PRI Gateway Deployment Guide

FortiVoice 7.0.7

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO LIBRARY

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE

https://training.fortinet.com

FORTIGUARD LABS

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

Change log

Date	Change description
2025-04-23	Initial release of the FortiVoice 7.0.7 PRI Gateway Deployment Guide.

Overview

The FortiVoice primary rate interface (PRI) gateway works in conjunction with your FortiVoice phone system, an IP private branch exchange (IP PBX), to expand resources and support additional phone lines.

With a PRI gateway, you connect your legacy telephony infrastructure composed of PRI (T1 or E1) digital lines to a FortiVoice phone system.

This document describes how to deploy a FortiVoice PRI gateway.

This section includes the following topics:

Supported models

The following table lists the supported FortiVoice PRI gateway models:

Model	Digital line	Port and span
FortiVoice Gateway GT01	One PRI (T1/E1) digital line	Single port configuration: PRI port 1 with span 1
FortiVoice Gateway GT02	Two PRI (T1/E1) digital lines	Dual port configuration: • PRI port 1 with span 1 • PRI port 2 with span 2 By default, both spans are assigned to a single trunk.
For more details about features and specifications, see the FortiVoice Gateways Data Sheet.		

A PRI T1 digital line is common in the United States, Canada, and Japan. A PRI T1 digital line has a span with 23 voice or data channels (B channels) and a single channel for signaling (D channel). Each of the 23 channels can hold one phone call at a time, for a maximum of 23 simultaneous phone calls.

A PRI E1 digital line is common in Europe and Australia. A PRI E1 digital line has a span with 30 voice or data channels (B channels) and a single channel for signaling (D channel). Each of the 30 channels can hold one phone call at a time, for a maximum of 30 simultaneous phone calls.

The following FortiVoice phone systems can manage a PRI gateway:

- FortiVoice 100E and larger

> The FortiVoice 100E continues to support the management of PRI gateways. However, this model has reached its end-of-order (EOO) date.

- FortiVoice-VM-100 and larger

For details about the capacity of FortiVoice phone systems for managed gateways, see the FortiVoice Phone System Capacities Data Sheet.

For more details about the FortiVoice phone systems, see the FortiVoice Phone Systems Data Sheet.

Topology

You can configure a PRI gateway to be on the same LAN as the FortiVoice phone system or over a VPN.

The FortiVoice phone system manages all configuration information for ports. However, the PRI gateway manages the following settings:

- Network settings
- Administrator accounts
- System options
- SIP settings

The following image shows an example topology of a FortiVoice phone system with a FortiVoice Gateway GT01 or GT02:
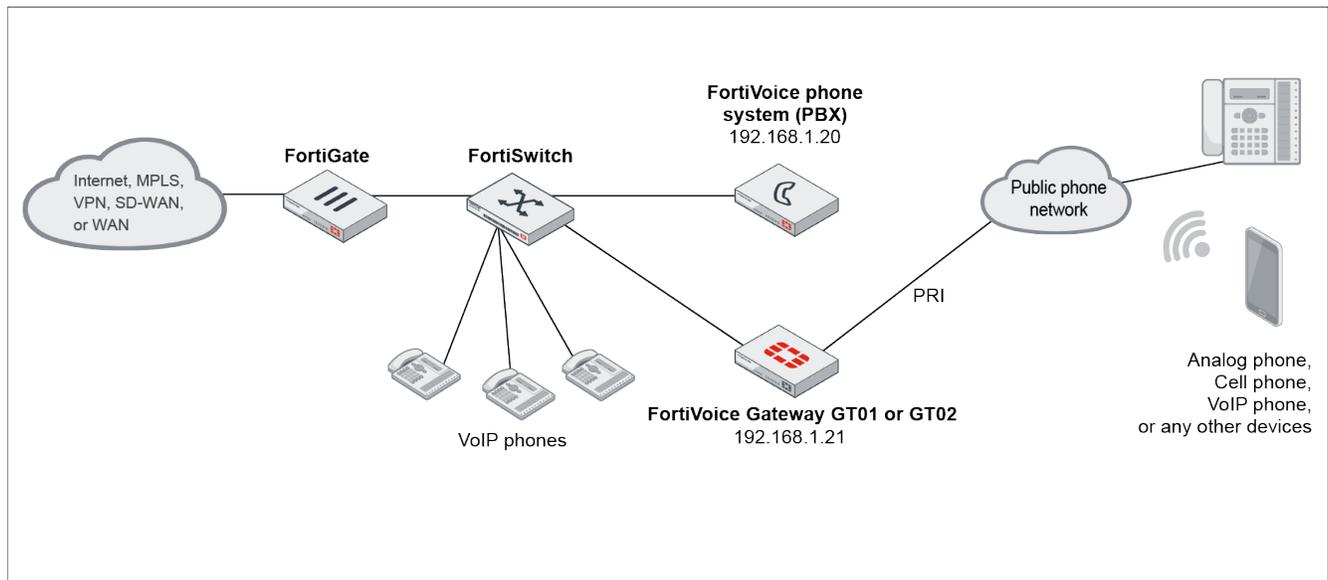
Deployment

Before starting procedures in this guide, make sure to complete the basic setup of the FortiVoice phone system and connect to the GUI of that system. For more details, see the FortiVoice Phone System Administration Guide.

