Pro user/group, and the PTT Pro user Hardware_proxy as the proxy client.

As a result of adding Hardware_proxy as the proxy client, the IWG registers with the PTT Pro server as the user Hardware_proxy. It will also verify that the Hardware group exists, and if not, flag an error.
After this setup, whenever the PTT Pro group Hardware starts a group call, the PTT Pro server will include the user Hardware_proxy and route control and audio to the IWG. The IWG forwards the communication to any other endpoints mapped to this PTT Pro Audio endpoint.

Note that when communication is forwarded from other IWG endpoints to the Hardware group, the speaker will be identified by the name of proxy – in our example, this is Hardware_proxy.

Once Hardware_proxy has been associated with the PTT Pro Audio endpoint Hardware, it may not be associated with any other PTT Pro Audio endpoint in the IWG. A separate proxy client must be used for each PTT Pro Audio endpoint.

PTT Pro audio endpoints are licensed in the IWG. The PTT Pro Proxy users are NOT licensed in the IWG; however, since they appear as normal users to the PTT Pro system, each proxy user consumes a PTT Pro user license when it is configured in the PTT Pro system.

**Announcer API**

The Announcer endpoint and associated Announcer REST APIs allow audio messages to be submitted to the IWG, along with the target endpoints. The audio message is processed and immediately broadcast to whichever of the target endpoints are available. Endpoints which are not available at the time of the broadcast do not receive the message.

There are two Announcer APIs supported by the IWG:

- Legacy RLS Announcer - This interface is supported by the RLS product and allows legacy applications to use the IWG as an RLS replacement. Use port 8111.
- IWG Announcer - An updated interface which adds enhanced security and the ability to reach additional endpoints, such as PTT Pro. The default port is 443.

Add multiple Announcer endpoints to allow the processing of multiple announcements simultaneously. An Announcer endpoint can process either the Legacy RLS Announcer or the IWG Announcer.

Below is a diagram of the system architecture for the announcer.

Mapping is not required for the Announcer endpoint, since the target endpoints are specified in the audio message submission.
Mapping Audio Endpoints

To enable communication between audio endpoints, the connection between the endpoints must be mapped. Each mapping allows audio to be transferred in one direction. To allow audio to transfer in either direction, both endpoints must be mapped to each other. For example, to allow audio to go in either direction between a PTT Pro Audio endpoint and a PTT Express endpoint, map from the PTT Pro Audio endpoint to the PTT Express endpoint, and then from the PTT Express endpoint to the PTT Pro Audio endpoint.
Map between more than two endpoints by daisy chaining them (endpoint 1 > endpoint 2 > endpoint 3) or by mapping an endpoint to two or more endpoints. For example, to share audio between an LMR channel, a PTT Express channel, and a PTT Pro group, you can map the LMR channel to the PTT Express channel and the PTT Pro group (daisy chain) or map the LMR channel to the PTT Express channel and PTT Pro group independently. In either case, all 3 endpoints will be connected.

**Endpoint Priority**

The IWG obeys the contention rules of each technology as it interworks between them. Some of the rules are as follows:

- In PTT Express, priority during contention is given to the device with the higher IP address. If the IWG has a lower IP address than other devices on the PTT Express channel, it will not have priority, and in case of contention, will drop audio destined to the PTT Express channel.
- In LMR, a speaker may not be interrupted. If the IWG detects incoming audio from an LMR channel, it will not send audio destined for the LMR channel.
- PTT Pro has call override and talk override features. The priority of each device for these features is provisioned in the PTT Pro system. The IWG will behave according to the provisioning in place for the PROXY USER it is using.

---

**Text Interworking**

PTT Pro users can text each other using the PTT Pro application. The IWG supports origination of text messages via an API instead of via the PTT Pro application. This allows external applications to originate PTT Pro text messages.

At this point in time, text interworking is only supported from external applications TO the PTT Pro Text endpoint. Text messaging in the reverse direction is not supported.

Mapping is not required for text interworking.

**PTT Pro Text**

The PTT Pro Text endpoint is very similar to the PTT Pro Audio endpoint, but it is only used to transport text messages from the Messenger to the destination PTT Pro user or group.

A PTT Pro Text endpoint also requires a proxy client; however, unlike audio, the proxy client does not have to be unique to the PTT Pro Text endpoint. A proxy client may only be used for a SINGLE PTT Pro Audio endpoint, but it may be used for many PTT Pro Text endpoints.

In the below example, the enterprise owner desires for the PTT Pro groups Hardware”, Warehouse”, and Electrical” to be able to receive text messages from the Messenger (described in a following section). The same proxy client will be used for all 3 PTT Pro Text endpoints.
To enable this example, the following steps are followed:

1. A PTT Pro user called Text_Proxy” is added to the PTT Pro server.
2. Text_Proxy” is added to the groups Hardware”, Warehouse”, and Electrical” in the PTT Pro server.
3. A PTT Pro Text endpoint called PTT_Pro_Hardware” is added to the IWG, specifying the Hardware” group as the target PTT Pro user/group, and the PTT Pro user Text_proxy” as the proxy client.
4. A PTT Pro Text endpoint called PTT_Pro_Warehouse” is added to the IWG, specifying the Warehouse” group as the target PTT Pro user/group, and the PTT Pro user Text_proxy” as the proxy client.
5. A PTT Pro Text endpoint called PTT_Pro_Electrical” is added to the IWG, specifying the Electrical” group as the target PTT Pro user/group, and the PTT Pro user Text_proxy” as the proxy client.

As a result of adding Text_proxy” as the proxy client, the IWG registers with the PTT Pro server as the user Text_proxy”. As each endpoint is added, the IWG will also check to make sure the Hardware”, Warehouse”, and Electrical” groups exist; otherwise, it will flag an error.

After this setup, if messages are targeted to a specific PTT Pro Text endpoint, the IWG will use the proxy to send the text message to the targeted PTT Pro Text user/group. The originator of the text message will be the Text_proxy”.

PTT Pro audio endpoints are licensed in the IWG. The PTT Pro Proxy users are NOT licensed in the IWG; however, since they appear as normal users to the PTT Pro system, each proxy user consumes a PTT Pro user license when it is configured in the PTT Pro system.

**Messenger API**

The Messenger endpoint and associated Messenger REST API allows text messages to be submitted to the IWG, along with target PTT Pro Text endpoints. The audio text is processed and sent to the target PTT Pro Text endpoints. The PTT Pro system has the capability to store text messages; target endpoints which are not immediately available will see the text message when they become active again in PTT Pro.

Multiple Messenger endpoints may be added, which allows processing of multiple messages simultaneously.
Message of the Day (MOTD)

Message of the Day (MOTD) is a special use case of the Messenger endpoint. This is also sometimes referred to as streaming.

MOTD can be used in 2 ways:

1. **Direct MOTD**: Some versions of the PTT Pro client support MOTD. The PTT Pro client allows the user to record audio or video content and specify one or more PTT Pro recipients. The client will upload the content to the IWG, receive a URL in return, and then send the URL directly to the designated recipients via PTT Pro text. The IWG is not involved in sending any PTT Pro text messages when Direct MOTD is used.

2. **IWG-based MOTD**: An external application can upload audio or video content to the IWG and specify one or more PTT Pro recipients. The IWG will send the URL of the content to the designated recipients via PTT Pro text. Since the IWG is sending the PTT Pro text, the recipients must be configured as PTT Pro text endpoints in the IWG.

