FortiVoice Phone System - Administration Guide

Version 6.0.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FORTINET®

September 14, 2020
FortiVoice Phone System 6.0.2 Administration Guide
26-602-612335-20200914

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-03-19	Initial release of the FortiVoice Phone System 6.0.3 Administration Guide.
2020-09-14	Changed some of the master/slave terminologies (aside from the terms used in GUI) to primary and secondary.

Introduction

The FortiVoice Phone System enables you to completely control your organization’s telephone communications. Easy to use and reliable, the FortiVoice phone system delivers everything you need to handle calls professionally, control communication costs, and stay connected everywhere.

The FortiVoice system includes all the fundamentals of enterprise-class voice communications, with no additional cards to install. Auto attendants, voice messaging, ring groups, conferencing and much more are built-in. In addition, the FortiVoice personal web portal lets your staff view their call logs, configure and manage their own messaging, and access other features, such as the operator console and the agent console.

This document describes how to configure and use the FortiVoice phone system. Only the configuration procedures through the web-based manager are provided.

This topic includes:

- Registering your Fortinet product on page 10
- Training on page 11
- Documentation on page 11
- Scope on page 11
- Conventions on page 12

Registering your Fortinet product

Before you begin, take a moment to register your Fortinet product at the Fortinet Technical Support website.

Many Fortinet customer services, such as firmware updates and technical support, require product registration.

For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that you can install your Fortinet products quickly, configure them easily, and operate them reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support website.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article Technical Support Requirements.

Training

Fortinet Training Services provides classes that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services website or email them at training@fortinet.com.

Documentation

The Fortinet Technical Documentation website provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation website, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Base.

Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation website.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document to techdoc@fortinet.com.

Scope

This document describes how to connect the FortiVoice unit to its web-based manager and CLI and use the web-based manager to configure the FortiVoice unit.

This document does ***not*** cover commands for the command line interface (CLI).

Conventions

Fortinet technical documentation uses the following conventions:

- IP addresses on page 12
- Cautions and notes on page 12
- Typographical conventions on page 12

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets.

Cautions and notes

Fortinet technical documentation uses the following guidance and styles for cautions and notes.

Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Highlights useful additional information, often tailored to your workplace activity.

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Convention	Example
Button, menu, text box, field, or check box label	From *Minimum log level*, select *Notification*.

CLI input	`config system dns`
	`   set primary <address_ipv4>`
	`end`

CLI output	`FGT-602803030703 # get system Setting` `comments : (null)`

Convention	Example
	opmode : nat
Emphasis	HTTP connections are ***not*** secure and can be intercepted by a third party.
File content	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>
Hyperlink	Visit the Fortinet Technical Support website.
Keyboard entry	Type a name for the remote VPN peer or client, such as Central_Office_1.
Navigation	Go to *Monitor > Status > DHCP*.
Publication	For details, see the *FortiGate Administration Guide*.

Connecting to the FortiVoice System

After physically installing the FortiVoice unit, you need to connect to its management tools to configure, maintain, and administer the unit. You also need to inform your phone users on how to access the user web portal and use the FortiVoice features.

This topic includes:

- Connecting to the web-based manager or CLI on page 14
- Setting up the system on page 18
- Testing the setup on page 18
- Configuring setups for phone users on page 18

Connecting to the web-based manager or CLI

There are two methods to connect to the FortiVoice unit:

- use the web-based manager, a graphical user interface (GUI), from within a web browser
- use the command line interface (CLI), an interface similar to DOS or UNIX commands, from a Secure Shell (SSH) or Telnet terminal

Access to the CLI and/or web-based manager is not yet configured if:

- you are connecting for the first time
- you have just reset the configuration to its default state

In these cases, you must access either interface using the default Setting.

If the above conditions do not apply, access the web UI using the IP address, administrative access protocol, administrator account and password already configured, instead of the default Setting.

After you connect, you can use the web-based manager or CLI to configure basic network Setting and access the CLI and/or web-based manager through your network. However, if you want to update the firmware, you may want to do so before continuing. See System Information widget on page 21.

Until the FortiVoice unit is configured with an IP address and connected to your network, you may prefer to connect the FortiVoice unit directly to your management computer, or through a switch, in a peer network that is isolated from your overall network. However, isolation is not required.

This topic includes:

- Connecting to the web-based manager on page 15
- Connecting to the CLI on page 15

Connecting to the web-based manager

To connect to the web-based manager using its default Setting, you must have:

- a computer with an RJ-45 Ethernet network port
- a web browser such as Microsoft Internet Explorer version 6.0 or greater, or a recent version of Mozilla Firefox
- a crossover network cable

Default Setting for connecting to the web-based manager

Network interface	port1
URL	https://192.168.1.99/admin
Name	admin
Password	(none)

To connect to the web-based manager

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 with a netmask of 255.255.255.0.
2. Using the Ethernet cable, connect your computer's Ethernet port to the FortiVoice unit's port1.
3. Start your browser and go to https://192.168.1.99/admin.
   To support HTTPS authentication, the FortiVoice unit ships with a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiVoice unit. When you connect, depending on your web browser and prior access of the FortiVoice unit, your browser might 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 might 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 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 normal or not.

   Both warnings are normal for the default certificate.
4. 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.
5. In the *Name* field, type `admin`, then click *Login*. (In its default state, there is no password for this account.)
   Login credentials entered are encrypted before they are sent to the FortiVoice unit. If your login is successful, the web UI appears. To continue by updating the firmware, see System Information widget on page 21. Otherwise, to continue by following the configuration wizard.

Connecting to the CLI

Using its default Setting, you can access the CLI from your management computer in two ways:

- a local serial console connection
- an SSH connection, either local or through the network

To connect to the CLI using a local serial console connection, you must have:

- a computer with a serial communications (COM) port
- the RJ-45-to-DB-9 serial or null modem cable included in your FortiVoice package
- terminal emulation software, such as HyperTerminal for Microsoft Windows

To connect to the CLI using an SSH connection, you must have:

- a computer with an RJ-45 Ethernet port
- a crossover Ethernet cable
- an SSH client, such as PuTTY

Default Setting for connecting to the CLI by SSH

Network Interface	port1
IP Address	192.168.1.99
SSH Port Number	22
Name	admin
Password	(none)

If you are ***not*** connecting for the first time, nor have you just reset the configuration to its default state or restored the firmware, administrative access Setting may have already been configured. In this case, access the CLI using the IP address, administrative access protocol, administrator account and password already configured, instead of the default Setting.

The following procedure uses Microsoft HyperTerminal. Steps may vary with other terminal emulators.

To connect to the CLI using a local serial console connection

1. Using the RJ-45-to-DB-9 or null modem cable, connect your computer's serial communications (COM) port to the FortiVoice unit's console port.
2. Verify that the FortiVoice unit is powered on.
3. On your management computer, start HyperTerminal.
4. On *Connection Description*, enter a *Name* for the connection and select *OK*.
5. On *Connect To*, from *Connect using*, select the communications (COM) port where you connected the FortiVoice unit.
6. Select *OK*.
7. Select the following *Port* Setting and select *OK*.

Bits per second	9600
Data bits	8

Parity	None
Stop bits	1
Flow control	None

8. Press Enter.
   The terminal emulator connects to the CLI and the CLI displays a login prompt.
9. Type `admin` and press Enter twice. (In its default state, there is no password for this account.)
   The CLI displays a prompt, such as:
   FortiVoice #
10. Type `admin` and press Enter twice. (In its default state, there is no password for this account.)
   The CLI displays the following text:
   Type ? for a list of commands.
   You can now enter commands.

The following procedure uses PuTTy. Steps may vary with other SSH clients.

To connect to the CLI using an SSH connection

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 with a netmask of 255.255.255.0.
2. Using the Ethernet cable, connect your computer's Ethernet port to the FortiVoice unit's port1.
3. Verify that the FortiVoice unit is powered on.
4. On your management computer, start your SSH client.
5. In *Host Name (or IP Address)*, type `192.168.1.99`.
6. In Port, type `22`.
7. From *Connection type*, select *SSH*.
8. Select *Open*.
   The SSH client connects to the FortiVoice unit.
   The SSH client may display a warning if this is the first time you are connecting to the FortiVoice unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiVoice unit but it used a different IP address or SSH key. If your management computer is directly connected to the FortiVoice unit with no network hosts between them, this is normal.
9. Click *Yes* to verify the fingerprint and accept the FortiVoice unit's SSH key. You cannot log in until you accept the key.
   The CLI displays a login prompt.
10. Type `admin` and press Enter twice. (In its default state, there is no password for this account.)
   The CLI displays the following text:
   `Type ? for a list of commands.`
   You can now enter commands.

Setting up the system

You can follow this guide to set up the FortiVoice system. After the setup is complete, you can make phone calls through the FortiVoice unit.

Testing the setup

After completing the configuration, you can connect a SIP phone to your VoIP network and make an internal, external, or office peer test call.

If the SIP phone and the FortiVoice unit (PBX) are on different subnets, proper routing should be set to make them reachable

If you make a office peer test call, make sure that your FortiVoice unit and the peer office PBX are mutually registered. For more information, see Configuring office peers on page 201.

- Depending on the phone you use, the procedure to connect the phone may vary. Refer to the phone user manuals for instructions.
- Generally, you need to configure the following on the phone after powering it up and connecting it to the network:
- Enter the IP address of the phone if it is not DHCP-enabled.
- Enter the SIP server IP address and port number (5060 by default) of the FortiVoice unit.
- Enter the extension number and SIP password you have configured and make sure the extension is enabled.
  If you have not imported or added any extensions, do it first. For more information, see Configuring IP extensions on page 156. The extension number on the FortiVoice unit and your phone should match.

Configuring setups for phone users

The FortiVoice system provides a user web portal where phone users can view their call logs, configure and manage their own messaging, and access other features.

This section contains information that you may need to inform or assist your phone users so that they can use the FortiVoice features.

This information is ***not*** the same as what is included in the help for FortiVoice user web portal. It is included in this guide because:

- Phone users need to know how to access the FortiVoice user web portal and its online help.
- Phone users need to know the feature codes they can use on the phones.
- Phone users need to know how to change the voicemail password on the web portal and on the phone.
- Phone users may be confused if they try to enable a feature that you disabled (such as call waiting or do not disturb).
- You may need to tailor some information to your network or phone users.

This topic includes:

Accessing the user web portal

- FortiVoice user web portal is a special website located on a FortiVoice unit. This web portal allows a phone user to:
- Check your voicemail including playing, deleting, or saving the voicemails.
- Receive and send fax.
- Use the agent console to manage queue calls.
- Use the operator console to process company calls.
- Check your call record for received, placed, or missed calls.
- Check your recorded calls including playing, deleting, or saving the voicemails.
- View your corporate phone directory.
- Check the feature codes that you can dial on your phone keypad.
- Configure your extension according to your preferences.
- Manage calls.
- Configure phone profiles.
- Customize sound files.

Several modern, popular web browsers are supported, so you can use FortiVoice user web portal through the web browser of your choice.

For the phone user to access the web portal, you need to inform the phone user of:

- Web portal URL (same with that of the FortiVoice unit except without `/admin` in the end)
- user extension number
- default user PIN

With this information, a user can enter the URL in the browser's location or address bar. The user can then log into the portal using the extension number as user name and the user PIN as password.

Once they access the web portal, phone users can click the *Help* button to learn how to use the portal.

For information on adding extension numbers and user PINs, see Configuring IP extensions on page 156.