To deploy a PRI gateway and then manage that device with a FortiVoice phone system, review the tasks and perform the procedures listed in the following workflow:

Task sequence	Description	Procedure
Perform tasks 1 to 4 on the PRI gateway.		
Task 1	Perform the following actions to complete the initial setup of the PRI gateway: • Physically install the PRI gateway. • Connect the Ethernet port to your network. • Connect the PRI port(s) to the public phone network.	
Task 2	Connect to the GUI of the PRI gateway.	Connecting to the PRI gateway on page 8
Task 3	Configure the following system settings: • Network interfaces • Static routes • Administrator accounts • System options • SIP settings, optional	Configuring administrator and system settings on page 10
Task 4	Upgrade the firmware of the PRI gateway to the latest GA release.	Upgrading the PRI gateway firmware on page 12
Perform tasks 5 to 11 on the FortiVoice phone system, as applicable.		
Task 5	Add a PRI gateway. The FortiVoice phone system can auto-discover a PRI gateway when they are both on the same LAN.	Perform one of the following procedures: • Adding a PRI gateway (auto-discovered) on page 13 • Adding a PRI gateway (not auto-discovered) on page 15
Task 6	Apply the gateway configuration file from the FortiVoice phone system to the PRI gateway.	Applying the PRI gateway configuration on page 17

Task sequence	Description	Procedure
Task 7	Verify that the SIP communication between the FortiVoice phone system and the PRI gateway is successful and that a PRI trunk exists between the PRI gateway and the public phone network.	Verifying the PRI gateway configuration on page 17
Task 8	Add a trunk profile to an inbound dial plan.	Adding a PRI gateway trunk to an inbound dial plan on page 18
Task 9	Add a trunk profile to an outbound dial plan.	Adding a PRI gateway trunk to an outbound dial plan on page 18
Task 10	Optionally, edit a trunk profile.	Optional - Editing a trunk profile for a PRI gateway on page 19
Task 11	Optionally, create additional trunk profiles.	Optional - Creating an additional trunk profile for a FortiVoice Gateway GT02 on page 23

Connecting to the PRI gateway

After physically installing the PRI gateway and connecting its Ethernet and PRI ports, review the following table and perform the procedure that applies to your scenario to connect to the GUI of the FortiVoice Gateway.

Scenario	Procedure
You are connecting to the device for the first time.	Perform the steps in Connecting to the GUI of the FortiVoice Gateway on page 9.
You have reset the device configuration to its default state.	Perform the steps in Connecting to the GUI of the FortiVoice Gateway on page 9.
You are a returning user who has completed the basic configuration of the device.	Access the GUI using the IP address, administrative access protocol, administrator account, and password that you have already configured, instead of the default settings. 1. Start a web browser and enter the URL: `https://<IP_address>/admin` Where `<IP_address>` is the IP address of the PRI gateway that you want to connect to. If the PRI gateway configuration is using a non-default HTTPS port, then add :<port_number> after the IP address. For example: `https://<IP_address>:446/admin`. 2. Enter the name and password associated with your account. 3. Click **Login**. You have completed this procedure. 4. Go to Configuring administrator and system settings on page 10 to make sure that you configure the required settings.

Connecting to the GUI of the FortiVoice Gateway

To connect to the GUI of the FortiVoice Gateway using its default settings, you must have the following hardware and software:

- A computer with an RJ-45 Ethernet network port
- One of the recommended web browsers:
  - Google Chrome version 135
  - Microsoft Edge version 135
  - Mozilla Firefox Standard Release version 137
  - Apple Safari version 18.4
- An Ethernet cable

Procedure steps

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 and a subnet mask of 255.255.255.0.
2. Using the Ethernet cable, connect the Ethernet port of the management computer to port1 of the PRI gateway.
3. Start your browser and enter the default URL https://192.168.1.99/admin.
4. To support HTTPS authentication, the PRI gateway ships with a self-signed security certificate, which it presents to users whenever they initiate an HTTPS connection to the PRI gateway. When you connect, your browser may display two security warnings related to this certificate:
   - The certificate is not automatically trusted because it is self-signed, rather than being signed by a valid certificate authority (CA). Self-signed certificates cannot be verified with a proper CA, and therefore might be fraudulent. You must manually indicate whether or not to trust the certificate.
   - The certificate may belong to another website. The common name (CN) field in the certificate, which usually contains the host name of the website, does not exactly match the URL you requested. This could indicate a server identity theft, but could also simply indicate that the certificate contains a domain name while you have entered an IP address. You must manually indicate whether this mismatch is expected or not.