After the recipients receive the PTT Pro Text message with the URL, the user(s) may click on the URL to initiate file download and view the content.
Licensing

When a customer purchases a subscription license for the IWG, they receive the WFC IWG Base System Package, which includes:

- The software rights for the IWG
- 32 PTT Express resources / endpoints
- 32 LMR resources / endpoints
- 8 Announcer resources / endpoints
- 8 Messenger resources / endpoints

**NOTE:** The contents of the WFC IWG Base System Package are subject to change.

In addition, the customer may also purchase PTT Pro resources / endpoints:

- The WFC IWG PTT Pro Talk Group Resource provides 1 PTT Pro Audio endpoint in the IWG, as well as a PTT Pro user license for the proxy user.
- The WFC IWG PTT Pro Text Resource provides 1 PTT Pro Text endpoint in the IWG, as well as a PTT Pro user license for the proxy user.

For each product that the customer purchases (i.e. Base System, PTT Pro Talk Group, PTT Pro Text), an Activation ID (AID) will be provided which must be entered in the IWG to activate the licenses. The current status of the licenses (i.e. how many the IWG has available, how many are used, and expiration dates) may be viewed at the Licensing Tab of the IWG Admin Portal.

See the WFC IWG Licensing Guide, which goes into activation IDs and activation in more detail.

When the IWG Admin adds an endpoint, a corresponding license is used. If there are no more licenses available, adding the endpoint will fail.
Installation and Upgrade

Introduction

This chapter describes how to set up and upgrade the IWG.

Requirements

The IWG runs on a virtual machine and requires the following:

- VMware vSphere ESXi 6.0 or greater
- 4 GB memory, 4 processors, and 20 GB hard disk (SCSI)
- A single network connection
- The IWG Virtual Machine OVA file package
- Activation ID(s) provided in software entitlement email.
- Access to a licensing server. Ensure that:
  - TCP port 443 is open on the firewall to enable access
  - TCP port 80 is open for activation (and available for working with DNS)
- which adds TCP and UDP port 53.

To access the IWG Management Portal, use a host computer with one of the following supported web browsers:

- Chrome 63 or higher
- Internet Explorer 11 or higher
- Firefox 44 or higher
- Safari 11 or higher
- Edge 16 or higher

NOTE: Mobile browsers are not supported.

Installing the IWG Virtual Machine

To install the virtual machine:

1. Install VMware vSphere. Refer to www.vmware.com/products/vsphere.html for more information.
2. Start vSphere.
   In vSphere, deploy a virtual machine from the OVA file.
   The virtual machine initializes and the Main Service Menu displays. See Main Utility Menu on page 59 for more information.

### Restarting the IWG

It is not recommended to reset the IWG from the vSphere console. To perform a graceful shutdown and restart of the IWG, use one of the following methods:

- Restart the IWG using the IWG Management Portal. See Administration on page 53.
- Restart the IWG using the Main Utility Menu. See Start Stop Restart on page 32.
- Restart the system using the Main Utility Menu. See Shutdown or Reboot System on page 64.

### Activating the IWG

Before activating the IWG, the virtual machine must be configured to use DHCP or a static IP address. See Change IP Address on page 60.

The following tasks are recommended before activating the IWG:

- Check for IWG updates. See Updating the IWG on page 23.
- Change the hostname for the virtual machine. See Change Hostname on page 60.
- Set a permanent IP address for the virtual machine. See Change IP Address on page 60.

**NOTE:** It is highly recommended to use a permanent IP address, such as a static IP address or DHCP reservation. This allows easy access to the IWG Management Portal, and predictable addresses for use in the Announcer and Messenger APIs.

- Set the date and time for the virtual machine. See Change Date and Time on page 61.

**NOTE:** If the time zone is changed, reboot the virtual machine. See Shutdown or Reboot System on page 64.

- Set the administrator password to allow remote access. See Change Admin Password on page 63.

Activate the IWG using one of the following methods:

- Configuration File
- IWG Management Portal

### Activating the IWG Using a Configuration File

1. Create a dynamic or static configuration file. See Configuration File Types on page 34.

2. In the configuration file, enter in the LicenseCodes parameter using the IWG **activation ID(s)**. Multiple activation IDs may be required.
   - To enter multiple activation IDs, separate the codes with a comma. Do not add spaces.
   - To enter a single activation ID multiple times, after the code add a colon and the number of times to retrieve the license. For example, to use an activation ID 10 times, enter `XXXX-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx:10`.

**NOTE:** If the time zone is changed, reboot the virtual machine. See Shutdown or Reboot System on page 64.
3. Enter in the hostAlias parameter using a unique **Host Alias (optional)**.

   ✓ **NOTE:** It is highly recommended to enter a unique Host Alias for each instance of the IWG. The host alias identifies the IWG when communicating with customer support.

4. From the virtual machine Main Service Menu, enter 7 and press **Enter**.

5. From the IWG Service Menu, upload the configuration file using one of the following methods:
   - Static Configuration File Change on page 30
   - Dynamic Configuration File Change on page 31

6. From a web browser, navigate to the IWG Management Portal at the following URL:
   
   \[https://IWG_host:8443/\]

   Where **IWG_host** is the IP address of the host running the IWG instance.

   ✓ **NOTE:** If a warning displays to indicate that the connection is not secure, import a certificate. See Install New Certificate on page 29 for more information.

**Figure 9  Management Portal Login**

7. Enter the Admin Name. The default Admin Name is: admin.

8. Enter the Admin Password. The default Admin Password is: zamboni.

9. Click **Sign In**.

10. Click the **Administration** tab.

11. If the IWG has stopped, click **Start** to start the IWG.

   ✓ **NOTE:** For security, change the login information. See Administration on page 53.
Activating the IWG Using the IWG Management Portal

1. From a web browser, navigate to the IWG Management Portal at the following URL: https://IWG_host:port/gw
   Where IWG_host is the IP address of the host running the IWG instance.

   ✓ NOTE: If a warning displays to indicate that the connection is not secure, import a certificate. See Install New Certificate on page 29 for more information.

   Figure 10  Management Portal Login

2. Enter the Admin Name. The default Admin Name is: admin.
3. Enter the Admin Password. The default Admin Password is: zamboni.
4. Click Sign In.
5. On the activation screen, enter the IWG **activation ID(s)**. Multiple activation IDs may be required. See Adding Activation Codes on page 52.
   - To enter multiple activation IDs, separate the codes with a comma. Do not add spaces.
   - To enter a single activation ID multiple times, after the code add a colon and the number of times to retrieve the license. For example, to use an activation ID 10 times, enter `XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX:10`.

6. Enter a unique **Host Alias (optional)**.

   ✓ **NOTE:** It is highly recommended to enter a unique Host Alias for each instance of the IWG. The host alias identifies the IWG when communicating with customer support.

7. Click **Activate code(s)**.

8. Click the **Administration** tab.

9. If the IWG has stopped, click **Start** to start the IWG.

   ✓ **NOTE:** For security, change the login information. See Administration on page 53.
Updating the IWG

Use the IWG Service Menu to update or uninstall the IWG.

To access the IWG Service Menu from the virtual machine Main Service Menu, enter 7 and press Enter. See Main Utility Menu on page 59 for more information.

**Figure 12** IWG Service Menu

Use the IWG Service Menu to:

- View the current IWG version number
- Check for updates
- Update from a file
- Change the version
- Uninstall.

To choose a menu option, enter the option number and press Enter.

To exit a menu, enter 0 and press Enter.

**Check for New Version Online**

Use the Check for New Version Online option to check for new versions of the IWG software. Online updates are used to apply bug fixes and security updates.