Changing the user PIN

Inform the phone users how to change the default user PIN on the phone. The information for changing the user PIN on the web portal is in the online help of the portal.

Receiving and sending fax

Inform the phone users that they can receive and send faxes on the user web portal. For more information, see Configuring fax on page 263.

Using the operator console

If you have enabled the operator role for an extension, inform the extension user so that the user can process corporate calls on the user web portal. For more information, see Operator Role on page 127.

Setting user privileges and preferences

The call features each phone user can use is controlled by the user privilege and preferences Setting associated with the user's extension. You may need to inform users of the features that they can use.

For information, see Configuring user privileges on page 126 and Setting extension user preferences on page 173.

Setting the feature codes

By default, the FortiVoice unit has feature codes for users to access certain features by dialing the codes. You can go to *Service* > *Feature Code* > *Feature Code* and double-click a feature name to modify its code and description, but that does not change the mapping between the code and the feature.

For details, see Modifying feature access codes on page 271.

Using the dashboard

Dashboard displays system statuses, most of which pertain to the entire system, such as CPU usage and mail statistics.

This section includes:

Viewing the dashboard

Dashboard > *Status* displays first after you log in to the web UI. It contains a dashboard with widgets that each indicate performance level or other statistics.

By default, widgets display the serial number and current system status of the FortiVoice unit, including uptime, system resource usage, license information, service status, firmware version, system time, and statistics history.

To view the dashboard, go to *Dashboard* > *Status*.

Hiding, showing and moving widget

The dashboard is customizable. You can select which widgets to display, where they are located on the tab, and whether they are minimized or maximized.

To move a widget, position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

To show or hide a widget select *Manage Widget* and then select the widgets you want displayed on the Dashboard. If the widget is greyed out, the widget will not display. Select *Apply* when you have made your selections.

Options vary slightly from widget to widget, but always include options to close, refresh, or minimize/maximize the widget.

System Information widget

The *System Information* widget displays the serial number and basic system statuses such as the firmware version, system time, and up time.

In addition to displaying basic system information, the *System Information* widget lets you change the firmware. To change the firmware, click *Update* for *Firmware version*. For more information, see Installing firmware on page 294.

To view the widget, go to *Status* > *Dashboard*. If the widget is not currently shown, click *Add Content*, and mark the check box for the widget.

License Information widget

The *License Information* widget displays the last queried license statuses for the number of extensions supported (if you use FortiVoice VM), hotel management, and call center (if you have purchased these options).

Depending on the license you have purchased, when you first access the FortiVoice web-based manager, you need to upload the license to enable the functions you need.

To upload the license file, first place the license file to your management computer, then click *Update license* and browse for the license file.

A full VMware license is required to upload a hotel management license onto the FortiVoice VM.

To view the widget, go to *Status* > *Dashboard*. If the widget is not currently shown, click *Add Content*, and mark the check box for the widget.

System Resource widget

The *System Resource* widget displays the CPU, memory, and disk space usage. It also displays the system load and current number of IP sessions.

To view the widget, go to *Status* > *Dashboard*. If the widget is not currently shown, click *Add Content*, and mark the check box for the widget.

The system resources history can also be viewed in this widget by clicking *History*. The system resources history contains four graphs. Each graph displays readings of one of the system resources: CPU, memory, IP sessions, and network bandwidth usage. Each graph is divided by a grid.

Statistics History widget

The *Statistics History* widget contains charts that summarize the number of calls in each time period that the FortiVoice unit recorded.

To view the widget, go to *Status* > *Dashboard.* If the widget is not currently shown, click *Add Content*, and mark the check box for the widget.

Also see Viewing Call Statistics on page 23.

Service Status widget

The *Service Status* widget displays the number of current calls, extension status, trunk status, and device connection status.

To view the widget, go to *Status* > *Dashboard*. If the widget is not currently shown, click *Add Content*, and mark the check box for the widget.

Device (200D-T and 2000E-T2 models only) displays the connection status of the FortiVoice physical ports:

- *Connected*: The port is connected to a device.
- *Disconnected*: The port is not connected to any device and is ready for use.

- *Alarmed*: The port has an error and is not usable.
- *Occupied*: The port is being used.

Recent Calls widget

The *Recent Calls* widget displays the calls processed by the FortiVoice unit, including phone numbers, call directions, call starting time and duration, and call status.

To view the widget, go to *Status* > *Dashboard*. If the widget is not currently shown, click *Add Content*, and mark the check box for the widget.

The maximum call records shown is 8.

Viewing Call Statistics

The *Dashboard* > *Call Statistics* tab contains summaries of the number of calls by time and direction that the FortiVoice unit recorded.

Using the CLI Console

Go to *Dashboard* > *Console* to access the CLI without exiting from the web UI.

You can click the *Open in New Window* button at the bottom of the page to move the CLI Console into a pop-up window that you can resize and reposition.

Monitoring the FortiVoice System

The *Monitor* menu displays system usage, log messages, reports, and other status-indicating items.

This topic includes:

Viewing phone system status

Monitor > Phone System displays all the ongoing phone calls, parked calls, conference calls, trunks, and DHCP clients.

This topic includes:

Viewing active calls

Monitor > Phone System > Active Calls displays all the ongoing phone calls in realtime, including the callers and receivers, the trunks through which phone calls are connected, the call status, and the call duration.

You can stop a phone call by clicking the *Hang up* icon.

The call statuses include:

- *Ringing*: The receiver's phone is ringing.
- *Connected*: Callers are connected. The voice channel is established.
- *Voicemail*: The call goes to the voicemail.

Viewing parked calls

A parked call is similar to a call that is on hold, except that the parked call can then be picked up from any extension.

To view parked calls, go to *Monitor > Phone System > Parked Call.*

For more information on call parking, see Configuring call parking on page 262.

Viewing conference calls

Monitor > Phone System > Conference displays the conference call records, including the name of the conference call, the extension number of the call, the displayed name of the caller, and the call duration.

You can stop a caller from attending the conference call by selecting the caller and clicking the *Kick Out* icon.

For more information, see Configuring conference calls on page 256.

Viewing trunk status

Monitor > Phone System > Trunk displays all the trunks in realtime, including their names, IP addresses, types, status, and registration/connection status with the VoIP or PSTN service provider.

The trunk statuses include:

- *Not registered*: The trunk is not registered with the VoIP or PSTN service provider and is not in service.
- *In service*: The trunk is registered with the VoIP or PSTN service provider and is in service.
- *Unavailable*: The trunk is not reachable.
- *Alarm detected*: There is a problem with the trunk.
- *Admin down*: The trunk is disabled.
- *Unmonitored*: The trunk is not monitored.

Registration/Connection indicates if a trunk has been registered with or connected to the VoIP or PSTN service provider.

You can stop a phone call by clicking the *Hang up* icon.

For more information, see Configuring Trunks on page 190.

Viewing DHCP client list

Monitor > Phone System > DHCP displays all the DHCP-enabled devices connected to the FortiVoice unit in realtime.

Once a DHCP-enabled phone connects to the FortiVoice unit and is auto-discovered, the FortiVoice unit assigns an IP address to the phone and sends the basic PBX setup information to it.

For the supported DHCP-enabled phone to connect to the FortiVoice unit:

- In the FortiVoice DHCP server configuration, select DHCP option 66 (an advanced option on the web-based manager) and include the IP address of the FortiVoice interface connected to the same network as the SIP phones to be auto-provisioned. For more information, see Configuring DHCP server on page 44.
  DHCP server option 66 identifies a TFTP server and includes the IP address of the TFTP server and downloads the TFTP server identity to the device that gets an IP address from the DHCP server. DHCP option 66 is defined in RFC 2132.
- If using your own DHCP server, set the DHCP server option 66 to the FortiVoice unit's *TFTP server (Opt66)* value. For more information, see Configuring DHCP server on page 44.
- If the FortiVoice unit and the SIP phone with an IP assigned by a DHCP server are on different subnets, proper route should be set to make them reachable.

GUI field	Description
Export	Select to save the DHCP client list in `csv` format.
MAC	The Media Access Control address (MAC address) of the DHCP client.
Interface	The FortiVoice unit port to which the DHCP client connects. For information on FortiVoice interfaces, see Configuring network settings on page 37.
IP	The IP address of the DHCP client assigned by the FortiVoice DHCP server.
Expiry Time	The expiration time of the DHCP client IP address.
Device Type	The brand names of the DHCP clients.
Extension	When a DHCP-enabled device connects to the FortiVoice unit, the FortiVoice unit assigns a temporary ID to the device if it is a supported device. If an extension number is assigned to the phone, the extension number appears. For information on assigning extensions, see Viewing desktop FortiFones on page 27.
Configuration Status	• *OK*: The DHCP client is assigned to a new or an existing extension user. • *Not assigned*: The DHCP client is not assigned to a new or an existing extension user. • *Misconfigured*: The DHCP client's configuration has errors.

Viewing extensions and devices

Monitor > Extension & Device displays all the extensions, the extensions configured for hot desking, desktop FortiFones, software FortiFones, and generic SIP phones.

This topic includes:

Viewing extension status

Monitor > Extension & Device > Extension displays all the extensions in realtime, including their statuses, IDs, numbers, display names, types, IPs for SIP extensions, phone information, and if it has any auxiliary devices.

For more information, see Configuring Extensions on page 156.

Viewing desktop FortiFones

Monitor > Extension & Device > Desktop FortiFone lists the supported phones auto-discovered by the FortiVoice unit, assigned or not assigned to any extensions.

Once an unassigned phone connects to the FortiVoice unit and is auto-discovered, the FortiVoice unit assigns an IP address to the phone and sends the basic PBX setup information to it.

After assigning an extension to the phone, the extension's full configuration file will be sent to the phone if the auto-provisioning option is selected in the user privilege applied to the extension. For details, see Setting up local extensions on page 156 and Configuring user privileges on page 126.

GUI field	Description
New	Click to add a new desktop FortiFone. For details, see Configuring desktop FortiFones on page 132.
Delete	Select one or more SIP phone records and click this button to remove them all at once.
Action	• *Assign to New Extension*: Select a SIP phone in *Not Assigned* status and click this option to add an extension and assign this phone to the extension at the same time. For more information, see To assign a new extension user to an unassigned phone on page 28. • *Assign to Existing Extension:* Select an unassigned phone and click this option to assign this phone to an existing extension. The phone record disappears from the *Unassigned Phone* list. For more information, see To assign a new extension user to an unassigned phone on page 28. • *Assign to Multi-cell Device*: Select a multi-cell device (for example, FortiFone 870i) in *Not Assigned* status and click this option to add an extension and assign this phone to the extension at the same time. For more information, see To assign a new extension user to an unassigned phone on page 28 and Configuring FortiFone-870i on page 134. • *Assign as Auxiliary to Existing Extension:* Select a SIP phone in *Not Assigned* status and click this option to assign it to an existing extension as an auxiliary device. For more information, see To assign a new extension user to an unassigned phone as an auxiliary device on page 28and Auxiliary Device on page 160. • *View Phone Configuration*: Select a SIP phone in *Assigned* status and click this option display its configuration file. • *Export*: The name displaying on the gateway, such as ABC Company Gateway.
MAC Address	The Media Access Control address (MAC address) of the SIP phone.
Phone Model	The phone brand and model.
User	The user associated with the phone.
Number	The extension number of the phone.
Display Name	The name displaying on the phone, such as John Doe.
IP	The IP address of the phone assigned by the FortiVoice unit.
Phone Info	The model, MAC address, and firmware version of the phone for this extension.