   Both warnings are normal for the default certificate.
5. Verify and accept the certificate, either permanently (the web browser will not display the self-signing warning again) or temporarily. You cannot log in until you accept the certificate. For details on accepting the certificate, see the documentation for your web browser.
6. In **Name**, enter `admin`.
7. Leave the **Password** field empty. In its default state, there is no password for this account.
8. Click **Login**.
   With a successful login, the GUI appears.
9. Set the password for this account:
   a. In the right corner of the GUI, click **admin**.
   b. Click **Change Password**.

   > ⚠ Enter an administrator password that is six characters or more. For better security, enter a longer password with a complex combination of characters and numbers, and change the password regularly. Failure to provide a strong password could compromise the security of your FortiVoice PRI gateway.

   c. Enter a password in **New password** and **Confirm password**.
      The password can contain any character except spaces.
   d. Click **OK**.

You have completed this procedure.

10. Go to .

Configuring administrator and system settings

Configure administrator and system settings on the FortiVoice Gateway by completing the following procedures:

- Editing a physical network interface on page 10
- Configuring a static route on page 10
- Creating an additional administrator account on page 11, optional
- Configuring system options on page 11
- Configuring SIP settings on page 12, optional

> If you need more details about the configuration of system settings presented in this section, see the Configuring system settings section in the FortiVoice Gateway Administration Guide.

Editing a physical network interface

Perform this procedure to set the IP address, netmask, and administrative access protocols of the PRI gateway.

1. In the GUI of the FortiVoice Gateway, go to **System > Network**.
    The **Network** tab displays the following ports:
    Port 1 has a default IP address and netmask set to 192.168.1.99/24.
    Port 2 has a default IP address set to 192.168.2.99/24.
2. Double-click a network interface that you want to use to set the IP address of the PRI gateway.
3. In **Addressing Mode, Manual**, go to **IP/Netmask** and edit the IP address and netmask of the interface. Make sure that this IP address is outside of the FortiGate DHCP range.
4. In **Advanced Setting**, make sure to enable the protocols that you want the network interface to use to accept connections to the PRI gateway.
5. In **Administrative status**, make sure that **Up** is selected for the network interface to be available to receive traffic.
6. Click **OK**.

Configuring a static route

Perform this procedure to configure a static route to the router.

1. In the GUI of the FortiVoice Gateway, go to **System > Network**, and then click the **Routing** tab.
2. Click **New**.
3. Make sure that **Enable** is selected.
4. In **Destination IP/Netmask**, enter the destination IP address and netmask of packets subject to this static route. To create a default route that matches all destination IP addresses, enter **0.0.0.0/0**.
5. In **Interface**, select the interface that this route applies to.
6. In **Gateway**, enter the IP address of the router.

7. In **Comment**, enter any notes for this static route.
8. Click **OK**.

Creating an additional administrator account

Optionally, perform this procedure to create an additional administrator account with restricted permissions. By default, the PRI gateway has a single administrator account called *admin*.

Before you begin

If you want to create or edit an admin profile, perform this task on the FortiVoice phone system first. For more details about the admin profile, see the Configuring administrator profiles section in the FortiVoice Phone System Administration Guide.

Procedure steps

1. In the GUI of the FortiVoice Gateway, go to **System > Administrator**.
2. Click **New**.
3. In **Administrator**, enter the name for this administrator account.
   The name can contain numbers (0-9), uppercase and lowercase letters (A- Z, a- z), hyphens (-), and underscores (_). Other special characters and spaces are not allowed.
4. In **Email address**, enter the email address of the administrator.
5. In **Admin profile**, select the admin profile. This profile determines which functional areas the administrator account can view or affect.
6. In the **New password** and **Confirm password**, enter the password for this account.
   The password can contain any character except spaces.

> ⚠️ Do not enter a PRI gateway administrator password that is less than six characters long. For better security, enter a longer password with a complex combination of characters and numbers, and change the password regularly. Failure to provide a strong password can compromise the security of your PRI gateway.

7. In **Trusted hosts type**, use **User defined**.
8. In **Trusted hosts**, enter the IPv4 or IPv6 address or subnet and netmask from which this administrator can log in.
   For example, if your private network has an IP address of 192.168.1.0 and you want to allow the administrator to log in to the PRI gateway from your private network, enter `192.168.1.0/24`.
   If you want the administrator to access the PRI gateway from any IP address, use `0.0.0.0/0`.
9. In **Select language**, select the language to display in the GUI when this administrator logs in.
10. In **Select theme**, select the theme to display in the GUI when this administrator logs in.
11. In **Description**, enter any notes for this account.
12. Click **Create**.