**NOTE:** The Check for New Version Online menu option may not be available on some versions of the IWG software.

**Install Version from File**

**NOTE:** An SFTP client, such as Filezilla, is required.

Use the Install Version from File option to update to a new version, or reinstall the IWG software using an RPM file. A notification is sent by email when a new RPM file is available.
To update using an RPM file:

1. From the IWG Service Menu, choose option 2.

**Figure 13** Install from File

2. Write down the SFTP password that displays. For security, a new password is generated upon each SFTP connection.

3. Open an SFTP client, such as Filezilla.

4. Enter the hostname. For example: sftp://192.168.1.125.

5. Enter the username: iwgsftp.

6. Enter the password from step 2.

7. Connect to the remote site.

8. Change the remote site directory to sftpdata.

9. Transfer the file from the host computer to the virtual machine sftpdata directory.

10. From the virtual machine IWG Service Menu, press Enter.

11. To confirm the installation of the new version, enter 1 and press Enter.

When the update is complete, the IWG software restarts.

**Change Version to Older Version**

Use the Change Version to Older Version option to revert the IWG software to a previous version.

1. From the IWG Service Menu, choose option 3.

**Figure 14** Change the IWG Version

2. Enter 1 and press Enter to continue with the downgrade.

3. Choose an option:
   - To choose the currently displayed version, enter 1 and press Enter.
   - To view the next available software version, enter 2 and press Enter.
Figure 15  Choose the IWG Version

When the downgrade is complete, the IWG software restarts.

Uninstall Version

Use the Uninstall Version option to uninstall the IWG.

1. From the IWG Service Menu, choose option 4.
2. Enter 1 and press Enter to confirm removal of the IWG software from the virtual machine.

Figure 16  Uninstall the IWG

To reinstall the IWG select option 7 from the Main Service Menu. See Install Version from File on page 23 to install the IWG software using an RPM file.
Configuration

Introduction

This chapter explains how to configure the Zebra Workforce Connect Interworking Gateway (IWG).

**IMPORTANT:** Using interworking services requires a mapping between at least two licensed and configured endpoints. For more information, see Using the IWG Management portal on page 37.

**IMPORTANT:** It is highly recommended to release licenses before making physical changes to the platform or using a configuration file to modify activation IDs. To release licenses using the IWG Management portal, see Releasing Licenses on page 52. To release licenses using the configuration file, see Configuration File Parameters on page 35.

If licenses are not properly released and become unusable, contact Zebra support and have your Host ID, Alias, and activation ID available.

Configuring the IWG

Configure the IWG using the following methods:

- Using the IWG Management Portal Graphical User Interface.
- Using the IWG Management Portal to import a configuration file.
- Using the virtual machine IWG Service Menu configuration options.
Use the IWG management portal to:

- Configure endpoints
- Create mappings
- Modify licensing
- Perform administrative actions
- View call log
- View system log.

For more information on the management portal and available configuration actions, see Using the IWG Management portal on page 37.
To import an XML configuration file through the IWG Management Portal:

1. Click the Administration tab in the IWG Management Portal.
2. Click Import Config.
3. On the pop-up dialog click Choose File and navigate to the new static or dynamic configuration file.
4. Click Open.
5. Click Apply.

When configuration is complete, the IWG restarts. For more information on the Administration tab, see Administration on page 53.

For an example of the format for the XML configuration file, see Configuration Examples.

IWG Service Menu - Configuration Options

Use the virtual machine IWG Service Menu to configure the IWG.

To access the IWG Service Menu from the virtual machine Main Service Menu, enter 7 and press Enter. See Main Utility Menu for more information.
Use the IWG Service Menu to:

- Install a certificate
- Change the static configuration file
- Change the dynamic configuration file change
- Start, stop, and restart the IWG
- Pull logs
- Change Audio Video Repository Time for Keeping Files.

To choose a menu option, enter the option number and press Enter.

To exit a menu, enter 0 and press Enter.

**Install New Certificate**

Use the **Install New Certificate** option to install a certificate on the IWG.

✓ **NOTE:** A certificate is required to use the Messenger endpoint.

1. From the IWG Service Menu, choose option 5.

**Figure 20  Install from File**

2. Write down the SFTP password that displays. For security, a new password is generated upon each SFTP connection.

3. Open an SFTP client, such as Filezilla.
4. Enter the hostname. For example: sftp://192.168.1.125.
5. Enter the username: iwgsftp.
6. Enter the password from step 2.
7. Connect to the remote site.
8. Change the remote site directory to sftpdata.
9. Transfer the file from the host computer to the virtual machine sftpdata directory.

Figure 21  Install from File

10. From the virtual machine IWG Service Menu, press Enter.
11. To confirm the installation of the new certificate, enter 1 and press Enter.

Figure 22  Certificate Installed

When the certificate installation is complete, the IWG static configuration file is automatically updated and the IWG software restarts.

Static Configuration File Change

Use the Static Configuration File Change option to update the static configuration file. See Static Configuration on page 34 for more information.

1. From the IWG Service Menu, choose option 6.

Figure 23  Install from File

2. Write down the SFTP password that displays. For security, a new password is generated upon each SFTP connection.
3. Open an SFTP client, such as Filezilla.
4. Enter the hostname. For example: sftp://192.168.1.125.
5. Enter the username: iwgsftp.
6. Enter the password from step 2.
7. Connect to the remote site.
8. Change the remote site directory to sftpdata.
9. Transfer the file from the host computer to the virtual machine sftpdata directory.
10. From the virtual machine IWG Service Menu, press Enter.
11. To confirm the installation of the new static configuration file, enter 1 and press Enter.
12. If prompted, press Enter again.

The location of the backup configuration file displays.

**Figure 24  Configuration File Installed**

```
New file to install is Iwg.conf.txt
Do you want to install this file? 1 for yes 2 for no 3 for exit: 1
The file will be installed
backup of file was move to /home/iwgftp/backupfiles/
Shutting down:
Iwg is Running: 1003
Stopping Iwg (via systemctl): [ OK ]
Iwg is now stopped
Starting Iwg up:
Starting Iwg (via systemctl): [ OK ]
Iwg has started: 11233
Press [Enter] key to continue...
```

When the configuration file update is complete, the IWG restarts.

**Dynamic Configuration File Change**

Use the Dynamic Configuration File Change option to update the dynamic configuration file. See Dynamic Configuration on page 34.

1. From the IWG Service Menu, choose option 7.

**Figure 25  Install from File**

```
Directions:
1.) Open up a client such as Filezilla
2.) SFTP://192.168.8.12
3.) Username is WFConnect
4.) Password is 121810233
5.) Change directories to sftpdata.
6.) When file transfer is complete then please press enter to continue.
Press [Enter] key to continue...
```

2. Write down the SFTP password that displays. For security, a new password is generated upon each SFTP connection.
3. Open an SFTP client, such as Filezilla.
4. Enter the hostname. For example: sftp://192.168.8.12.
5. Enter the username:WFConnect.
6. Enter the password from step 2.
7. Connect to the remote site.
8. Change the remote site directory to sftpdata.
9. Transfer the file from the host computer to the virtual machine sftpdata directory.
10. From the virtual machine IWG Service Menu, press Enter.
11. To confirm the installation of the new dynamic configuration file, enter 1 and press Enter.
12. If prompted, press Enter again.
   The location of the backup configuration file displays. When the configuration file update is complete, the IWG restarts.

**Start Stop Restart**

✓ NOTE: To start, stop, or restart all endpoints configured on the IWG, see Administration on page 53.
   The IWG stop option in the IWG Service Menu shuts down the IWG, making the IWG Management Portal unavailable.

Use the Start Stop Restart option to start, stop, or restart the IWG. Available options depend on the current IWG status.
1. From the IWG Service Menu, choose option 8.
2. Choose an option:
   • If the IWG is running, press 1 to restart the IWG or press 2 to stop the IWG.