GUI field	Description
Phone Profile	The profile for this phone. See Configuring SIP profiles on page 115.
Management	Displays if the phone has been assigned to an extension.
Description	Any notes about the phone.
Status	Displays if the phone is registered with the FortiVoice unit. A registered phone is assigned an IP address and basic PBX setup information.
Role	Shows if the device is used for phone calls or as an auxiliary device.

To assign a new extension user to an unassigned phone

1. Go to *Monitor* > *Extension & Device* > *Desktop FortiFone*.
2. Select a phone in *Not assigned* status.
3. Click *Action* and select *Assign to New Extension.*
4. Review the extension details and click *Next*. For details, see Configuring IP extensions on page 156.
5. Review the phone details and click *Next*.
6. Review the summary and click *Finish*.

To assign an existing extension user to an unassigned phone

1. Go to *Monitor* > *Extension & Device* > *Desktop FortiFone*.
2. Select a phone in *Not assigned* status.
3. Click *Action* and select *Assign to Existing Extension.*
4. Select the extension to associate with the unassigned phone and click *Next*.
5. Review the extension details and click *Next*. For details, see Configuring IP extensions on page 156.
6. Review the phone details and click *Next*.
7. Review the summary and click *Finish*.

To assign a new extension user to an unassigned phone as an auxiliary device

1. Go to *Monitor* > *Extension & Device* > *Desktop FortiFone*.
2. Select a phone in *Not assigned* status.
3. Click *Action* and select *Assign as Auxiliary to Existing Extension.*
4. Select the extension to associate with the unassigned phone and click *Next*.
5. Review the extension details and click *Next*. For details, see Configuring IP extensions on page 156.
6. Review the phone details and click *Next*.
7. Review the summary and click *Finish*.

Viewing software FortiFones

Monitor > *Extension & Device* > *Software FortiFone* lists the software FortiFones auto-discovered by the FortiVoice unit.

Viewing generic SIP phones

Monitor > Extension & Device > Generic SIP Phone lists the third party SIP phones auto-discovered by the FortiVoice unit.

Viewing activity details of hot desking extensions

Monitor > Extension & Device > Hot Desking displays details of hot desking users, including:

- *Logout*: Click to log out a Hot-Desked phone
- *Renew*: Click to refresh the expiration of the hot desk session.
- *Status*:The status of the hot desking extension: logged in or logged out.
- *Number*: The hot desking extension number.
- *Display Name*: The name displayed on the hot desking extension.
- *Host Device*: The extension number or MAC address (for a unassigned phone) of the phone that a hot desking user logs into.
- *Last Login*: The last login time at the host device.
- *Expiry*: The login expiry time.

Hot desking enables users to log into another phone. However, unlike using Follow Me or Call Forwarding which simply redirect a user's calls to another user's phone, hot desking takes total control of another phone by applying all of the user's own phone Setting to that phone until the user logs out. Each user can log into another phone by pressing *11 and enter his extension number and user PIN following the prompts. To log out, a user can press *12.

Depending of the phone model, the host phone may reboot.

For information on configuring hot desking, see Hot-desking on page 129.

Viewing unmanaged gateways

Monitor > Extension & Device > Unmanaged Gateway lists the supported FortiVoice gateways auto-discovered by the FortiVoice unit but not added to the FortiVoice unit.

Once a gateway connects to the FortiVoice unit and boots up, it will automatically discover the FortiVoice unit through SIP PNP.

After adding a FortiVoice gateway to the FortiVoice unit, the gateway's full configuration file will be sent to the gateway. For details, see Managing FortiVoice Gateways, Local Survivability, and Firmwares on page 136.

GUI field	Description
Action	• *Create New Device*: Select an unmanaged gateway and click this option to add the gateway to the FortiVoice unit. The gateway record disappears from the *Unmanaged Gateway* list. For more information, see To add a gateway to the FortiVoice unit on page 30 • *Replace Existing Device:* If you need to replace a gateway for any reason, select the gateway and click this option to find a new gateway for replacement. For more information, see To replace an existing gateway on page 30.
Serial number	The serial number of the unmanaged gateway.

GUI field	Description
Type	The gateway brand and model.
IP	The IP address of the unmanaged gateway assigned by the FortiVoice unit.

To add a gateway to the FortiVoice unit

1. Go to *Monitor* > *Extension & Device* > *Unmanaged Gateway*.
2. Select an unmanaged gateway.
3. Click *Action* and select *Create New Device.*

GUI field	Description
Gateway	
Name	Enter a unique name for the gateway.
Enabled	Select to activate the gateway if required.
Display Name	The name displaying on the gateway, such as ABC Company Gateway.
Hostname/IP address	Enter the hostname or IP address of LAN1 of the gateway. If you are using a different network interface, enter its IP. If the gateway has been configured to use a different HTTPS port, enter the port number after the IP address. • *Get device information*: Click to get the serial number, device type, and Mac address of the gateway. This will confirm the systems are able to communicate with each other and that the password entered is valid. If preconfiguring the system before deployment, manually enter in the serial number and MAC address of the gateway. • *Connect Device*: Click to go to the Web GUI of the gateway.
Admin user name	Enter the user name for logging into the gateway.
Admin password	Enter the password for logging into the gateway. If you want to change the administrator password for logging into the gateway, click *Change password*, enable and enter the new password, confirm it, and click *OK*.
Serial number	The serial number of the gateway.
Type	Select the gateway brand and model.
MAC address	Enter the Mac address of the gateway.
Description	Enter any comments for the gateway.

4. Click *Finish*.

To replace an existing gateway

1. Go to *Monitor* > *Phone System* > *Unmanaged Gateway*.
2. Select the gateway to be replaced.
3. Click *Action* and select *Replace existing device.*
4. Select a new device to replace the old one.

5. Click *Next.*
6. Click *Close*.

Viewing call records

Monitor > *Call History* > *Call Detail Record* (CDR) displays all the phone calls made during a certain time period, including time of the call, caller and receiver, call duration, call status, call direction, trunks used, call type, and call recordings.

Double-clicking a record displays the detailed call information, including the CDR flow.

Using the *More Action* dropdown list, you may select a caller or callee and add them to your contact list or block them.

You can filter the call records display by clicking the *Search* button and enter criteria that records must match in order to be visible. You can also save the call records by selecting an option under *Download*. If you enable *With call flow*, you can download call records with detailed call flow information.

Viewing generated reports

Monitor > *Call Report Report* tab displays the call reports and call center reports generated by the FortiVoice unit. You can delete, view, and/or download generated reports.

FortiVoice units can generate reports automatically according to the report schedules that you configure. For more information, see Configuring call center report profiles and generating reports on page 239.

To reduce the amount of hard disk space consumed by reports, regularly download then delete generated reports from the FortiVoice unit.

To view call or call center reports

1. Go to *Monitor > Call Report> Report/Call Center Report*.

GUI field	Description
Download	Click to create a PDF or HTML version of the report.
Directory	Lists the name of the generated report, and the date and time at which it was generated. For example, `Report 1-2012-03-31-2112` is a report named Report 1, generated on March 31, 2012 at 9:12 PM. To view an individual section of the report in HTML format, click + next to the report name to expand the list of HTML files that comprise the report, then double-click one of the file names.
Last Access Time	Lists the date and time when the FortiVoice unit completed the generated report.
Size	Lists the file size of the report in HTML format, in bytes.

2. To view the report in PDF file format, select a report and click *Download.* On the pop-up menu, select *Download PDF*.
3. To view the report in HTML file format, you can view all sections of the report together, or you can view report sections individually.
   - To view **all** report sections together, select a report, such as `2012-03-31-2112`, then click *Download* and select *Download HTML*. Your browser downloads a file with an archive (`.tgz.gz`) file extension to your management computer. To view the report, first extract the report files from the archive, then open the HTML files in your web browser.
   - Each *Query Selection* in the report becomes a separate HTML file. You can view the report as individual HTML files. In the row corresponding to the report that you want to view, click + next to the report name to expand the list of sections, then double-click the file name of the section that you want to view, such as `report1.html`. The report appears in a new browser window.
4. To view the report in CSV (comma-separated value) file format that can be viewed in a spreadsheet application such as Microsoft Excel or OpenOffice Calc, select a report and click *Download.* On the pop-up menu, select *Download CSV*.

Viewing log messages

The *Log* submenu displays locally stored log files. If you configured the FortiVoice unit to store log messages locally (that is, to the hard disk), you can view the log messages currently stored in each log file.

Logs stored remotely cannot be viewed from the web-based manager of the FortiVoice unit. If you want to view logs from the web-based manager, also enable local storage. For details, see Configuring Logs and Reports on page 278.

Monitor > Log displays the logs of administrator activities and system events as well as mail, voice, fax, queue, hotel management (with license only), and call center (with license only).

The log messages vary by levels. For more information, see Configuring Logs and Reports on page 278.

The log messages are also filtered by subtypes:

- *Configuration*: Display only log messages containing `subtype=config`.
- *Administration*: Display only log messages containing `subtype=admin`.
- *System*: Display only log messages containing `subtype=system`.

- *HA*: Display only log messages containing `subtype=ha`.
- *DHCP*: Display only log messages containing `subtype=dhcp`.

To view the list of log files and their contents

1. Go to *Monitor* > *Log* > *System/Generic/Voice/Fax*/*Queue/Hotel/Call Center*.
   The list of log files appears with the beginning and end of a log file's time range and the size of a log file in bytes. The queue log files display more information.
2. To search the log files, click the *Search* button and enter criteria that records must match in order to be visible. Unlike the search when viewing the contents of an individual log file, this search displays results regardless of which log file contains them. For more information, see Searching log messages on page 34.
3. To view messages contained in logs, double-click a log file.
   To view the current page's worth of the log messages, right-click and select *Export*. You can then open or save the .csv file.

   You can click the *Configure View* icon to show or hide columns, save the customized view, or reset the view to default. When you save a customized view, future log message reports appear in this view.

Displaying and arranging log columns

When viewing logs, you can display, hide, sort and re-order columns.

For most columns, you can also filter data within the columns to include or exclude log messages which contain your specified text in that column. For more information, see Searching log messages on page 34.

By default, each page's worth of log messages is listed with the log message with the lowest index number towards the top.

To sort the page's entries in ascending or descending order

1. Click the column heading by which you want to sort.
   The log messages are sorted in ascending order.
2. To sort in descending order, click the column heading again.
   Depending on your currently selected theme:
   - The column heading may darken in color to indicate which column is being used to sort the page.
   - A small upwards-or downwards-pointing arrow may appear in the column heading next to its name to indicate the current sort order.

To display or hide columns

1. Go to *Monitor* > *Log* > *System /Generic/Voice/Fax*/*Queue/Hotel/Call Center*.
2. Click *Configure View* > *Show/Hide Columns*.
3. Mark the check boxes of columns that you want to display.
4. Click *OK*.

To change the order of the columns

1. Go to *Monitor* > *Log* > *System /Generic/Voice/Fax*/*Queue/Hotel/Call Center.*
2. For each column whose order you want to change, click and drag its column heading to the left or right.
3. Click *Configure View* > *Save View*.

Using the right-click pop-up menus

When you right-click on a log message, a context menu appears.

Log report right-click menu options

View Details	Select to display the content of the log message.
Select All	Select to select all log messages in the current page, so that you can export all messages to a table.
Clear Selection	Select to deselect one or multiple log messages.
Export	Select to export the selected log messages as a .csv file.