Configuring system options

Perform this procedure to set the system idle timeout and administration ports.

1. In the GUI of the FortiVoice Gateway, go to **System > Configuration**, and then click the **Option** tab.
2. In **Idle timeout**, enter the amount of time in minutes that an administrator can be inactive before the PRI gateway automatically logs out the administrator.

3. In **Administration Ports**, specify the TCP ports for the administrative access on all interfaces.

   Default port numbers:

   - **HTTP port number**: 80
   - **HTTPS port number**: 443
   - **SSH port number**: 22
   - **TELNET port number**: 23

4. Click **Apply**.

Configuring SIP settings

Optionally, perform this procedure to configure SIP settings.

1. In the GUI of the FortiVoice Gateway, go to **System > Advanced Setting**, and then click the **SIP** tab.
2. In **SIP Transport**, enable the ports as required.

   SIP communications commonly uses TCP or UDP port 5060.

   Port 5060 is used for nonencrypted SIP signaling sessions.

   Port 5061 is typically used for SIP sessions encrypted with the TLS protocol.
3. In **RTP Setting**, keep the default values.
4. Click **Apply**.

   You have completed this procedure.
5. Go to .

Upgrading the PRI gateway firmware

Perform this procedure to upgrade the PRI gateway firmware.

Procedure steps

1. Identify the firmware version that is running on the gateway:
   a. In the GUI of the FortiVoice Gateway, go to **Dashboard**.
   b. In the **Status** tab, go to the **System Information** widget and review the **Firmware version** row.
   c. Take note of the firmware version and build number.
2. Identify the latest software release that is available for the gateway firmware:
   a. Go to the Fortinet Support website.
   b. Log in to your existing account or register for an account.
   c. Click **Support** and then in **Downloads**, click **Firmware Download**.
   d. In **Select Product**, select **FortiVoice**.
   e. In the **Release Notes** tab, review the FortiVoice 7.0 list to identify the latest firmware version.
   f. Compare the firmware version and build number with the firmware version that is running on the gateway.
   g. If the build number of the firmware version running on the gateway matches the one on the Fortinet Support website, then you do not need to perform an upgrade. You have completed this procedure. Go to one of the following procedures:
      -
      -
   h. If the build number of the firmware version running on the gateway is an earlier build, then you need to prepare for an upgrade:

      i.   Review the FortiVoice Phone System Release Notes. This document includes the most current upgrade information such as supported upgrade paths and may also contain details that were unavailable at the time this procedure was created.

     ii.   In the **Download** tab, navigate through the v7.00 directories to locate the firmware image file. For example, FVG_GT-v70-build0094-FORTINET.out.

    iii.   To download the firmware image file to your management computer, click **HTTPS**.

    iv.   Save the file on your management computer and take note of the location where you save the file.

3. Back up the configuration file:

    a.   In the GUI of the FortiVoice Gateway, go to **Dashboard**.

    b.   In the **Status** tab, go to the **System Information** widget and the **System configuration** row.

    c.   Click **Backup**.

    d.   Save the file on your management computer and take note of the location where you save the file.

4. Upgrade the firmware:

    a.   In the **System Information** widget, go to the **Firmware version** row.

    b.   Click **Update**.

    c.   Locate the firmware file and then upload that file.
        Your web browser uploads the firmware file to the gateway.

    d.   To confirm, click **Yes**.
        The gateway installs the firmware and restarts.

    e.   To make sure that the FortiVoice Gateway GUI reloads correctly and displays all changes, clear the cache of your web browser and restart it.

5. Verify that the firmware is successfully installed:

    a.   In the **System Information** widget, go to the **Firmware version** row.

    b.   Make sure that the firmware version is the one that you upgraded to.
    You have completed this procedure.

6. Go to one of the following procedures:

- Adding a PRI gateway (auto-discovered) on page 13
- Adding a PRI gateway (not auto-discovered) on page 15

Adding a PRI gateway (auto-discovered)

The FortiVoice phone system can auto-discover a PRI gateway when they are both on the same LAN. With an auto-discovered device, you can create a new configuration for that gateway or replace an existing gateway configuration.

Procedure steps

1. Connect to the GUI of the FortiVoice phone system.
2. Go to **Managed System > Gateway**, and then click the **PRI Gateway** tab.
3. Click **Actions** > **Unmanaged Gateway**.
   The dialog opens and displays all the gateways discovered on the LAN of the FortiVoice phone system.
4. Select the PRI gateway that you want to add.
5. In the **Action** drop-down list, select one of the following actions:

- **Create New Device** to add the gateway as a new entry into the FortiVoice phone system. Go to step 6.
- **Replace Existing Device** to choose which gateway to replace. You can use this option in a situation where, for example, you want to replace a defective gateway. Go to step 17.