![Figure 26 IWG Restart or Stop](image)

   • If the IWG is stopped, press 3 to start the IWG.

![Figure 27 IWG Start](image)

**Pull Logs**

Use the Pull Logs option to pull system logs from the IWG. To view system logs using the IWG from the Management Portal, see System Log on page 54.
1. From the IWG Service Menu, choose option 9.
2. Write down the SFTP password that displays. For security, a new password is generated upon each SFTP connection.

3. Open an SFTP client, such as Filezilla.

4. Enter the hostname. For example: sftp://192.168.8.12.

5. Enter the username: iwgsftp.

6. Enter the password from step 2.

7. Connect to the remote site.

8. Change the remote site directory to sftpdata.

9. Transfer the file from the virtual machine sftpdata directory to the host computer.

10. From the virtual machine IWG Service Menu, press Enter.

Change Audio Video Repository Time for Keeping Files

Use the Change Audio Video Repository Time for Keeping Files option to set the number of days that the IWG stores media files uploaded to a local file repository.

1. From the IWG Service Menu, choose option 10.

2. From the Change Audio Video Repository Time for Keeping Files menu choose option 1 and press Enter.

3. Enter the number of days to keep media files in the IWG repository.
Configuration File Types

Use configuration files to make static or dynamic changes to the IWG configuration.

Dynamic Configuration

The IWG checks for an XML configuration file at start-up and while running. To make changes to the IWG configuration, create a temporary configuration file to `push.xml` and save it to `/root/.IWG`. Parameters in the `push.xml` file replace values set in the `IWG.xml` file for each IWG. When the IWG detects this file, it loads the configuration information in the file and restarts. When the update is complete, the IWG deletes the XML configuration file.

For an example of the format for the XML configuration file, see Configuration Examples on page 55.

Static Configuration

The static configuration file cannot contain endpoint information. To configure endpoints, use the dynamic configuration file.

The IWG supports static definition parameters that override dynamic parameters when the IWG starts or restarts. Static parameters allow each IWG to define a separate set of parameters, while multiple IWGs share common parameters using one dynamic configuration file.

To make changes to the IWG configuration using static configuration, save static parameters in a `key=value` format to `IWG.conf` and save it to `/root/.IWG`. Parameters in the `IWG.conf` file replace values set in the `IWG.xml` file for each IWG. When the update is complete, the IWG does not delete the static configuration file.

For an example of the format for the dynamic configuration file, see Configuration Examples on page 55.

Dynamic and Static Configuration Files

The dynamic `push.xml` configuration file can contain any valid IWG configuration parameters. The static `IWG.conf` configuration file can only contain the subset of parameters which are listed in table 2. These parameters affect the IWG globally. The static configuration can not contain endpoint specific configuration.

The following table shows how these files interact. The default value is used when a parameter is not defined in either file, or if no configuration files are present.

<table>
<thead>
<tr>
<th>Dynamic File</th>
<th>Static File</th>
<th>IWG Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>none</td>
<td>Initializes with no configuration information.</td>
</tr>
<tr>
<td>push.xml</td>
<td>none</td>
<td>Initializes with <code>push.xml</code> configuration information, and then deletes the file.</td>
</tr>
<tr>
<td>none</td>
<td>IWG.conf</td>
<td>Initializes with <code>IWG.conf</code> and does not delete the file.</td>
</tr>
<tr>
<td>push.xml</td>
<td>IWG.conf</td>
<td>The dynamic configuration information is imported from <code>push.xml</code>. The static information is imported from <code>IWG.conf</code>. If parameters are present in both files, the <code>IWG.conf</code> information replaces the <code>push.xml</code> information. When the update is complete, only the <code>push.xml</code> file is deleted.</td>
</tr>
</tbody>
</table>
## Configuration File Parameters

Table 2 lists common configuration parameters for the IWG.conf and IWG.xml files.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostIp</td>
<td>Value automatically</td>
<td>Primary host address the IWG uses to identify the network interface</td>
</tr>
<tr>
<td></td>
<td>detected during initial</td>
<td>utilized by some endpoints and services. If the host has multiple</td>
</tr>
<tr>
<td></td>
<td>configuration.</td>
<td>interfaces, manually set this to the correct value.</td>
</tr>
<tr>
<td>httpPort</td>
<td>8080</td>
<td>HTTP listening port for the management portal.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On production builds, the HTTP port is restricted to local interface.</td>
</tr>
<tr>
<td>httpsPort</td>
<td>8443</td>
<td>HTTPS listening port for the management portal.</td>
</tr>
<tr>
<td>enabled</td>
<td>true</td>
<td>Initial state of the IWG on start or restart. If set to false, the IWG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>initializes in the stop state and must be started or restarted. For more</td>
</tr>
<tr>
<td></td>
<td></td>
<td>information, see Administration on page 53.</td>
</tr>
<tr>
<td>logLevel</td>
<td>1</td>
<td>The IWG main log level:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0 - OFF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 - SEVERE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 - WARNING</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3 - INFO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 4 - FINE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 5 - FINER</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 6 - FINEST</td>
</tr>
<tr>
<td>hostAlias</td>
<td>Value set by administrator.</td>
<td>Identifies the host on the license server. Set by the administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>during activation of the IWG.</td>
</tr>
<tr>
<td>keystore</td>
<td>File name of the</td>
<td>Certificate the IWG uses for HTTPS connections. Import the certificate</td>
</tr>
<tr>
<td></td>
<td>certificate the IWG uses</td>
<td>into the IWG using the IWG Utility. See Install New Certificate on page 29.</td>
</tr>
<tr>
<td></td>
<td>for HTTPS connections.</td>
<td></td>
</tr>
<tr>
<td>keystore_pass</td>
<td>The password for the keystore file.</td>
<td></td>
</tr>
<tr>
<td>licenseServer</td>
<td><a href="https://zebrauat.flex">https://zebrauat.flex</a></td>
<td>The URL of the Flexera back office or local license sever.</td>
</tr>
<tr>
<td></td>
<td>netoperations.com/</td>
<td></td>
</tr>
<tr>
<td></td>
<td>control/mtzb/device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>services</td>
<td></td>
</tr>
</tbody>
</table>
### Table 2  Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>releaseCodes</td>
<td></td>
<td>Release all licenses for one or more activation IDs. Remove the activation ID(s) from the licenseCodes parameter and then define the releaseCodes parameter before the licenseCodes parameter. Multiple activation IDs are comma separated. The releaseCodes parameter releases all licenses associated with an activation ID. To increase or decrease how many licenses are associated with an activation ID, modify the licenseCodes parameter.</td>
</tr>
<tr>
<td>licenseCodes</td>
<td></td>
<td>Add or modify one or more activation IDs. Multiple activation IDs are comma separated. To enter a single activation ID multiple times, add a colon after the code followed by the number of times to activate the license. For example, to release an activation ID 10 times, enter: XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX:10 To increase or decrease how many licenses are associated with an activation ID, change the number after the colon. Note: When you activate a license code, releasing the license requires that you remove it from the licenseCodes parameter and add it to the releaseCodes parameter.</td>
</tr>
</tbody>
</table>
Using the IWG Management portal

Introduction

The IWG provides a Graphical User Interface (GUI) allowing the administrator to enable interworking between services by:

• Managing **endpoints**. The IWG supports several types of endpoints: PTT Express channels, PTT Pro channels, LMR channels, and the Announcer. Endpoints are specific instances of an endpoint type (i.e. PTT Express channel 1 or LMR channel 3). Endpoints are the source and destination of audio.

• Managing **mappings** which define how audio is routed between endpoints.

✓ **NOTE:** In the IWG Management Portal, activation IDs are referred to as activation codes.