Searching log messages

You can search logs to quickly find specific log messages in a log file, rather than browsing the entire contents of the log file.

To search log messages

1. Go to *Monitor* > *Log* > *System/Generic/Voice/Fax/Queue/Hotel/Call Center*.
2. Click *Search*.
3. Enter your search criteria by configuring one or more of the following:

GUI field	Description
Keyword	Enter any word or words to search for within the log messages. For example, you might enter `GUI session` to locate all log messages containing that exact phrase in any log field.
Message	Enter all or part of the *Message* log field.
Log ID	Enter all or part of the log ID in the log message.
Match condition	• *Contain*: searches for the exact match. • *Wildcard*: supports wildcards in the entered search criteria.
Date	Select the start and end time of log messages to include in the search results.
Time span	Select the time span of log messages to include in the search results. For example, you might want to search only log messages that were recorded during the two weeks and 8 hours previous to the current date. In that case, you would specify the current date, and also specify the size of the span of time (two weeks and 8 hours) before that date.
Load Previous Setting	Select to populate the fields with the Setting entered previously.

4. Click *Search*.
   The FortiVoice unit searches for log messages that match your search criteria, and displays any matching log messages.

Viewing call directory

The *Monitor* > *Directory* menu lets you view phone directories. For more information, see Creating contacts.

Blocking SIP device IPs

The FortiVoice unit automatically blocks the IP addresses of the SIP devices that initiate the attacks against any extensions based on the thresholds and parameters set. For more information on configuring security Setting, see Configuring intrusion detection on page 152.

You may select an IP to delete it, add it to the exempt list if it is wrongly blocked, and view its blocked history.

To view the blocked IPs, go to *Monitor* > *Security* > *Blocked IP.*

Viewing call/fax storage

Monitor > *Storage* displays the recorded calls, faxes, archived faxes, and faxes in queue.

This topic includes:

Playing recorded calls

The *Recorded Call* tab lists the calls recorded by the FortiVoice unit.

To listen to a call, go to *Monitor* > *Storage* > *Recorded Call* and double-click a call record folder to open the archived call files. Select a call file and click the *Play* button.

To save a recorded call, go to *Monitor* > *Storage* and select a call record folder to open the archived call files. Select a call file and click the *Download* button.

For information on configuring recording calls, see Recording calls on page 258.

Viewing current fax accounts

The *Fax* tab lists the fax accounts created on the FortiVoice unit. For more information about creating fax accounts, see Configuring fax on page 263.

To view fax accounts, go to *Monitor* > *Storage* > *Fax.* The fax accounts are listed with their names, numbers, display names, storage sizes, and faxes stored.

You can double-click a fax account and view the detailed information on the faxes it stores. You can also click *Download PDF* to save a fax.

Viewing archived faxes

The *Fax Archive* tab lists the faxes sent and received through the FortiVoice unit. For more information about fax, see Configuring fax on page 263.

To view archived faxes, go to *Monitor > Storage > Fax Archive.*

You can double-click a fax folder and view the detailed information on the faxes it stores.

Viewing fax queues

The *Fax Queue* tab lists the faxes waiting to be sent on the FortiVoice unit. For more information about fax, see Configuring fax on page 263.

Configuring System Setting

The *System* menu lets you set up configurations of the FortiVoice operation system, including administrator accounts, network Setting, system time, SIP Setting, system maintenance, and more.

This topic includes:

Configuring network settings

The *Network* submenu provides options to configure network connectivity and administrative access to the web-based manager or CLI of the FortiVoice unit through each network interface.

This topic includes:

About IPv6 Support

IP version 6 (IPv6) handles issues that were not around decades ago when IPv4 was created such as running out of IP addresses, fair distributing of IP addresses, built-in quality of service (QoS) features, better multimedia support, and improved handling of fragmentation. A bigger address space, bigger default packet size, and more optional header extensions provide these features with flexibility to customize them to any needs.

IPv6 has 128-bit addresses compared to IPv4's 32-bit addresses, effectively eliminating address exhaustion. This new very large address space will likely reduce the need for network address translation (NAT) since IPv6 provides more than a billion IP addresses for each person on Earth. All hardware and software network components must support this new address size, an upgrade that may take a while to complete and will force IPv6 and IPv4 to work side-by-side during the transition period.

The FortiVoice unit supports the following IPv6 features:

- Network interface
- Network routing
- DNS
- DHCP
- Phone extension
- Trunk

About the management IP

The FortiVoice unit has an IP address for administrators to configure it through a network connection rather than a local console. The management IP address enables administrators to connect to the FortiVoice unit through *port1* or other network ports, even when they are currently bridging.

By default, the management IP address is indirectly bound to *port1* through the bridge. If other network interfaces are also included in the bridge with *port1*, you can configure the FortiVoice unit to respond to connections to the management IP address that arrive on those other network interfaces.

You can access the web-based manager and the FortiVoice user account using the management IP address. For details, see Connecting to the web-based manager on page 15.

About FortiVoice logical interfaces

In addition to the FortiVoice physical interfaces, you can create the following types of logical interfaces on the FortiVoice unit:

- VLAN subinterfaces on page 38
- Redundant interfaces on page 39
- Loopback interfaces on page 39

VLAN subinterfaces

A Virtual LAN (VLAN) subinterface, also called a VLAN, is a virtual interface on a physical interface. The subinterface allows routing of VLAN tagged packets using that physical interface, but it is separate from any other traffic on the physical interface.

Virtual LANs (VLANs) use ID tags to logically separate devices on a network into smaller broadcast domains. These smaller domains forward packets only to devices that are part of that VLAN domain. This reduces traffic and increases network security.

One example of an application of VLANs is a company’s accounting department. Accounting computers may be located at both main and branch offices. However, accounting computers need to communicate with each other frequently and require increased security. VLANs allow the accounting network traffic to be sent only to accounting computers and to connect accounting computers in different locations as if they were on the same physical subnet.

For information about adding VLAN subinterfaces, see Configuring the network interfaces on page 39.

Redundant interfaces

On the FortiVoice unit, you can combine two or more physical interfaces to provide link redundancy. This feature allows you to connect to two or more switches to ensure connectivity in the event one physical interface or the equipment on that interface fails.

In a redundant interface, traffic is only going over one interface at any time. This differs from an aggregated interface where traffic is going over all interfaces for increased bandwidth. This difference means redundant interfaces can have more robust configurations with fewer possible points of failure. This is important in a fully-meshed high availability (HA) configuration.

A physical interface is available to be in a redundant interface if:

- it is a physical interface, not a VLAN interface
- it is not already part of a redundant interface
- it has no defined IP address and is not configured for DHCP
- it does not have any VLAN subinterfaces
- it is not monitored by HA

When a physical interface is included in a redundant interface, it is not listed on the *System* > *Network* > *Network* page. You cannot configure the interface anymore.

For information about adding redundant interfaces, see Configuring the network interfaces on page 39.

Loopback interfaces

A loopback interface is a logical interface that is always up (no physical link dependency) and the attached subnet is always present in the routing table.

The FortiVoice’s loopback IP address does not depend on one specific external port, and is therefore possible to access it through several physical or VLAN interfaces. In the current release, you can only add one loopback interface on the FortiVoice unit.

For information about adding a loopback interface, see Configuring the network interfaces on page 39.

Configuring the network interfaces

The *System* > *Network* > *Network* tab displays the FortiVoice unit’s network interfaces.

You must configure at least one network interface for the FortiVoice unit to connect to your network. Depending on your network topology and other considerations, you can connect the FortiVoice unit to your network using two or more of the network interfaces. You can configure each network interface separately. You can also configure advanced interface options, including VLAN subinterfaces, redundant interfaces, and loopback interfaces. For more information, see About FortiVoice logical interfaces on page 38, and Editing network interfaces on page 40.

To view the list of network interfaces, go to *System* > *Network* > *Network*.

GUI field	Description
Name	Displays the name of the network interface, such as *port1*.

GUI field	Description
Type	Displays the interface type: physical, VLAN, redundant, or loopback. For details, see About FortiVoice logical interfaces on page 38.
IP/Netmask	Displays the IP address and netmask of the network interface.
IPv6/Netmask	Displays the IPv6 address and netmask of the network interface. For more information about IPv6 support, see About IPv6 Support on page 37.
Access	Displays the administrative access and phone user access that are enabled on the network interface, such as HTTPS for the web-based manager.
Status	Indicates the **up** (available) or **down** (unavailable) administrative status for the network interface. • *Green up arrow*: The network interface is up and can receive traffic. • *Red down arrow*: The network interface is down and cannot receive traffic. To change the administrative status (that is, bring up or down a network interface), see Editing network interfaces on page 40.

Editing network interfaces

You can edit FortiVoice's physical network interfaces to change their IP addresses, netmasks, administrative access protocols, and other Setting. You can also create or edit logical interfaces, such as VLANs, redundant interfaces and the loopback interface.

Enable administrative access only on network interfaces connected to trusted private networks or directly to your management computer. If possible, enable only secure administrative access protocols such as HTTPS or SSH. Failure to restrict administrative access could compromise the security of your FortiVoice unit.

You can restrict which IP addresses are permitted to log in as a FortiVoice administrator through network interfaces. For details, see Configuring administrator accounts on page 46.

To create or edit a network interface

1. Go to *System* > *Network* > *Network*.
2. Double-click a network interface to modify it or select the interface and click *Edit*. If you want to create a logical interface, click *New*.
   The *Edit Interface* dialog appears.
3. Configure the following:

GUI field	Description
Interface Name	If you are editing an existing interface, this field displays the name (such as port2) and media access control (MAC) address for this network interface. If you are creating a logical interface, enter a name for the interface.

GUI field	Description
Type	If you are creating a logical interface, select which type of interface you want to create. For information about logical interface types, see About FortiVoice logical interfaces on page 38. • *VLAN*: If you want to create a VLAN subinterface, select the interface for which you want to create the subinterface. Then specify a VLAN ID. Valid VLAN ID numbers are from 1 to 4094, while 0 is used for high priority frames, and 4095 is reserved. • *Redundant*: If you want to create a redundant interface, select the interface members from the available interfaces. Usually, you need to include two or more interfaces as the redundant interface members. • *Loopback*: If you want to add a loopback interface, select the Loopback type and the interface name will be automatically reset to “loopback”. You can only add one loopback interface on the FortiVoice unit.
Addressing Mode	• *Manual*: Select to enter the IP address or IPv6 address and netmask for the network interface in *IP/Netmask* or *IPv6/Netmask*. • *DHCP*: Select and click *Update request* to retrieve a dynamic IP address using DHCP.
Advanced Setting	
Access	Enable protocols that this network interface should accept for connections **to** the FortiVoice unit itself. (These options do not affect connections that will travel **through** the FortiVoice unit.) • *HTTPS*: Enable to allow secure HTTPS connections to the web-based manager, and extension user account through this network interface. • *HTTP*: Enable to allow HTTP connections to the web-based manager, and extension user account through this network interface. • *PING*: Enable to allow ICMP ECHO (ping) responses from this network interface. • *SSH*: Enable to allow SSH connections to the CLI through this network interface. • *SNMP*: Enable to allow SNMP connections (queries) to this network interface. For information on further restricting access, or on configuring the network interface that will be the source of traps, see Configuring the network interfaces on page 39. • *TELNET*: Enable to allow Telnet connections to the CLI through this network interface. • *TFTP*: Enable to allow TFTP connections to this network interface. • *NTP:* Enable to allow SIP phones to connect to this server to synchronize time. • *LDAP*: Enable to allow SIP phones to connect to this server to retrieve phone directories. • *SIPPnP*: Enable SIPPnP multicast function for the connected phones to find the provisioning server contained in its message for the phones. • *MDNS*: Enable MDNS multicast function for the connected phones to find the TFTP provisioning server contained in its message for the

GUI field	Description
	phones. This is mainly for backward support of legacy FortiFones. HTTP and Telnet connections are **not** secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiVoice unit. For information on further restricting access of administrative connections, see Configuring administrator accounts on page 46.