6. If you selected **Create New Device**, then configure the following settings:

GUI field	Description
Enabled	Select to activate the configuration of the PRI gateway.
Name	Enter a unique name to identify the PRI gateway.
Display name	Not required. You can leave this field empty.
Hostname/IP address	The hostname or IP address of the auto-discovered PRI gateway. For an auto-discovered PRI gateway, the FortiVoice phone system autopopulates this field. **Get Device Information**: • Before you click this button, make sure to enter the required information in the **Admin user name** and **Admin password** fields below. • Click this button to poll the PRI gateway and get the MAC address of the gateway. This action can confirm that the systems can communicate and that the password is valid. **Connect Device**: This procedure does not use this button. With this button, you would access the FortiVoice Gateway GUI in a separate tab in your web browser.
Admin user name	Enter the user name of the administrator account used for logging in to the PRI gateway. The default is admin.
Admin password	Enter the password associated with the Admin user name. To show the password, click the eye icon 👁. The default is no password.
Serial number	The serial number of the gateway that you are adding to the FortiVoice phone system. For an auto-discovered PRI gateway, the FortiVoice phone system autopopulates this field.
Type	The type of gateway that you are adding to the FortiVoice phone system.
MAC address	The MAC address of the gateway that you are adding to the FortiVoice phone system.
Survivability branch	The FortiVoice LSG solution can support a FortiVoice PRI gateway at a branch office. To link this PRI gateway with a survivability branch, select that branch from the list. For details about deploying a FortiVoice LSG unit, see the FortiVoice Local Survivable Gateway Deployment Guide.
Physical location	Select **Internal** if the PRI gateway and FortiVoice phone system are on the same LAN. The PRI gateway connects to the internal IP address of the FortiVoice phone system. Select **External** if the PRI gateway connects to the FortiVoice phone system with an external IP.

GUI field	Description
Description	Optionally, add any applicable notes for this gateway.

7. Click **Finish** and **Close**.
   The FortiVoice phone system creates a PRI trunk with one span (for FortiVoice Gateway GT01) or two spans (for FortiVoice Gateway GT02).
8. Reload your web-browser to make sure that the GUI displays the latest changes.
9. To review trunk details, go to **Trunk > Gateway**.
10. In the list, find the newly added gateway.
11. Verify that the **Status** column displays *In service*.
12. Double-click the newly added PRI gateway.
13. In the **Edit span** field, click **Edit** .
14. Make sure that the **Advanced Options** are set to your service provider specifications.
15. For a FortiVoice Gateway GT02, repeat steps 13 and 14 for span 2.
    You have completed this procedure.
16. Go to .
17. If you selected **Replace Existing Device**, choose which gateway you want to replace and then use the UI to replace it.
    You have completed this procedure.
18. Go to .

Adding a PRI gateway (not auto-discovered)

Perform this procedure to add a PRI gateway to the FortiVoice phone system in cases such as in the following examples:

- You are preconfiguring the FortiVoice phone system before deploying the PRI gateway.
- You are setting up the FortiVoice phone system and locating the PRI gateway on a VPN. Therefore, the devices are not on the same LAN.

Procedure steps

1. Connect to the GUI of the FortiVoice phone system.
2. Go to **Managed System > Gateway**, and then click the **PRI Gateway** tab.
3. Click **New**.
4. Configure the following settings:

GUI field	Description
Enabled	Select to activate the configuration of the PRI gateway.
Name	Enter a unique name for the PRI gateway.
Display name	Not required. You can leave this field empty.
Hostname/IP address	Enter the hostname or IP address or hostname of the PRI gateway. If the PRI gateway is configured to use a non-default HTTPS port, then add :<port number> after the IP address. For example, 192.168.1.21:4430.

GUI field	Description
	Get Device Information: • Before you click this button, make sure to enter the required information in the **Admin user name** and **Admin password** fields below. • Click this button to poll the PRI gateway to get the serial number and the MAC address of the gateway. This action can confirm that the systems can communicate and that the password is valid. **Connect Device**: This procedure does not use this button. With this button, you would access the FortiVoice Gateway GUI in a separate tab in your web browser.
Admin user name	Enter the user name of the administrator account used for logging in to the PRI gateway. The default is admin.
Admin password	Enter the password associated with the Admin user name. To show the password, click the eye icon 👁. The default is no password.
Serial number	The serial number of the PRI gateway that you are adding to the FortiVoice phone system.
Type	The type of gateway that you are adding to the FortiVoice phone system.
MAC address	The MAC address of the PRI gateway that you are adding to the FortiVoice phone system.
Survivability branch	The FortiVoice LSG solution can support a FortiVoice PRI gateway at a branch office. To link this PRI gateway with a survivability branch, select that branch from the list. For details about deploying a FortiVoice LSG unit, see the FortiVoice Local Survivable Gateway Deployment Guide.
Physical location	Select **Internal** if the PRI gateway and FortiVoice phone system are on the same LAN. The PRI gateway connects to the internal IP address of the FortiVoice phone system. Select **External** if the PRI gateway connects to the FortiVoice phone system with an external IP.
Description	Optionally, add any applicable notes for this PRI gateway.