IWG Management Portal

Use the IWG management portal to add endpoints, map between endpoints, modify licensing information, perform administrative actions, and display logs. The management portal is divided into the following tabs:

• **Endpoints** on page 38
• **Call Log** on page 49
• **Media** on page 50
• **License** on page 51
• **Administration** on page 53
• **System Log** on page 54
Endpoints

Use the Endpoints tab to add endpoints/resources and connect them by specifying mapping rules. The left side of the Endpoints tab displays a list of all available endpoint types. Endpoint types that are not licensed appear in gray below the horizontal line.

To add an endpoint, on the left side click on a licensed endpoint type. A dialog box appears that is unique for each endpoint type. For detailed information on adding endpoints, see Endpoint Types on page 41.

✓ **NOTE:** Endpoints may also be referred to as resources. For example, the PttPro Audio endpoint may also be referred to as the PttPro Audio resource. Resources display as licensed endpoints on the License tab, and are configured as endpoints on the Endpoints tab.

The right side of the Endpoints tab displays all running endpoints. Use the Filter field to filter the list of endpoints by type, name, or information.

Figure 30  Endpoints Tab

- **EID** - A unique ID of the endpoint. The IWG automatically assigns an EID to a new endpoint when it is added via the IWG management portal. An administrator assigns custom EID values by modifying the setting the values in the XML configuration file. For information on importing or pushing the configuration file, see Configuration on page 26. The EID value can be any string but must be unique within each IWG. Note that the EID is used when assigning mappings in the mapping field of the endpoint.
• **Type** - The endpoint type. Icons identify the type.
  - Announcer
  - Messenger
  - Ptt-Express
  - PttPro Audio
  - PttPro Text
  - LMR

• **NAME** - The endpoint display name. Set when a new endpoint is added. The default name is the type of endpoint plus a main parameter, such as a channel number. For example, the default name for Ptt-Express on channel four is Ptt-Express(4).

• **MAPPING** - Defines how endpoints are connected. For example, in Figure 30, audio transmitted on the PTT Express Hardware channel (the originating endpoint), is forwarded to the LMR Loading channel (the target endpoint), since the Hardware endpoint is mapped to the Loading endpoint. Click the **Mapping** field of an endpoint to modify the mapping for that endpoint.

  Each mapping can have a FOLLOW flag which forces IWG to add all mappings assigned to the target endpoint to incoming communications from the originating endpoint.

**NOTE:** The Announcer sends audio to the endpoints specified in the incoming Announcer request and cannot be mapped to other endpoints. The FOLLOW flag does not apply to audio originating from the Announcer.

• **MODE** - An icon defines the audio mode for the endpoint. This is updated in real-time.
  - Idle
  - Sending
  - Receiving

• **STATE** - The state of the endpoint is shown as a colored icon:
  - red - DOWN
  - blue - REGISTERING
  - green - UP
  - orange - IN_CALL.

  The endpoint is receiving/sending audio or in the active session. This depends on endpoint type. This is updated in real-time.

• **LOG LEVEL** - The log level of the endpoint. The logging level for each endpoint can fine tuned (OFF, SEVERE, WARNING, INFO, FINE, FINER, FINEST). ALARM is the lowest log level.

  The system-wide IWG log level, set on the System Log tab, overrides the endpoint's individual log level set on this page.

• **PARAMS** - Displays various parameters based on the endpoint type. For information on endpoint types, see **Endpoint Types on page 41**.
• **Actions** - Buttons used to perform actions on the endpoint:
  
  • [edit]
  • [delete]
  • [pause/resume]
  • [restart]

  Other actions are based on the endpoint type. For example, the Announcer includes an action to send an announcement from the management portal.
Endpoint Types

This section describes the available endpoint types and how to add endpoint instances to the IWG for each endpoint type.

PTT.Express Endpoint

The PTT.Express endpoint connects other communication types (LMR, for example) to a PTT Express channel. Each PTT.Express endpoint is associated with a PTT Express channel at creation.

The IWG routes audio to and from the PTT Express channel as specified by the mapping, allowing audio in both directions.

**IMPORTANT:** The IWG uses the following default base multi-cast address and port for PTT Express: IP address 239.192.2.2 port 5000.

To add a new PTT-Express endpoint:

1. Ensure UDP ports 5000 to 5031 are open. See System Firewall on page 62.
2. From the IWG management portal, click the **Endpoints** tab.
3. Click **Ptt-Express** on the left menu to add a new announcer endpoint.

**Figure 31** Add PTT-Express Endpoint

4. In the pop-up dialog, use the drop-down menu to select a channel number.
5. Enter a display name (optional).
6. Click **Add**.

Announcer Endpoint

This endpoint runs the Announcer service and allows a third party application to send a WAV audio file to one or more endpoints configured on the IWG. Each instance of the Announcer on the IWG must have a separate license. The Announcer endpoint forwards audio to other endpoints, but other endpoints cannot forward audio to the Announcer endpoint.

To add a new Announcer endpoint:

1. If using the RLS Announcer API, ensure TCP port 8111 is open. See System Firewall on page 62.
2. From the IWG management portal, click the **Endpoints** tab.
3. Click **Announcer** on the left menu to add a new announcer endpoint.
Figure 32  Add New Announcer Endpoint

4. On the pop-up dialog, select the **Automatically map announcer** check-box.

✓ **NOTE:** The endpoint receiving audio for each Announcer request is specified via the REST API or via the Announce function in the IWG management portal.

5. Click **Add**.

   A new row appears in the right table displaying a new announcer endpoint.

✓ **NOTE:** Multiple announcer endpoints are allowed on the IWG.

**How to Send an Announcement**

Make an announcement by transmitting a WAV audio file to the desired endpoints. Announcements are sent from third party applications or from the IWG management portal.

To send announcements from a third party application, use one of the following APIs:

- Announcer REST API - Refer to the Announcer REST API document for more information.
- RLS Announcer API - Refer to the RLS API documentation.

To send announcements from the Endpoints tab:

1. From the **Actions** field for the Announcer endpoint, click the **Announce** icon.

Figure 33  Send Announcement

2. On the pop-up dialog, click **Choose File** and navigate to the WAV file.
3. Click **Open**.
4. Click on the checkbox(s) next to the target endpoint(s).
5. Click **Send**.
**Messenger Endpoint**

This endpoint runs the Messenger service and allows a third party application to send a message to one or more PTT Pro endpoints configured on the IWG. Each instance of the Messenger on the IWG must have a separate license. The Messenger endpoint forwards messages to other endpoints, but other endpoints cannot forward messages to the Messenger endpoint at this time.

To add a new Messenger endpoint:

1. From the IWG management portal, click the Endpoints tab.
2. Click **Messenger** on the left menu to add a new announcer endpoint.

![Add Messenger Endpoint](image)

3. On the pop-up dialog, enter a display name (optional).
4. Click **Add**.
   
   A new row appears in the right table displaying a new announcer endpoint.

   ✓ **NOTE:** Multiple announcer endpoints are allowed on the IWG.

**How to Send a Message**

Messages are sent from third party applications or from the IWG management portal.

To send messages from a third party application, use the Messenger REST API. Refer to the Messenger REST API Developer’s Guide for more information.

To send messages from the Endpoints tab:

1. From the **Actions** field for the Announcer endpoint, click the **Message** icon.
2. On the pop-up dialog, enter a text message.
3. Click **Choose File** to attach an image to the message (optional).
4. Click on the checkbox(s) next to the target endpoint(s).
5. Click **Send**.

**LMR Endpoint**

Land Mobile Radio (LMR) is a two-way mobile radio system that supports Push-To-Talk (PTT) communications. The LMR endpoint is used to connect other communication types (PTT Express, for example) to an LMR system. Each LMR endpoint represents one LMR radio channel.