	• *MTU*:Enable to change the maximum transmission unit (MTU) value, then enter the maximum packet or Ethernet frame size in bytes.
	If network devices between the FortiVoice unit and its traffic destinations require smaller or larger units of traffic, packets may require additional processing at each node in the network to fragment or defragment the units, resulting in reduced network performance. Adjusting the MTU to match your network can improve network performance.
	The default value is 1500 bytes. The MTU size must be between 576 and 1500 bytes. Change this if you need a lower value; for example, RFC 2516 prescribes a value of 1492 for the PPPoE protocol.
	• *Administrative status*: Select either:
	  ◦ *Up*: Enable (that is, bring up) the network interface so that it can send and receive traffic.
	  ◦ *Down*: Disable (that is, bring down) the network interface so that it cannot send or receive traffic.

Configuring static routes

The *System* > *Network* > *Routing* tab displays a list of routes and lets you configure static routes and gateways used by the FortiVoice unit.

Static routes direct traffic exiting the FortiVoice unit. You can specify through which network interface a packet will leave, and the IP address of a next-hop router that is reachable from that network interface. The router is aware of which IP addresses are reachable through various network pathways, and can forward those packets along pathways capable of reaching the packets' ultimate destinations.

A default route is a special type of static route. A default route matches all packets, and defines a gateway router that can receive and route packets if no other, more specific static route is defined for the packet's destination IP address.

You should configure at least one static route, a default route, that points to your gateway. However, you may configure multiple static routes if you have multiple gateway routers, each of which should receive packets destined for a different subset of IP addresses.

To determine which route a packet will be subject to, the FortiVoice unit compares the packet's destination IP address to those of the static routes and forwards the packet to the route with the large prefix match.

When you add a static route through the web-based manager, the FortiVoice unit evaluates the route to determine if it represents a different route compared to any other route already present in the list of static routes. If no route having the same destination exists in the list of static routes, the FortiVoice unit adds the static route.

To view or configure static routes

1. Go to *System > Network > Routing*.

GUI field	Description
Enabled	Displays the route status.
Destination IP/Netmask	Displays the destination IP address and subnet of packets subject to the static route. `A setting of 0.0.0.0/0.0.0` indicates that the route matches all destination IP addresses.
Gateway	Displays the IP address of the next-hop router to which packets subject to the static route will be forwarded.
Interface	The interface that this route applies to.
Comment	Displays any notes on the static route.

2. Either click *New* to add a route or double-click a route to modify it.
   A dialog appears.
3. Select *Enable* to activate the route.
4. In *Destination IP/netmask*, enter the destination IP address and netmask of packets that will be subject to this static route.
   To create a default route that will match all packets, enter `0.0.0.0/0.0.0.0`.
5. Select the interface that this route applies to.
6. In *Gateway*, type the IP address of the next-hop router to which the FortiVoice unit will forward packets subject to this static route. This router must know how to route packets to the destination IP addresses that you have specified in *Destination IP/netmask*. For an Internet connection, the next hop routing gateway routes traffic to the Internet.
7. Enter any comments you have for the route.
8. Click *Create* or *OK*.

Configuring DNS

FortiVoice units require DNS servers for features such as reverse DNS lookups. Your ISP may supply IP addresses of DNS servers, or you may want to use the IP addresses of your own DNS servers.

For improved FortiVoice unit performance, use DNS servers on your local network.

The *DNS* tab lets you configure the DNS servers that the FortiVoice unit queries to resolve domain names into IP addresses.

To configure the primary and secondary DNS servers

1. Go to *System* > *Network* > *DNS*.
2. In *Primary DNS server*, enter the IP address of the primary DNS server.
3. In *Secondary DNS server*, enter the IP address of the secondary DNS server.
4. Click *Apply*.

Configuring DHCP server

A DHCP server provides an address to a client on the network, when requested, from a defined address range.

You can configure one or more DHCP servers on any FortiVoice interface. A DHCP server dynamically assigns IP addresses to the clients on the network connected to the interface. These clients must be configured to obtain their IP addresses using DHCP.

To configure the DHCP server

1. Go to *System* > *Network* > *DHCP*.
2. Click *New* and configure the following:

GUI field	Description
Network Interface Setting	
ID	The system will generate an ID for this configuration. This is view only.
Enable	Select to enable the DHCP server.
Interface	If this FortiVoice is in HA mode, make sure that the secondary unit has the same interface as the primary unit. For information on HA, see Using high availability on page 53.
Gateway	Enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
DNS options	Select to use either a specific DNS server or the system's DNS Setting. If you select a specific DNS server, enter the *Primary DNS server* and the *Secondary DNS server* fields. For more information, see Configuring DNS on page 43.
Domain	Enter the domain that the DHCP server assigns to its clients.
Netmask	Enter the netmask of the addresses that the DHCP server assigns.
Advanced Setting	
Lease time (Seconds)	Enter the length of time an IP address remains assigned to a client. Once the lease expires, the address is released for allocation to the next client request for an IP address. The default time is 604800 seconds.

GUI field	Description
Vender Class Identifier option	Select this option to apply the DHCP configuration to the phones of a specific vendor identified by the VCI string supplied by the vendor or by checking *Monitor > PBX Status > DHCP > VCI*.
VCI string	Enter the phone VCI string supplied by the vendor.
Option 66	
DHCP IP Range	Enter the start and end for the range of IP addresses that this DHCP server assigns to the DHCP clients.
DHCP Excluded IP Range	Enter a range of IP addresses that this server should not assign to the DHCP clients.
Reserved IP Address	Enter an IP address from the DHCP server to match it to a specific client using its MAC address. In a typical situation, an IP address is assigned ad hoc to a client, and that assignment times out after a specific time of inactivity from the client, known as the lease time. To ensure a client always has the same IP address, that is, there is no lease time, use this option.

3. Click *Create*.

Capturing voice and fax packets

When troubleshooting networks, it helps to look inside the contents of the packets. This helps to determine if the packets, route, and destination are all what you expect. Traffic capture can also be called packet sniffing, a network tap, or logic analyzing.

Packet sniffing tells you what is happening on the network at a low level. This can be very useful for troubleshooting problems, such as:

- Finding missing traffic.
- Seeing if sessions are setting up properly.
- Locating ARP problems such as broadcast storm sources and causes.
- Confirming which address a computer is using on the network if they have multiple addresses or are on multiple networks.
- Confirming routing is working as you expect.
- Intermittent missing PING packets.

If you are running a constant traffic application such as ping, packet sniffing can tell you if the traffic is reaching the destination, how the port enters and exits the FortiVoice unit, if the ARP resolution is correct, and if the traffic is returning to the source as expected. You can also use packet switching to verify that NAT or other configuration is translating addresses or routing traffic the way that you want it to.

Before you start sniffing packets, you need to have a good idea of what you are looking for. Sniffing is used to confirm or deny your ideas about what is happening on the network. If you try sniffing without a plan to narrow your search, you could end up with too much data to effectively analyze. On the other hand, you need to sniff enough packets to really understand all of the patterns and behavior that you are looking for.

To capture voice and fax packets

1. Go to *System > Network > Traffic Capture.*

GUI field	Description
Stop	Click to stop the packet capture.
Download	When the capture is complete, click *Download* to save the packet capture file to your hard disk for further analysis.
Name	The name of the packet capture file.
Size	The size of the packet capture file.
Status	The status of the packet capture process, *Complete* or *Running*.

2. Click *New*.
3. Enter a prefix for the file generated from the captured traffic. This will make it easier to recognize the files.
4. Enter the time period for performing the packet capture.
5. If you choose *SIP* or *Use protocol* for *Filter*, from the *Available peers* field, select the extension or trunk of which you want to capture the voice packets and click -> to move them into the *Selected peers* field. You can select up to 3 peers.
6. If you want to limit the scope of traffic capture, in the *IP/HOST* field, enter a maximum of 3 IP addresses or host names for the extensions and trunks you selected. Only traffic on these IP addresses or host names is captured.
7. Select the filter for the traffic capture:
   - *SIP*: Only SIP traffic of the peers you select will be captured.
   - *Use protocol*: Only UDP or TCP traffic of the peers you select will be captured.
   - *Capture all*: All network traffic will be captured.
8. For *Exclusion*, enter the IP addresses/host names and port numbers of which you do not want to capture voice traffic.
9. Click *Create*.

Configuring administrator accounts and access profiles

The *Administrator* submenu configures administrator accounts and access profiles.

This topic includes:

- Configuring administrator accounts on page 46
- Configuring administrator profiles on page 49

Configuring administrator accounts

The *Administrator* tab displays a list of the FortiVoice unit's administrator accounts and the trusted host IP addresses administrators use to log in (if configured).

By default, FortiVoice units have a single administrator account, `admin`. For more granular control over administrative access, you can create additional administrator accounts with restricted permissions.

To view and configure administrator accounts

1. Go to *System > Administrator > Administrator*.

GUI field	Description
Enabled	Displays the administrator status.
Name	Displays the name of the administrator account.
Admin Profile	The administrator profile that determines which functional areas the administrator account may view or affect.
Authentication Type	The administrator authentication type: *Local* or *LDAP.*
Authentication Profile	The LDAP authentication profile. For more information, see Configuring LDAP profiles on page 121.
Trusted Hosts	Displays the IP address and netmask from which the administrator can log in.

2. Either click *New* to add an account or double-click an account to modify it.
   A dialog appears.
3. Configure the following:

GUI field	Description
Enable	Click to activate the administrator status. By default, this is enabled.
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.
Email address	Enter the administrator's email address.
Single sign-on manager	Select the extension for the administrator account. If you add an extension, a *User portal* icon appears at the top of the web-based manager when you log into the FortiVoice unit. Clicking the icon opens the user web portal. Click *Edit* to modify the selected extension or click *New* to configure a new one. For more information on extensions, see Configuring IP extensions on page 156.
Admin profile	Select the name of an admin profile that determines which functional areas the administrator account may view or affect. Click *New* to create a new profile or *Edit* to modify the selected profile. For details, see Configuring administrator profiles on page 49.
Access mode	Specify the access privilege: CLI, GUI, or REST API.
Authentication type	Select an administrator authentication type: *Local* or *LDAP*.
New password	Enter this account's password. The password can contain any character except spaces. This field does not appear if *Authentication type* is *LDAP*.