5. Click **Create**.
   The FortiVoice phone system creates a PRI trunk and one span (for FortiVoice Gateway GT01) or two spans (for FortiVoice Gateway GT02).
6. Reload your web-browser to make sure that the GUI displays the latest changes.
7. To review trunk details, go to **Trunk > Gateway**.
8. In the list, find the newly added gateway.
9. Verify that the **Status** column displays _In service_.
10. Double-click the newly added PRI gateway.

11. In the **Edit span** field, click **Edit** 🖉 .

12. Make sure that the **Advanced Options** are set to your service provider specifications.

13. For a FortiVoice Gateway GT02, repeat steps 11 and 12 for span 2.
    You have completed this procedure

14. Go to .

Applying the PRI gateway configuration

The FortiVoice phone system stores a gateway configuration file. Perform this procedure to apply the gateway configuration file to the PRI gateway.

Procedure steps

1. In the GUI of the FortiVoice phone system, go to **Managed System > Gateway**, and then click the **PRI Gateway** tab.

2. Review the list to find and select the gateway to which you want to apply the configuration file.

3. If you want to apply the configuration file to a single gateway:

   a. Click **Actions** > **Apply Configuration**.
   FortiVoice displays the following message:
   Do you want to update the selected gateway?

   b. Click **Yes**.

   FortiVoice applies configuration changes to the dial plan routes of the PRI gateway.

   With a successful update, the PRI gateway displays the following message:

   The gateway update is complete.

   <gateway_name>

   c. Click **OK**.

4. If you want to apply the configuration file to multiple gateways:

   a. Click **Actions** > **Start Config Job**.

   b. Select **All** or **Selected**.

   c. Enter the configuration job name and complete the job schedule.

   d. Click **Create**.

   e. Click **Go To Jobs** to view, delete, or stop the configuration job.
   You have completed this procedure.

5. Go to .

Verifying the PRI gateway configuration

Perform this procedure to verify that the SIP communication between the FortiVoice phone system and the PRI gateway is successful and that a PRI trunk exists between the PRI gateway and the public phone network.

Procedure steps

1. In the GUI of the FortiVoice gateway, go to **Gateway > SIP**.
2. Verify that the **Status** column shows *Unmonitored*.
3. Go to **Gateway > PRI**.
4. Verify that the **Status** column shows *In service*.
   You have completed this procedure.
5. Go to Adding a PRI gateway trunk to an inbound dial plan on page 18.

Adding a PRI gateway trunk to an inbound dial plan

Perform this procedure to add a PRI gateway trunk to an inbound dial plan. This plan defines the call flow for incoming calls to the FortiVoice phone system.

Procedure steps

1. In the GUI of the FortiVoice phone system, go to **Call Routing > Inbound**.
2. In the **Inbound** tab, click **New**.
3. Enter a unique name for this inbound dial plan.
4. In the **From Trunk** section, click the plus sign (+) and then select the entries that you want to add.
5. In the **Call Handling** section, update the settings to address your requirements for inbound call routing. You can select one of the following action types:
   - **Endpoint Action**: To handle incoming calls according to a specified action and an operation schedule, select this option. For example, send calls to the voicemail after business hours.
   - **Dial Local Number**: To send incoming calls to a local destination at any time, select this option. For example, enter 222xxxx as a pattern and strip 222. The FortiVoice phone system will only dial the last four digits for all called numbers matching this pattern.
   - **Call Routing**: To route incoming calls received by the FortiVoice phone system to an external phone system using an outbound dial plan, select this option.

   For more details, see the Configuring inbound dial plans section in the FortiVoice Phone System Administration Guide.
6. Click **Create**.
   You have completed this procedure.
7. Go to Adding a PRI gateway trunk to an outbound dial plan on page 18.

Adding a PRI gateway trunk to an outbound dial plan

Perform this procedure to add a PRI gateway trunk to an outbound dial plan. This plan defines the call flow for outgoing calls from the FortiVoice phone system.

Procedure steps

1. In the GUI of the FortiVoice phone system, go to **Call Routing > Outbound**.
2. Click **New**.
3. In the **Name** field, enter a unique name for this outbound dial plan.
4. To activate this plan, make sure that **Enable** is selected.
5. To allow emergency calls with this plan, select **Emergency Call**.