Additional equipment is required to connect the IWG to an LMR system:

- **IP gateway** - Provides conversion between an internet audio stream and the audio format required to transmit over an LMR radio.
- **LMR donor radio** - Relays audio between the LMR gateway and the LMR radio interface.

The following example demonstrates the IWG connecting a PTT Express channel to an LMR channel using an AudioMate IP Gateway and a Motorola Donor Radio.

**Figure 36** LMR Example

You can configure multiple instances of LMR endpoints, each connecting to a different IP gateway and donor radio. For more information on the LMR gateway and configuration, see [IP Gateway Configuration on page 58](#).
To add a new LMR endpoint:

1. From the IWG management portal, click the **Endpoints** tab.
2. Click **LMR** on the left menu to add a new announcer endpoint.

**Figure 37  Add LMR Endpoint**

3. In the pop-up dialog, enter the following information:
   - **Remote Server Address** - IP address of the remote IP gateway.
   - **Remote Server Port** - Port number of the remote IP gateway.
   - **Local Port** - Port number of the host machine.
   - **Display Name** (optional)
4. Click **Add**.

**PTT Pro Endpoints**

There are two PTT Pro endpoints available to communicate with the PTT Pro system.

- **PttPro Audio** - Use to send audio from other endpoints, through a proxy client to the PTT Pro system.
- **PttPro Text** - Use to send text messages from the Messenger endpoint, through a proxy client to the PTT Pro system.

PTT Pro supports multiple group types. When PTT Pro surveillance and unicast groups are configured as PTT Pro endpoints, communication is only in one direction, from the IWG to PTT Pro. Use surveillance and unicast groups to send IWG initiated communication, such as announcements and text messages. For a definition of PTT Pro group types, refer to the PTT Pro Management Portal Administrator Guide.

**PttPro Audio Endpoint**

The PttPro Audio endpoint represents a user from the PTT Pro system. To communicate with the PTT Pro system, the IWG uses a proxy client that must be pre-configured as a user on the PTT Pro server. The proxy client connects PttPro Audio endpoints to other endpoints, such as PTT Express, as shown in Figure 38. Use a different proxy for each PttPro Audio endpoint.

**NOTE:** A PTT Pro account is required to use a PttPro Audio endpoint. For information on configuring PTT Pro, refer to the PTT Pro Management Portal Customer Administrator Guide.
To add a PttPro Audio endpoint:

1. From the PTT Pro Administrative Portal, create a user account for the proxy client.

   **Figure 39  PTT Pro Add User Screen**

   a. In the Users tab, add a user (for example, Proxy1) and ensure it is activated.

   b. Record the activation code to use for the PttPro Audio endpoint in the IWG.

   **Figure 40  PTT Pro Groups Screen**

   c. In the Groups tab, add the user (Proxy1) as a member of a group (for example, Hardware).
2. From the IWG Administration Portal, add the group (Hardware) as an Endpoint.
3. Enter the activation code recorded from the PTT Pro Administrative Portal. This creates the proxy client, enabling communication between PttPro Audio and other endpoints on the IWG.

**PttPro Text Endpoint**

The PttPro Text endpoint represents a user from the PTT Pro system. To communicate with the PTT Pro system, the IWG uses a proxy client that must be pre-configured as a user on the PTT Pro server. When text messages are sent using the Messenger API to the Messenger endpoint, the proxy client forwards the messages to the PTT Pro system. See Messenger Endpoint on page 43. A single PTT Pro proxy client may be used for multiple PttPro Text endpoints.

![PttPro Text Endpoint Communication](Image)

**NOTE:** A PTT Pro account is required to use a PttPro Text endpoint. For information on configuring PTT Pro, refer to the PTT Pro Management Portal Customer Administrator Guide.

**Figure 42** PttPro Text Endpoint Communication

To add a PttPro Text endpoint:

1. From the PTT Pro Administrative Portal, create a user account for the proxy client.
Using the IWG

Figure 43  PTT Pro Add User Screen

a. In the Users tab, add a user (for example, Proxy1) and ensure it is activated.

b. Record the activation code to use for the PTT Pro endpoint in the IWG.

Figure 44  PTT Pro Groups Screen

c. In the Groups tab, add the user (Proxy1) as a member of a group (for example, Hardware).

Figure 45  IWG Add Text Endpoint

2. From the IWG Administration Portal, add the group (Hardware) as an Endpoint.

3. Enter the activation code recorded from the PTT Pro Administrative Portal. This creates the proxy client, enabling communication between PttPro Audio and the Messenger endpoint on the IWG.

✓ NOTE: To use one proxy client user account to create multiple PTT Pro text endpoints, enter the same activation code.
Content Sharing

Share video and audio files by uploading them to the IWG using the Messenger REST API. This feature enhances the Messenger endpoint. See Messenger Endpoint on page 43.

Share uploaded content using the following methods:

- Content sharing with direct notification - The source application uploads a file, receives a URL, and uses PTT Pro to send the URL directly to recipients. Content sharing with direct notification is available in some versions of the PTT Pro client.
- Content sharing with automatic notification - The source application uploads the file and a list of PTT Pro users or groups to the IWG. The IWG uses PttPro Text endpoints to send the URL to the PTT Pro recipients.

**NOTE:** To share content, the IWG Streaming feature must be licensed. The IWG streaming feature is not associated with an endpoint. When a Streaming license is added to the IWG, the streaming feature becomes available. See License on page 51.

To share video or audio, use the Messenger REST API to:

- Upload the file.
- Copy the file location.
- Send the file location as a hyper-link in a PTT Pro message.

For detailed information on the streaming feature, refer to the Messenger REST API Developer’s Guide.

Call Log

**Figure 46**  IWG Call Log Tab
The Call Log lists all audio transactions that take place in this IWG. The following fields display for each audio transaction:

- **Call ID** - a unique numerical value identifying this call/transaction.
- **Source** - a source endpoint name.
- **Forwarded To** - a list of endpoints to which audio forwards.
- **Failed** - a list of endpoints where IWG was not able to forward audio because of busy or invalid state reasons.
- **Started At** - the time stamp when transaction started.
- **Duration** - the duration of the call in seconds.
- **Codec** - audio codec used by this call.
- **Actions** - use to delete the row.

Delete all Call Log records by clicking on the **Delete All** button on the top right.

---

**Media**

**Figure 47**  IWG Media Tab

The Media tab lists all media files uploaded into this IWG. Use the Filter field to filter the list of media files by type, name, or other information.

![IWG Media Tab](image)

The Media tab lists all media files uploaded into this IWG. Use the Filter field to filter the list of media files by type, name, or other information.

**NOTE:** You can order the listing of items by clicking on the column heading: Type, Name, Created, or Size.

The following fields display for each media file:
Using the IWG

- **Type** - the form of file; typically **Upload**, or **Send**.
- **Name** - file name.
- **Created** - date and time the file was uploaded into the IWG.
- **Size** - file size in bits.
- **Actions** - click ▶ to play the file: click 🗑️ to delete the file.
- Delete all Media Files records by clicking on the **Delete All** button on the top right.

**License**

**Figure 48** IWG License Tab

The License tab lists all IWG features with license information for each. Each row in the License tab represents a single feature activation code. For example, **Figure 48** shows multiple activation codes for PTT.Express, each with a different expiration date. **Table 3** describes the columns that appear on the licensing tab.
Using the IWG

Host information for the IWG is displayed on the left side of the License tab. It is recommended to record this information since it may be needed for customer support.