GUI field	Description
	Do not enter a FortiVoice administrator password 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 could compromise the security of your FortiVoice unit.
Confirm password	Enter this account’s password again to confirm it. This field does not appear if *Authentication type* is *LDAP*.
LDAP profile	If you select *LDAP* for *Authentication type*, select an LDAP authentication profile. For more information, see Configuring LDAP profiles on page 121.
Trusted Hosts	Enter an IPv4 or IPv6 address or subnet from which this administrator can log in. If you want the administrator to access the FortiVoice unit from any IP address, use `0.0.0.0/0.0.0.0`. Enter the IP address and netmask in dotted decimal format. For example, you might permit the administrator to log in to the FortiVoice unit from your private network by typing `192.168.1.0/255.255.255.0`. For additional security, restrict all trusted host entries to administrative hosts on your trusted private network. For example, if your FortiVoice administrators log in only from the 10.10.10.10/24 subnet, to prevent possibly fraudulent login attempts from unauthorized locations, you could configure that subnet in the *Trusted Host #1*, *Trusted Host #2*, and *Trusted Host #3* fields. For information on restricting administrative access protocols that can be used by these hosts, see Editing network interfaces on page 40. Click the + sign to add additional IP addresses or subnets from which the administrator can log in.
Select language	Select this administrator account’s preference for the display language of the web-based manager.
Select theme	Select this administrator account’s preference for the display theme or click *Use Current* to choose the theme currently in effect. The administrator may switch the theme at any time during a session by clicking *Next Theme*.
Department only	Select the checkbox if this is a department administrator.
Description	Select *Edit* to enter any comments for the administrator account.
Departments	Select the department to which the administrator belongs.

GUI field	Description
	This option is only available if you select *Department only*.

4. Click *Create*.

Configuring administrator profiles

The *Admin Profile* tab displays a list of administrator access profiles.

Administrator profiles govern which areas of the web-based manager and CLI that an administrator can access, and whether or not they have the permissions necessary to change the configuration or otherwise modify items in each area.

To configure administrator access profiles

1. Go to *System* > *Administrator* > *Admin Profile*.
2. Either click *New* to add an account or double-click an access profile to modify it.
3. In *Profile name*, enter the name for this access profile.
4. For each access control option, select the permissions to be granted to administrator accounts associated with this access profile:
   - *None*
   - *Read Only*
   - *Read-Write*
5. Click *Create*.

Configuring RAID

If your FortiVoice unit model supports RAID, go to *System* > *RAID* to configure a redundant array of independent disks (RAID) for the FortiVoice unit hard disks that are used to store logs and voice data.

FVE-2000F, 3000F, 3000E, and 5000F can be configured to use RAID with their hard disks. The default RAID level should give good results, but you can modify the configuration to suit your individual requirements for enhanced performance and reliability. For more information, see Configuring RAID on page 50.

RAID events can be logged and reported with alert email. These events include disk full and disk failure notices. For more information, see About FortiVoice logging on page 278, and Configuring alert email on page 291.

If your FortiVoice unit model does not support RAID, the *RAID* menu won’t be displayed.

About RAID levels

The FortiVoice models supporting RAID use hardware RAID controllers that require that the log disk and voice disk use the same RAID level.

Each of the models has 2 factory-installed hard drives. The available RAID levels are 0 and 1 and the default is 1. You can replace a hard drive if required. For details, see Replacing a RAID disk on page 52.

Configuring RAID

You can modify the RAID level configuration to suit you individual requirements for enhanced performance and reliability.

To configure RAID

1. Go to *System* > *RAID* > *RAID System*.

GUI item	Description
Model	Displays the model of the hardware RAID controller.
Rescan	Click to rebuild the RAID unit with disks that are currently a member of it, or detect newly added hard disks, and start a diagnostic check.
Driver	Displays the version of the RAID controller’s driver software.
Firmware	Displays the version of the RAID controller’s firmware.
List of RAID units in the array	
Device	Displays the name of the RAID unit. This indicates whether it is used for voice data or log message data. This is hard-coded and not configurable.
Unit	Indicates the identifier of the RAID unit, such as *u0*.
Level	Indicates the RAID level currently in use. You may change the level. For more information, see About RAID levels on page 49.
Status	Indicates the status of the RAID unit. • *OK*: The RAID unit is operating normally. • *Warning*: The RAID controller is currently performing a background task (rebuilding, migrating, or initializing the RAID unit). Do not remove hard disks while this status is displayed. Removing active hard disks can cause hardware damage. • *Error*: The RAID unit is degraded or inoperable. Causes vary, such as when too many hard disks in the unit fail and the RAID unit no longer has the minimum number of disks required to operate in your selected RAID level. To correct such a situation, replace the failed hard disks. • *No Units*: No RAID units are available. If both *Error* and *Warning* conditions exist, the status appears as *Error*.
Size	Indicates the total disk space, in gigabytes (GB), available for the RAID unit. Available space varies by your RAID level selection. Due to some space being consumed to store data required by RAID, available storage space will not equal the sum of the capacities of hard disks in the unit.
Speed	Displays the average speed in kilobytes (KB) per second of the data transfer for the resynchronization. This is affected by the disk being in use during the resynchronization.
Apply	Click to save changes.
List of hard disks in the array	

GUI item	Description
ID/Port	Indicates the identifier of each hard disk visible to the RAID controller.
Part of Unit	Indicates the RAID unit to which the hard disk belongs, if any. To be usable by the FortiVoice unit, you must add the hard disk to a RAID unit.
Status	Indicates the hardware viability of the hard disk. • *OK*: The hard disk is operating normally. • *UNKNOWN*: The viability of the hard disk is not known. Causes vary, such as the hard disk not being a member of a RAID unit. In such a case, the RAID controller does not monitor its current status.
Size	Indicates the capacity of the hard disk, in gigabytes (GB).
Delete	Click to unmount a hard disk before swapping it. After replacing the disk, add it to a RAID unit, then click *Rescan*.

To change RAID levels

Back up data on the disk before beginning this procedure. Changing the device’s RAID level temporarily suspends all mail processing and erases all data on the hard disk. For more information on creating a backup, see Backing up configuration on page 100.

1. Go to *System* > *RAID* > *RAID System*.
2. From *Level*, select a RAID level.
3. Click *Apply*.
   The FortiVoice unit changes the RAID level and reboots.

Replacing a RAID disk

When replacing a disk in the RAID array, the new disk must have the same or greater storage capacity than the existing disks in the array. If the new disk has a larger capacity than the other disks in the array, only the amount equal to the smallest hard disk will be used. For example, if the RAID has 400 GB disks, and you replace one with a 500 GB disk, to be consistent with the other disks, only 400 GB of the new disk will be used.

FortiVoice units support hot swap; shutting down the FortiVoice unit during hard disk replacement is not required.

To replace a disk in the array

1. Go to *System* > *RAID* > *RAID System*.
2. In the row corresponding to the hard disk that you want to replace (for example, *p4*), select the hard disk and click *Delete*.
   The RAID controller removes the hard disk from the list.
3. Protect the FortiVoice unit from static electricity by using measures such as applying an antistatic wrist strap.
4. Physically remove the hard disk that corresponds to the one you removed in the web UI from its drive bay on the FortiVoice unit.
5. Replace the hard disk with a new hard disk, inserting it into its drive bay on the FortiVoice unit.

6. Click *Rescan*.

The RAID controller will scan for available hard disks and should locate the new hard disk. Depending on the RAID level, the FortiVoice unit may either automatically add the new hard disk to the RAID unit or allocate it as a spare that will be automatically added to the array if one of the hard disks in the array fails.

The FortiVoice unit rebuilds the RAID array with the new hard disk. Time required varies by the size of the array.

Using high availability

Go to *System > High Availability* to configure the FortiVoice unit to act as a high availability (HA) member in order to increase availability.

For the general procedure of how to enable and configure HA, see Enabling and configuring HA on page 56.

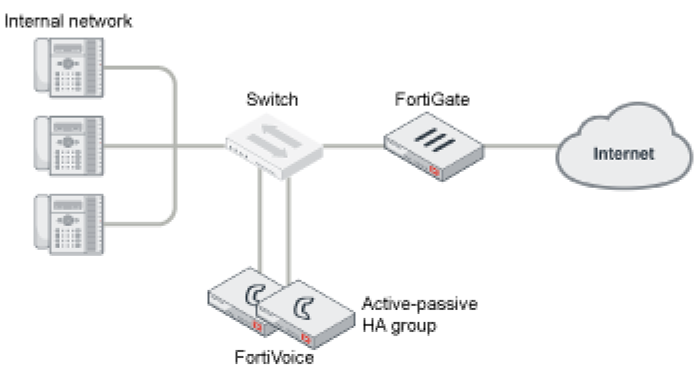
This section contains the following topics:

About high availability

FortiVoice units operate in n active-passive HA mode which has the following features:

- Two FortiVoice units are in the HA group.
- Both configuration and data are synchronized (For exceptions to synchronized configuration items, see Unsynchronized HA Setting on page 55.)
- Only the primary unit processes phone calls.
- There is no data loss when the hardware fails although active calls are disconnected and line appearance and extension appearance take time to restore.
- Both FortiVoice units have failover protection, but no increased processing capacity.

Active-passive HA group



Same FortiVoice models must be used in the same HA group. All units in the HA group must have the same firmware version with the same hardware.

Communications between HA members occur through the heartbeat and synchronization connection. For details, see About the heartbeat and synchronization on page 54.

To configure FortiVoice units operating in HA mode, you usually connect only to the primary unit. The primary unit's configuration is almost entirely synchronized to secondary units, so that changes made to the primary unit are propagated to the secondary units.

Exceptions to this rule include connecting to a secondary unit in order to view log messages recorded about the secondary unit itself on its own hard disk, and connecting to a secondary unit to configure Setting that are not synchronized. For details, see Unsynchronized HA Setting on page 55.

For instructions of how to enable and configure HA, see Enabling and configuring HA on page 56.

About the heartbeat and synchronization

Heartbeat and synchronization traffic consists of TCP packets transmitted between the FortiVoice units in the HA group through the primary and secondary heartbeat interfaces.

Service monitoring traffic can also, for short periods, be used as a heartbeat. For details, see Remote services as heartbeat on page 61.

Heartbeat and synchronization traffic has three primary functions:

- To monitor the responsiveness of the HA group members.
- To synchronize configuration changes from the primary unit to the secondary units.
  For exceptions to synchronized configuration items, see Unsynchronized HA Setting on page 55.
- To synchronize system and user data from the primary unit to the secondary unit.
  Call data consists of the FortiVoice call detailed records, recorded calls, voicemail, call directories, fax, and voice prompts.

When the primary unit's configuration changes, it immediately synchronizes the change to the secondary unit through the primary heartbeat interface. If this fails, or if you have inadvertently de-synchronized the secondary unit's configuration, you can manually initiate synchronization. For details, see click HERE to start a configuration/data sync on page 58. You can also use the CLI command `diagnose system ha sync` on either the primary unit or the secondary unit to manually synchronize the configuration.

During normal operation, the secondary unit expects to constantly receive heartbeat traffic from the primary unit. Loss of the heartbeat signal interrupts the HA group and generally triggers a failover. For details, see Failover scenario 1: Temporary failure of the primary unit on page 66.

Exceptions include system restarts and the `execute reload` CLI command. In case of a system reboot or reload of the primary unit, the primary unit signals the secondary unit to wait for the primary unit to complete the restart or reload. For details, see Failover scenario 2: System reboot or reload of the primary unit on page 67.

Periodically, the secondary unit checks with the primary unit to see if there are any configuration changes on the primary unit. If there are configuration changes, the secondary unit will pull the configuration changes from the primary unit, generate a new configuration, and reload the new configuration. In this case, both the primary and secondary units can be configured to send alert email. For details, see Failover scenario 3: System reboot or reload of the secondary unit on page 68 and Configuring alert email on page 291.