6. In **Caller ID Match**, you can edit or create a caller ID pattern.
   For details about caller ID patterns, see the Pattern-matching syntax section in the FortiVoice Phone System Administration Guide.
7. In **Dialed Number Match**, you can edit or create a phone number pattern.
   For details about adding a dialed number match, see the Creating dialed number match section in the FortiVoice Phone System Administration Guide.
8. In **Call Handling**, click **New**.
9. Configure the following settings:

GUI field	Description
Schedule	Select the FortiVoice operation schedule to implement this plan.
Action	Select the call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern.
	If you select *Allow with warning* or *Deny with warning*, then you set the warning details in the **Warning message** field.
Outgoing trunk	Select the gateway trunk to be used for outbound calls.
Caller ID modification	Optionally, select the caller ID modification configuration. This choice changes the phone number, caller name, or both that the FortiVoice phone system displays on the destination phone.
	For more details, see the Modifying caller IDs section in the FortiVoice Phone System Administration Guide.
Warning message	If you select *Allow with warning* or *Deny with warning*, in the **Action** field, then select the sound file for the warning. For details about sound files, see the Managing sound files and music on hold section in the FortiVoice Phone System Administration Guide.
Delay	If you want to discourage certain users from making outbound calls, enter the call delay time in seconds.

10. To save changes to the Call Handling section, click **Create**.
11. To save changes to the outbound call routing profile, click **Create**.
    You have completed this procedure and the deployment of the PRI gateway.
12. If you want to edit a trunk profile, go to Editing a trunk profile for a PRI gateway on page 19.
    If you want to create an additional trunk profile, make sure to free the span in the default trunk and then go to Creating an additional trunk profile for a FortiVoice Gateway GT02 on page 23.

Editing a trunk profile for a PRI gateway

To edit the trunk profile for a PRI gateway, perform this procedure.

Procedure steps

1. In the GUI of the FortiVoice phone system, go to **Trunk > Gateway**.
2. Double-click the profile that you want to edit.

3. The following tables include details about the gateway settings:

PRI gateway trunk options

GUI field	Description
Enabled	Select to activate this trunk profile.
Trunk gateway	The name of the PRI gateway. This field is read only.
Type	The gateway type. This field is read only.
Display name	Not required. You can leave this field empty.
Main number	Optionally, you can add a main number for reference. For example, you can use the number assigned by your service provider to identify the trunk.
Span	Click + to select the span and assign it to the trunk gateway. To edit settings of the PRI span, move your cursor to the **Span** field and click **Edit** ☑ . For details, see PRI gateway span options on page 20. The FortiVoice Gateway GT01 has one PRI port with one span. The FortiVoice Gateway GT02 has two PRI ports. Each PRI port has one span. By default, both spans are assigned to a single trunk.
Gateway device	The device type for this profile.
Caller ID modification	Optionally, select the caller ID modification configuration. This choice changes the phone number, caller name, or both that display on the destination phone. For more details, see the Modifying caller IDs section in the FortiVoice Phone System Administration Guide.
Description	Optionally, add notes for this trunk profile.

PRI gateway span options

GUI field	Description
Standard Options	
Name	The name of this span. This field is read only.
Type	Select PRI T1 or PRI E1.
Signaling	Select the PRI signaling: • PRI signaling, CPE (customer premises equipment) side • PRI signaling, network side • PRI R2 signaling - For more details about additional

GUI field	Description
	settings, see the PRI R2 Setting on page 22 section.
Advanced Options	
Framing and coding options	Specify the type of framing and coding to provision the PRI with your PSTN service provider.
Clocking options	Select the clock synchronization option for the FortiVoice phone system: • Clock sourcing from PSTN network • Internal clocking source This option setting does not need to match the one used by your PSTN service provider.
Receive sensitivity	Select the level of receiver sensitivity. This option allows the phone receiver to pick up the required level of phone signals and operate more efficiently. This option setting does not need to match the one used by your PSTN service provider.
D-channel signaling format	Select a signaling method for the D channel. This format carries the information needed to connect or disconnect calls and negotiate special calling parameters such as automatic number ID, call waiting, and data protocol. The D channel can also carry packet-switched data using the X.25 protocol.
Line build out	Select the line build out (LBO). Use LBO settings to adjust the output power of the transmission signal to achieve equal level point (ELP) at the DSX.
D-channel	Depending on your selection in **Type**, the default channel numbers are: • Full T1: 24 • Full E1: 16 Make sure to configure this setting to match the one used by your PSTN service provider.
B-channel	Depending on your selection in **Type**, the default channel numbers are: • Full T1: 1-23 • Full E1: 1-15, 17-31 You can also configure individual channels alongside channel ranges. For example, for T1/E1, the channels can be the following: • 1-12 • 2, 3, 4, 9-15