### Releasing Licenses

To release all licenses associated with this IWG, click the **Release Licenses** button. Activation codes must then be reentered to license the IWG and enable interworking services.

### Adding Activation Codes

Each activation code provides additional licenses for the IWG. To add licensing activation codes click **Add Activation** code.

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Feature     | Feature name. Usually the endpoint or resource name. Supported features are:  
- IWG (base feature associated with the software version)  
- PTT Express  
- PTT Pro  
- LMR  
- Announcer  
- Messenger  
- Streaming |
| Version     | Version of the feature. |
| State       | GREEN - license is valid  
RED - license is not available |
| Total Licenses | Total number of licenses acquired for this feature. |
| Used Licenses | Number of licenses currently in use by endpoints. |
| Expires     | Expiration date of the feature. |
| Issued      | Date the feature was added. |
| Perpetual   | Indicates if the feature is set to last perpetually. |
| Notice      | Provides a notice when the feature is a trial license. |
Enter the activation code and click **Apply**.

- To enter multiple activation codes, separate the codes with a comma. Do not add spaces.
- To enter a single activation code multiple times, after the code add a colon and the number of times to retrieve the license. For example, to use an activation code 10 times, enter `XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX:10`.

---

**Administration**

**Figure 50**  IWG Administration Tab

The left side of the Administrator tab displays overall IWG status and lists the following administrative actions:

- **NOTE:** To shut down the IWG using the **IWG stop** option in the IWG Service Menu, see **Start Stop Restart** on page 32.
  - **Restart** - restarts all endpoints configured on the IWG.
  - **Stop** - stops all endpoints configured on the IWG.
• **Start** - starts all endpoints configured on the IWG.
• **Import Config** - imports a new configuration XML file and restarts the IWG. See *IWG Management Portal - Import Configuration File on page 28.*
• **Export Config** - exports current configuration as an XML file to the machine running the web browser.
• **Change login** - sets a new administrator login name and password. The default login is **admin**, the default password is **Zamboni**.

✓ **NOTE:** To change the credentials needed to log into the IWG Service Menu, go to *Change Admin Password on page 63.*

The right side of the tab shows a table with current statistics.

---

### System Log

**Figure 51** IWG System Log Tab

This tab displays the last 1000 logging messages from IWG. It is updated in real-time. The following actions are available on the System Log tab:

• **Filter** - sets a new filter for displaying log messages. For example, to show only ALARMS, set Filter to **ALM**.

• **Download IWG Logs** - downloads a zip file with all log files from IWG. The IWG starts a new logging file at each restart and preserves the previous log file.

• **IWG Logging Level** - sets a new logging level.

To configure logging levels for each endpoint, see *Log Level on page 39.*
Introduction

This chapter provides examples for configuring the IWG using the management portal, or configuration files. For information on how to use configuration files to configure the IWG, see Configuration on page 26.

Management Portal Examples

The following examples demonstrate how to use the IWG and enable interworking.

Connect PTT Express and LMR

An enterprise wants to connect a group using PTT Express channel 1 with another group using an LMR channel, allowing them to communicate with each other.

**Figure 52** Connecting PTT Express and LMR

To configure interworking between PTT Express and LMR:

1. Add PTT Express channel 1 as an endpoint. See PTT.Express Endpoint on page 41.
2. Add LMR channel 2 as an endpoint. See LMR Endpoint on page 44.
3. Add audio mappings from PTT Express channel 1 to LMR channel 2 and vice versa to enable 2-way communication. See Mapping on page 39.

Each voice transaction occurring on PTT Express channel 1 forwards to LMR channel 2, and vice versa.

Connect PTT Express and Announcer

An enterprise wants to send announcements to a group using a PTT Express channel.
To configure interworking between PTT Express and Announcer:

1. Add the Announcer as an endpoint. See Announcer Endpoint on page 41.
2. Add PTT Express channel 4 as an endpoint. See PTT.Express Endpoint on page 41.
3. Add an audio mapping from the Announcer to PTT Express channel 4. See Mapping on page 39.

When Announcer requests are received with a destination of PTT Express channel 4, the audio is transmitted on PTT Express channel 4.

**NOTE:** Using Announcer requires an external application to send the announcement to the IWG. For the Announcer API and a sample script to send an announcement refer to the Announcer.

Endpoints must be licensed before the IWG can use them. For example, the IWG may be licensed for the Announcer endpoint and 5 PTT Express channels/endpoints, but may not be licensed for LMR channels/endpoints. Enter activation codes provided with your order confirmation information into the IWG to add endpoints. For more information, see License on page 51.

---

**Static Configuration Example**

The following is an example of a `IWG.conf` file using parameters from Table 2.

```plaintext
licenseCodes="XXX-XXXX-XXXX-XXXX"
logLevel="5"
hostAlias="My IWG Alias"
```

**NOTE:** The static configuration file cannot contain endpoint information. To configure endpoints, use the dynamic configuration file.

---

**Dynamic Configuration Example**

When creating an `IWG.xml` configuration file, the following are required:

- A single root node named `IWG` with optional parameters.
- At least one child node defining a new endpoint instance with unique values for `node ID and type` parameters.
- PTT.Express nodes must define a `channel`.
- LMR nodes must define an IP address and port information.
- At least one mapping value with optional follow flag. See Mapping on page 39.
ID[: [follow]], ID[: [follow]]

where

• ID is the node ID
• follow flag forces IWG to add all mappings assigned to the target endpoint to incoming communications from the originating endpoint.
• [ ] indicates optional elements.

The example below is an IWG.xml file with the IWG node, a map of general parameters and three child nodes (PTT.Express, LMR and Announcer).

```xml
<?xml version="1.0" encoding="utf-8"?>
<preferences>
  <node id="IWG"
    licenseCodes="XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX"
    logLevel="5"
    hostAlias="My IWG Alias"
    type="IWG"
    enabled="true">
  </node>

  <node id="1"
    mapping="2"
    autoMap="true"
    type="Announcer">
  </node>

  <node id="2"
    channel="10"
    epname="Warehouse Dept"
    type="PTT.Express">
  </node>

  <node id="3"
    epname="Hardware Dept"
    remoteip="10.50.51.213"
    remoteport="9696"
    localport="9696"
    type="LMR">
  </node>

</preferences>
```
IP Gateway Configuration

The IWG requires an IP Gateway to provide connectivity to LMR radios. The AudioMate AM260r IP Voice Gateway is an example of one of the many IP Gateways that can provide this connectivity.

The AM360r supports the following specifications:

- RTP over UDP
- G.711 u-law codec @ 64 kbps
- Receipt of 20 ms frames at any bundling ratio per UDP packet
- Transmission of 20 ms frames at any bundling ratio per UDP packet.

Consider the following principles when configuring your IWG for LMR services:

- One IP Gateway supports one LMR Donor Radio
- One LMR Donor Radio supports one LMR Talk-Group
- The IP Gateway can participate in only one LMR Talk Group
- Each LMR Endpoint in the IWG corresponds to one IP Gateway.

Using multiple LMR radio channels with the IWG require multiple LMR Donor Radios, multiple IP Gateways, and multiple LMR endpoints.

The planned deployment site must meet the following requirements:

- The IP Gateway must have Internet or intranet access to the IWG.
- A static and unique IP address must be assigned to each IP Gateway.
- The data network connectivity between each IP Gateway and the IWG must support 90 kbps of traffic.

When adding an LMR Endpoint in the IWG, the following information is required:

- IP address and port number of the associated IP Gateway. The IP address/port number pair must be unique for each IP Gateway connecting to this IWG.
- Local port of the IWG host machine. The local port must be unique for each LMR Endpoint on this IWG.