Unsynchronized HA Setting

All configuration Setting on the primary unit are synchronized to the secondary unit, except the following:

GUI item	Description
Host name	The host name distinguishes members of the cluster.
Static route	Static routes are not synchronized because the HA units may be in different networks (see Configuring static routes on page 42).
Interface configuration	Each FortiVoice unit in the HA group must be configured with different network interface Setting for connectivity purposes. For details, see Configuring the network interfaces on page 39. Exceptions include some active-passive HA Setting which affect the interface configuration for failover purposes. These Setting are synchronized.
Main HA configuration	The main HA configuration, which includes the HA mode of operation (such as *master* or *slave*), is not synchronized because this configuration must be different on the primary and secondary units. For details, see Configuring the HA mode and group on page 59.
HA service monitoring configuration	In active-passive HA, the HA service monitoring configuration is not synchronized. The remote service monitoring configuration on the secondary unit controls how the secondary unit checks the operation of the primary unit. The local services configuration on the primary unit controls how the primary unit tests the operation of the primary unit. For details, see Configuring service-based monitoring on page 64. You might want to have a different service monitoring configuration on the primary and secondary units. For example, after a failover you may not want service monitoring to operate until you have fixed the problems that caused the failover and have restarted normal operation of the HA group.
System appearance	The appearance Setting you configured under *System* > *Configuration* > *Appearance* are not synchronized.

Synchronization after a failover

During normal operation, extensions are in one of two states:

- registered and idle
- active call

When a failover occurs, active calls are interrupted and users have to reinitiate the calls. However, registered idle extensions can still make and receive phone calls without being affected.

When a failover is corrected, one of the following occurs automatically:

1. The secondary unit detects the failure of the primary unit, and becomes the new primary unit.
2. The former primary unit restarts, detects the new primary unit, and becomes a secondary unit.

You may have to manually restart the failed primary unit.

Enabling and configuring HA

In general, to enable and configure HA, you should perform the following:

1. Physically connect the FortiVoice units that will be members of the HA group.
   You must connect at least one of their network interfaces for heartbeat and synchronization traffic between members of the group. For reliability reasons, Fortinet recommends that you connect both a primary and a secondary heartbeat interface, and that they be connected directly or through a dedicated switch that is not connected to your overall network.
2. On each member of the group:
   - Enable the HA mode that you want to use and select whether the individual member will act as a primary unit or secondary unit. For information about the differences between the HA modes, see About high availability on page 53.
   - Configure the local IP addresses of the primary and secondary heartbeat and synchronization network interfaces.
   - Configure a virtual IP address that is shared by the HA group and remains the same after a failover. The virtual IP address is used to auto-provision the server IP address and the SIP trunk client IP address.
   - Configure the behavior on failover, and how the network interfaces should be configured for whichever FortiVoice unit is currently acting as the primary unit.
3. If you want to trigger failover when hardware or a service fails, even if the heartbeat connection is still functioning, configure service monitoring. For details, see Configuring service-based monitoring on page 64.
4. Monitor the status of each group member. For details, see Monitoring the HA status on page 56. To monitor HA events through log messages and/or alert email, you must first enable logging of HA activity events. For details, see Configuring logging on page 280.

Monitoring the HA status

The *Status* tab in the *High Availability* submenu shows the configured HA mode of operation of a FortiVoice unit in an HA group. You can also manually initiate synchronization and reset the HA mode of operation. A reset may be required if a FortiVoice unit's effective HA mode of operation differs from its configured HA mode of operation, such as after a failover when a configured primary unit is currently acting as a secondary unit.

For FortiVoice units operating as secondary units, the *Status* tab also lets you view the status and schedule of the HA synchronization daemon.

Before you can use the *Status* tab, you must first enable and configure HA. For details, see Enabling and configuring HA on page 56.

To view the HA mode of operation status, go to *System > High Availability > Status*.

GUI item	Description
HA Status	Select a time interval for refreshing the HA status page. You can also manually update the page by clicking *Refresh*.

GUI item	Description
Mode Status	
Configured Operating Mode	Displays the HA operating mode that you configured, either: • *master*: Configured to be the primary unit of an active-passive group. • *slave*: Configured to be the secondary unit of an active-passive group. For information on configuring the HA operating mode, see Mode of operation on page 60. After a failure, the FortiVoice unit may not be acting in its configured HA operating mode. For details, see Effective Operating Mode on page 57.
Effective Operating Mode	Displays the mode that the unit is currently operating in, either: • *master*: Acting as primary unit. • *slave*: Acting as secondary unit. • *off*: For primary units, this indicates that service/interface monitoring has detected a failure and has taken the primary unit offline, triggering failover. For secondary units, this indicates that synchronization has failed once; a subsequent failure will trigger failover. For details, see On failure on page 60. • *failed*: Service/network interface monitoring has detected a failure and the diagnostic connection is currently determining whether the problem has been corrected or failover is required. For details, see On failure on page 60. The configured HA operating mode matches the effective operating mode unless a failure has occurred. For example, after a failover, a FortiVoice unit configured to operate as a secondary unit could be acting as a primary unit. For explanations of combinations of configured and effective HA modes of operation, see Combinations of configured and effective HA modes of operation on page 58. For information on restoring the FortiVoice unit to an effective HA operating mode that matches the configured operating mode, see click HERE to restore configured operating mode on page 58.
Daemon Status	This option appears only for secondary units in active-passive HA groups.
Monitor	Displays the time at which the secondary unit's HA daemon will check to make sure that the primary unit is operating correctly, and, if monitoring has detected a failure, the number of times that a failure has occurred. Monitoring occurs through the heartbeat link between the primary and secondary units. If the heartbeat link becomes disconnected, the next time the secondary unit checks for the primary unit, the primary unit will not respond. If the maximum number of consecutive failures is reached, and no secondary heartbeat or remote service monitoring heartbeat is available, the secondary unit will change its effective HA operating mode to become the new primary unit. For details, see HA base port on page 61.
Configuration	Displays the time at which the secondary unit's HA daemon will synchronize the FortiVoice configuration from the primary unit to the secondary unit.

GUI item	Description
	The message `slave unit is currently synchronizing` appears when the HA daemon is synchronizing the configuration. For information on items that are not synchronized, see Unsynchronized HA Setting on page 55.
Data	Displays the time at which the secondary unit HA daemon will synchronize mail data from the primary unit to the secondary unit. The message `slave unit is currently synchronizing` appears when the HA daemon is synchronizing data.
Actions	
click HERE to start a configuration/data sync	Click to manually initiate synchronization of the configuration and call data. For information on items that are not synchronized, see Unsynchronized HA Setting on page 55.
click HERE to restore configured operating mode	Click to reset the FortiVoice unit to an effective HA operating mode that matches the FortiVoice unit's configured operating mode. For example, for a configured primary unit whose effective HA operating mode is now secondary, after correcting the cause of the failover, you might click this option on the primary unit to restore the configured primary unit to active duty, and restore the secondary unit to its secondary role. If the effective HA operating mode has changed due to a failover, make sure to resolve any issues that caused the failover before selecting this option.

Combinations of configured and effective HA modes of operation

Configured operating mode	Effective operating mode	Description
master	master	Normal for the primary unit of an active-passive HA group.
slave	slave	Normal for the secondary unit of an active-passive HA group.
master	off	The primary unit has experienced a failure, or the FortiVoice unit is in the process of switching to operating in HA mode. HA processes and call processing are stopped.
slave	off	The secondary unit has detected a failure, or the FortiVoice unit is in the process of switching to operating in HA mode. After the secondary unit starts up and connects with the primary unit to form an HA group, the first configuration synchronization may fail in special circumstances. To prevent both the secondary and primary units from simultaneously acting as primary units, the effective HA mode of operation becomes *off*. If subsequent synchronization fails, the secondary unit's effective

Configured operating mode	Effective operating mode	Description
		HA mode of operation becomes *master*.
master	failed	The remote service monitoring or local network interface monitoring on the primary unit has detected a failure, and will attempt to connect to the other FortiVoice unit. If the problem that caused the failure has been corrected, the effective HA mode of operation switches from *failed* to *slave*, or to match the configured HA mode of operation, depending on the *On failure* setting.
master	slave	The primary unit has experienced a failure but then returned to operation. When the failure occurred, the unit configured to be the secondary unit became the primary unit. When the unit configured to be the primary unit restarted, it detected the new primary unit and so switched to operating as the secondary unit.
slave	master	The secondary unit has detected that the FortiVoice unit configured to be the primary unit failed. When the failure occurred, the unit configured to be the secondary unit became the primary unit.

Configuring the HA mode and group

The *Configuration* tab in the *System* > *High Availability* submenu lets you configure the high availability (HA) options, including:

- enabling HA
- whether this individual FortiVoice unit will act as a primary unit or a secondary unit in the group
- network interfaces that will be used for heartbeat and synchronization and virtual IP
- service monitor

HA Setting, with the exception of *Virtual IP Address* Setting, are not synchronized and must be configured separately on each primary and secondary unit.

You must maintain the physical link between the heartbeat and synchronization network interfaces. These connections enable a group member to detect the responsiveness of the other member, and to synchronize data. If they are interrupted, normal operation will be interrupted and a failover will occur. For more information on heartbeat and synchronization, see About the heartbeat and synchronization on page 54.

You can directly connect the heartbeat network interfaces of two FortiVoice units using a crossover Ethernet cable.

To configure HA options

1. Go to *System* > *High Availability* > *Configuration*.
2. Configure the following sections, as applicable:
   - Configuring the primary HA options on page 60
   - Configuring HA advanced options on page 60
   - Configuring interface monitoring on page 62
   - Configuring service-based monitoring on page 64

3. Click *Apply*.

Configuring the primary HA options

Go to *System* > *High Availability* > *Configuration* and click the arrow to expand the *HA Configuration* section, if needed.

GUI field	Description
Mode of operation	Enables or disables HA, and selects the initial configured role this FortiVoice unit in the HA group. • *Off*: The FortiVoice unit is not operating in HA mode. • *Master*: The FortiVoice unit is the primary unit in an active-passive HA group. • *Slave*: The FortiVoice unit is the secondary unit in an active-passive HA group.
On failure	Select one of the following behaviors of the primary unit when it detects a failure, such as on a power failure or from service/interface monitoring. • *Switch Off:* Do not process phone calls or join the HA group until you manually select the effective operating mode (see click HERE to start a configuration/data sync on page 58 and click HERE to restore configured operating mode on page 58). • *Wait for Recovery Then Restore Original Role*: On recovery, the failed primary unit's effective HA mode of operation resumes its configured primary role. This also means that the secondary unit needs to give back the primary role to the primary unit. This behavior may be useful if the cause of failure is temporary and rare, but may cause problems if the cause of failure is permanent or persistent. • *Wait for Recovery Then Restore Slave Role*: On recovery, the failed primary unit’s effective HA mode of operation becomes *slave*, and the secondary unit continues to assume the *master* role. The primary unit then synchronizes with the current primary unit. The new primary unit can then deliver phone calls. For information on manually restoring the FortiVoice unit to acting in its configured HA mode of operation, see click HERE to restore configured operating mode on page 58. In most cases, you should select the *Wait for Recovery Then Restore Slave Role* option. For details on the effects of this option on the *Effective Operating Mode*, see Combinations of configured and effective HA modes of operation on page 58. For information on configuring service/interface monitoring, see Configuring service-based monitoring on page 64. This option appears only if Mode of operation on page 60 is *master*.
Shared password	Enter an HA password for the HA group. You must configure the same *Shared password* value on both the primary and secondary units.