GUI field	Description
	• 2-4, 9-15 Make sure to configure this setting to match the one used by your PSTN service provider.
Dialplan type (TON)	Select a number format for placing a call from FortiVoice to the service provider. The values for this option are provided by the service provider. This option appears only if you select PRI signalling, CPE side or PRI signalling, network side for Editing a trunk profile for a PRI gateway on page 19.
Local dialplan type (TON)	Select a number format for placing a call from the service provider to FortiVoice. The values for this option are provided by the service provider. This option appears only if you select PRI signalling, CPE side or PRI signalling, network side for Editing a trunk profile for a PRI gateway on page 19.
Connected party notification dialplan Type (TON)	Select a number format used in caller-ID and remote party ID (if supported by the service provider). The values for this option are provided by the service provider. This option appears only if you select PRI signalling, CPE side or PRI signalling, network side for Editing a trunk profile for a PRI gateway on page 19.
PRI indication	Select a value that is typically provided by the service provider. However, some providers allow this value to be set on the PBX. • In Band: Call failure tones, for example, busy signal and out of service messages, are played back as audio from the service provider. • Out of Band: Call failure tones are generated by FortiVoice with the service provider sending a code instead of a tone. This is required for some automated dialing scenarios, but you will often lose extra information that may be included in the recorded message. This option appears only if you select PRI signalling, CPE side or PRI signalling, network side for Editing a trunk profile for a PRI gateway on page 19.
PRI R2 Setting	If you select PRI R2 signaling in the **Signaling** field, then this option is active. The PRI gateway supports many localized implementations of R2 signaling because there is no R2 signaling standard.

GUI field	Description
Country	Select the country for PRI R2 signaling settings.
Max ANI digits	Telephone companies use the automatic number identification (ANI) to identify the directory number (DN) of a calling subscriber. This number allows subscribers to capture or display a caller's telephone number. Enter the number of digits of a caller's phone number that the subscriber phone can capture or display.
Max DNIS digits	Telephone companies can provide a dialed number identification service (DNIS) that lets the receiver of a call know which number the caller has dialed. Enter the number of digits of a dialed call that the FortiVoice phone system sends to the telephone company.
Caller category	Select the caller type.
Incoming digits mode	Consult your telephone company about which incoming digits mode to select.
DTMF option	**DTMF dialing:** To allow dual-tone multi-frequency (DTMF) signaling, select this option. **DTMF answering:** To enable DTMF answering, select this option.
Allow collect calls	To allow a call to be billed to the called number, select this option.
MF timeout	To enable the multi-frequency (MF) timeout, enter a value in milliseconds. The default is -1, which disables the setting.
Metering pulse timeout	To enable the metering pulse timeout, enter a value in milliseconds. The default is -1, which disables the setting.

4. To save changes to the PRI gateway span (if applicable), click **OK**.
5. To save changes to the PRI gateway trunk, click **OK**.
6. Send the configuration changes to the PRI gateway by following the instructions in Applying the PRI gateway configuration on page 17.

Creating an additional trunk profile for a FortiVoice Gateway GT02

A FortiVoice Gateway GT02 has two spans, one for each PRI port. By default, both PRI spans are mapped to a single trunk. However, you can reassign a span to a second trunk, if required.

To create an additional trunk profile, perform this procedure.

Before you begin

> ⚠️ Before adding any span to a trunk, make sure to free the span in the default trunk. For more details, see Editing a trunk profile for a PRI gateway on page 19.

Procedure steps

1. In the GUI of the FortiVoice phone system, go to **Trunk > Gateway**.
2. Click **New**.
3. Configure the following settings:

GUI field	Description
Enabled	Select to activate this trunk profile.
Trunk gateway	Enter a unique name for this trunk profile.
Type	Select **PRI**.
Display name	Not required. You can leave this field empty.
Main number	Optionally, you can add a main number for reference. For example, you can use the number assigned by your service provider to identify the trunk.
Edit span	To edit settings of the PRI span, click **Edit** 📝 . For details, see PRI gateway span options on page 20.
Span	Make sure that the trunk profile is in the **Selected** list. If not, select the trunk profile in the **Available** list and click -> to move the trunk profile to the **Selected** list.
Gateway device	Select the device type for this profile.
Caller ID modification	Optionally, select the caller ID modification configuration. This choice changes the phone number, caller name, or both that display on the destination phone. For more details, see the Modifying caller IDs section in the FortiVoice Phone System Administration Guide.
Description	Optionally, add notes for this trunk profile.

4. To save changes to the PRI gateway span (if applicable), click **OK**.
5. To save changes to the PRI gateway trunk, click **Create**.
   You have completed this procedure.
6. Send the configuration changes to the PRI gateway by following the instructions in Applying the PRI gateway configuration on page 17.