When configuring the IP Gateway to connect to the IWG:

- The remote IP address of the IP Gateway must match the IP address of the IWG.
- The remote port of the IP Gateway must match the local port configured in the LMR endpoint on the IWG.
- The local port of the IP Gateway must match the remote server port configured in the LMR endpoint on the IWG.
Introduction

When the virtual machine initializes, the Main Service Menu displays.

Figure 54  Virtual Machine Utility Menu

Use the Main Service Menu to:

- Change the hostname
- Change the IP address
- Change date and time
- Check the system
- Configure the system
- Check the System Firewall
- Access the IWG Service Menu
- Change administrator password
- Shutdown or reboot system.

To choose a menu option, enter the option number and press Enter.
Change Hostname

Use this option to change the virtual machine hostname. The hostname is the FTP server address.

1. From the Main Service Menu, choose option 1.

**Figure 55 Change Hostname Menu**

```
Current Hostname: IWG_gold

1.) Change Hostname
2.) Exit Menu

Enter your menu choice [0-1]: _
```

2. From the Change Hostname menu choose option 1 and press Enter.
3. Enter the new hostname.
4. Press Enter.

Change IP Address

Use this option to set a static address or set up a DHCP.

√ **NOTE:** It is recommended to use a permanent IP address, such as a static IP address or DHCP reservation. This allows easy access to the IWG Management Portal, and predictable addresses for use in the Announcer and Messenger APIs.

1. From the Main Service Menu, choose option 2.

**Figure 56 Change IP Address Menu**

```
# Change IP Address Menu
#
1.) Static
2.) DHCP
0.) Exit Menu

Enter your menu choice [0-2]: 
```

2. From the Change IP Address menu select one of the following options:
   - **Option 1 - Static Address** - Update the IP address manually and restart the IWG.
     a. Enter the server IP address.
     b. Enter the gateway IP address.
     c. Enter the subnet mask.
     d. Enter the DNS IP address.
     e. Choose option 1 to confirm the changes, or choose option 2 to re-enter the information.
   - **Option 2 - DHCP** - Update the IP address automatically and restart the IWG.
Change Date and Time

Use this option to change the date and time.

**NOTE:** If the time zone is changed, reboot the virtual machine. See Shutdown or Reboot System on page 64.

1. From the Main Service Menu, choose option 3.

**Figure 57** Change Date and Time Menu

```
1.) Change Date Using NTPD
2.) Change Date Manually
8.) Exit

```

2. From the Change Date and Time menu select one of the following options:

- Option 1 - Change Date Using NTPD - Update the date and time automatically.
- Option 2 - Change Date Manually - Follow the prompts to manually enter the month, day, year, hour, and minutes. Hours are represented with the 24 hour clock.

**Figure 58** Change Date Manually

```
Please enter 2 digit month (example for March would be 03):
04
Enter 2 digit day of month (example 03 would be 3rd day of month):
13
Enter 4 digit year (example would be 2007):
2017
Enter 2 digit hour (example would be 23 would be 11:00PM):
23
Enter 2 digit minute (example would be would be 02):
50
```

System Check

Use this option to perform a system check.

From the Main Service Menu, choose option 4.

**Figure 59** System Check Menu

```
1.) Check CPU
2.) Check Drive Space
3.) Check Tap
4.) Ping Network Address
5.) Run Trace Dump
6.) Update Menu
8.) Exit Menu

```

On the System Check menu, select one of the following options:
Main Utility Menu

- **Option 1 - Check CPU** - Display the CPU utilization of the virtual machine.
- **Option 2 - Check Drive Space** - Display the memory utilization of your virtual machine.
- **Option 3 - Check Top** - Display running processes and process details. To exit this screen, enter `q` and press `Enter`.
- **Option 4 - Ping Network Address** - Enter an IP address or DNS to display network latency details.
- **Option 5 - Run Trace Dump** - Run a UDP or TCP trace to analyze traffic on the virtual machine. After running a trace dump, use the **Export a Trace** option to view the report in a packet viewer.

**NOTE:** Running a trace dump under heavy traffic or for a long period of time may consume a large amount of disk space.

- **Option 6 - Update Menu** - Update the **System Check** menu.
- **Option 0 - Exit Configuration Menu** - Exit the **System Check** menu.

---

**System Configuration**

Use the **System Configuration** menu to check the network configuration for the virtual machine.

From the Main Service Menu, choose option 5.

**Figure 60 System Configuration Menu**

```
+---------------------------------------------+
<table>
<thead>
<tr>
<th>Configuration Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.) Check Server IP</td>
</tr>
<tr>
<td>2.) Check DNS Server</td>
</tr>
<tr>
<td>3.) Check NTP Configuration</td>
</tr>
<tr>
<td>4.) Check Machine ID</td>
</tr>
<tr>
<td>0.) Exit Menu</td>
</tr>
</tbody>
</table>
+---------------------------------------------+
```

On the **System Configuration menu**, select one of the following options:

- **Option 1 - Check Server IP** - Display the server IP information for the virtual machine.
- **Option 2 - Check DNS Server** - Display the current DNS information for the virtual machine.
- **Option 3 - Check NTP Configuration** - Display the Network Time Protocol information for the virtual machine.
- **Option 4 - Check Machine ID** - Display the identification for the virtual machine.
- **Option 0 - Exit Configuration Menu** - Exit the System Configuration menu.

---

**System Firewall**

Use the **System Firewall** menu to check the firewall status, shows ports, add ports, and remove ports for the virtual machine.

To use PTT Express endpoints, add UDP ports 5000 to 5031.

To use the RLS Announcer API with an Announcer endpoint, add TCP port 8111.
NOTE: By default, TCP ports 443, 8443, and 22 are open.

From the Main Service Menu, choose option 6.

**Figure 61  System Firewall Menu**

On the **System Firewall menu**, select one of the following options:

- **Option 1 - Show ports** - Display the open ports for the virtual machine. Automatically exits back to the **System Firewall** menu after a few seconds.

- **Option 2 - Add tcp ports** - Enter a TCP port number then press Enter. The port is added and then the **Show ports** screen displays.

- **Option 3 - Remove tcp ports** - Enter a TCP port number then press Enter. The port is removed and then the **Show ports** screen displays.

- **Option 4 - Add udp ports** - Enter a UDP port number then press Enter. The port is added and then the **Show ports** screen displays.

- **Option 5 - Remove udp ports** - Enter a UDP port number then press Enter. The port is removed and then the **Show ports** screen displays.

- **Option 0 - Exit Configuration Menu** - Exit the System Configuration menu.

**IWG Service Menu**

For information on the IWG Service Menu, see **Updating the IWG on page 23**.

**Change Admin Password**

Use the **Change Admin Password** menu to set an administrative password, used to remotely access the IWG virtual machine using a PuTTY terminal.

From the Main Service Menu, choose option 8.

**Figure 62  Change Password Screen**
Password Policy

To set a secure administrative password:

- Use at least 8 characters
- Use at least one of each of the following:
  - Lowercase character
  - Uppercase character
  - Number

---

Shutdown or Reboot System

Use the **Shutdown or reboot system** menu to initiate a graceful shutdown or reboot of the virtual machine. In a graceful shutdown or reboot, data that is queued, but not transmitted, can be sent before the connection is closed.

From the Main Service Menu, choose option 9.

---

From the **Shutdown or reboot system** menu, select one of the following options:

- **Option 1 - Shutdown System Gracefully** - Initiate a graceful shutdown of the virtual machine.
- **Option 2 - Reboot System Gracefully** - Initiate a graceful reboot of the virtual machine.
- **Option 0 - Exit Configuration Menu** - Exit the **Shutdown or reboot system** menu without initiating a shutdown or reboot.