Configuring HA advanced options

Go to *System* > *High Availability* > *Configuration* > *Advanced Options*.

GUI item	Description
HA base port	Keep the default TCP port number (20000) that will be used for: • the heartbeat signal • synchronization control • data synchronization • configuration synchronization In addition to configuring the heartbeat, you can configure service monitoring. For details, see Configuring service-based monitoring on page 64. In addition to automatic immediate and periodic configuration synchronization, you can also manually initiate synchronization. For details, see click HERE to start a configuration/data sync on page 58.
Heartbeat lost threshold	Enter the total span of time, in seconds, for which the primary unit can be unresponsive before it triggers a failover and the secondary unit assumes the role of the primary unit. The heartbeat will continue to check for availability once per second. To prevent premature failover when the primary unit is simply experiencing very heavy load, configure a total threshold of three (3) seconds or more to allow the secondary unit enough time to confirm unresponsiveness by sending additional heartbeat signals. If the failure detection time is too short, the secondary unit may falsely detect a failure during periods of high load. If the failure detection time is too long, the primary unit could fail and a delay in detecting the failure could mean that a call is delayed or lost. Decrease the failure detection time if a call is delayed or lost because of an HA failover.
Remote services as heartbeat	Enable to use remote service monitoring as a secondary HA heartbeat. If enabled and both the primary and secondary heartbeat links fail or become disconnected, and remote service monitoring still detects that the primary unit is available, a failover will not occur. The remote service check is only applicable for temporary heartbeat link fails. If the HA process restarts due to system reboot or HA daemon reboot, then physical heartbeat connections will be checked first. If physical connections are not found, the remote service monitoring does not take effect anymore.

GUI item	Description
	Using remote services as heartbeat provides HA heartbeat only, not synchronization. To avoid synchronization problems, you should not use remote service monitoring as a heartbeat for extended periods. This feature is intended only as a temporary heartbeat solution that operates until you reestablish a normal primary or secondary heartbeat link.
Call recording sync	Select to sync recorded calls.

Configuring interface monitoring

Interface monitor checks the local interfaces on the primary unit. If a malfunctioning interface is detected, a failover will be triggered.

To configure interface monitoring

1. Go to *System* > *High Availability* > *Configuration*.
2. Select master or slave as the mode of operation.
3. Expand the *Interface* area, if required.

> The interface IP address must be different from, but on the same subnet as, the IP address of the other heartbeat network interface of the other member in the HA group.
>
> When configuring the other FortiVoice unit in the HA group, use this value as the remote peer IP.

4. Select a row in the table and click *Edit* to configure the following HA Setting on the interface.

GUI item	Description
Port	Displays the interface name you're configuring.
Enable port monitor	Enable to monitor a network interface for failure. If the port fails, the primary unit will trigger a failover.
Heartbeat status	Specify if this interface will be used for HA heartbeat and synchronization. • Disable Do not use this interface for HA heartbeat and synchronization. • Primary Select the primary network interface for heartbeat and synchronization traffic. For more information, see About the heartbeat and synchronization on page 54. This network interface must be connected directly or through a switch to the *Primary heartbeat* network interface of the other member in the HA group. • Secondary Select the secondary network interface for heartbeat and synchronization traffic. For more information, see About the heartbeat and synchronization on page 54. The secondary heartbeat interface is the backup heartbeat link between the units in the HA group. If the primary heartbeat link is functioning, the secondary heartbeat link is

GUI item	Description
	used for the HA heartbeat. If the primary heartbeat link fails, the secondary link is used for the HA heartbeat and for HA synchronization. This network interface must be connected directly or through a switch to the *Secondary heartbeat* network interfaces of the other member in the HA group. Using the same network interface for both HA synchronization/heartbeat traffic and other network traffic could result in issues with heartbeat and synchronization during times of high traffic load, and is not recommended. In general, you should isolate the network interfaces that are used for heartbeat traffic from your overall network. Heartbeat and synchronization packets contain sensitive configuration information, are latency-sensitive, and can consume considerable network bandwidth.
Peer IP address	Enter the IP address of the matching heartbeat network interface of the other member of the HA group. For example, if you are configuring the primary unit's primary heartbeat network interface, enter the IP address of the secondary unit's primary heartbeat network interface. Similarly, for the secondary heartbeat network interface, enter the IP address of the other unit's secondary heartbeat network interface. For information about configuration synchronization and what is not synchronized, see About the heartbeat and synchronization on page 54.
Peer IPv6 address	Enter the peer IPv6 address for this interface.
Virtual IP action	Select whether and how to configure the IP addresses and netmasks of the FortiVoice unit whose effective HA mode of operation is currently *master*. For example, a primary unit might be configured to receive phone call traffic through *port1* and receive heartbeat and synchronization traffic through *port3* and *port4*. In that case, you would configure the primary unit to set the IP addresses or add virtual IP addresses for *port1* of the secondary unit on failover in order to mimic that of the primary unit. • *Ignore*: Do not change the network interface configuration on failover, and do not monitor. For details on service monitoring for network interfaces, see Configuring service-based monitoring on page 64. • *Use*: Add the specified virtual IP address and netmask to the network interface on failover. Normally, you will configure your network so that clients use the virtual IP address. This option results in the network interface having two IP Addresses: the actual **and** the virtual.
Virtual IP address	Enter the virtual IPv4 address for this interface.
Virtual IPv6 address	Enter the virtual IPv6 address for this interface.

5. Click *OK*.

Configuring service-based monitoring

Go to *System > High Availability > Configuration* to configure remote service monitoring, local network interface monitoring, and local hard drive monitoring.

HA service monitoring Setting are not synchronized and must be configured separately on each primary and secondary unit.

With remote service monitoring, the secondary unit confirms that it can connect to the primary unit over the network using SIP and HTTP connections.

With local network interface monitoring and local hard drive monitoring, the primary unit monitors its own network interfaces and hard drives.

If service monitoring detects a failure, the effective HA operating mode of the primary unit switches to *off* or *failed* (depending on the *On failure* setting). A failover then occurs, and the effective HA operating mode of the secondary unit switches to *master*. For information on the *On failure* option, see Configuring the HA mode and group on page 59. For information on the effective HA operating mode, see Monitoring the HA status on page 56.

To configure service monitoring

1. Go to *System > High Availability > Configuration*.
2. Select master or slave as the mode of operation.
3. Expand *Service Monitor*, if required.
4. Select a row in the table and click *Edit* to configure it.
5. For *Remote HTTP,* configure the following:

GUI item	Description
Enable	Select to enable connection responsiveness tests for SMTP.
Name	Displays the service name.
Remote IP	Enter the peer IP address.
Port	Enter the port number of the peer SMTP service.
Timeout	Enter the timeout period for one connection test.
Interval	Enter the frequency of the tests.
Retries	Enter the number of consecutively failed tests that are allowed before the primary unit is deemed unresponsive and a failover occurs.

6. For *SIP UDP*, configure the following:

GUI Item	Description
Enable	Select to enable SIP UDP service.
Name	Displays the service name.
Remote IP	Enter the peer IP address.
Port	Enter the port number of the peer SIP UDP service.
Timeout	Enter the timeout period for one connection test.
Interval	Enter the frequency of the tests.
Retries	Enter the number of consecutively failed tests that are allowed before the primary unit is deemed unresponsive and a failover occurs.

7. For *Interface monitor* and *Local hard drives*, configure the following:

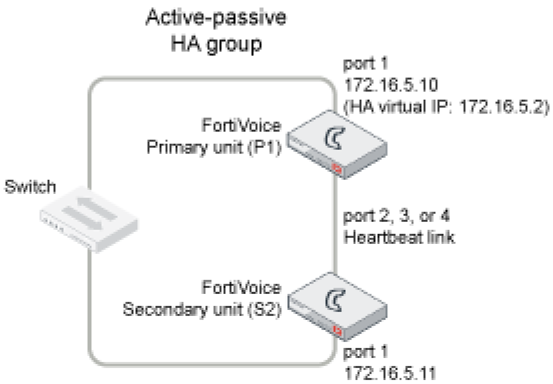
GUI item	Description
Enable	Select to enable local hard drive monitoring. Interface monitoring is enabled when you configure interface monitoring. See Configuring interface monitoring on page 62. Network interface monitoring tests all active network interfaces whose: Virtual IP action on page 63 setting is **not** *Ignore* Configuring interface monitoring on page 62 setting is enabled
Interval	Enter the frequency of the test.
Retries	Specify the number of consecutively failed tests that are allowed before the local interface or hard drive is deemed unresponsive and a failover occurs.

Failover scenario examples:

This section describes basic FortiVoice active-passive HA failover scenarios. For each scenario, refer to the HA group shown in Example active-passive HA group on page 65. To simplify the descriptions of these scenarios, the following abbreviations are used:

- P1 is the configured primary unit.
- S2 is the configured secondary unit.

Example active-passive HA group



This section contains the following HA failover scenarios:

- Failover scenario 1: Temporary failure of the primary unit on page 66
- Failover scenario 2: System reboot or reload of the primary unit on page 67
- Failover scenario 3: System reboot or reload of the secondary unit on page 68
- Failover scenario 4: System shutdown of the secondary unit on page 68
- Failover scenario 5: Primary heartbeat link fails on page 68
- Failover scenario 6: Network connection between primary and secondary units fails (remote service monitoring detects a failure) on page 70

Failover scenario 1: Temporary failure of the primary unit

In this scenario, the primary unit (P1) fails because of a software failure or a recoverable hardware failure (in this example, the P1 power cable is unplugged). HA logging and alert email are configured for the HA group.

When the secondary unit (S2) detects that P1 has failed, S2 becomes the new primary unit and continues processing phone calls.

There is no data loss when failover happens although active calls are disconnected and line appearance and extension appearance take time to restore. Call data consists of the FortiVoice call detailed records, recorded calls, voicemail, call directories, fax, and voice prompts. The user web portal is not affected.

Here is what happens during this process:

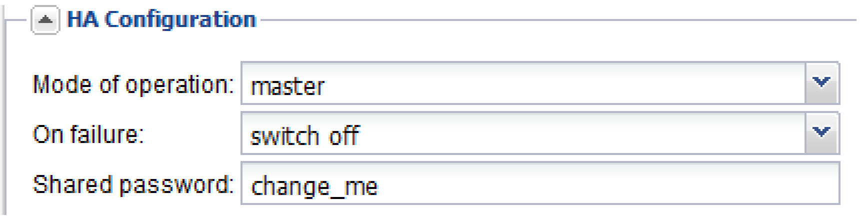
1. The FortiVoice HA group is operating normally.
2. The power is accidentally disconnected from P1.
3. S2’s heartbeat test detects that P1 has failed.
   How soon this happens depends on the HA daemon configuration of S2.
4. The effective HA operating mode of S2 changes to *master*.
5. S2 sends an alert email similar to the following, indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.
   ```
   This is the HA machine at 172.16.5.11.

   The following event has occurred
   'MASTER heartbeat disappeared'
   The state changed from 'SLAVE' to 'MASTER'
   ```
6. S2 records event log messages (among others) indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

Recovering from temporary failure of the primary unit

After P1 recovers from the hardware failure, what happens next to the HA group depends on P1's HA *On failure* Setting under *System > High Availability > Configuration*.

HA On Failure Setting



- *Switch Off*
  P1 will not process calls or join the HA group until you manually select the effective HA operating mode (see click HERE to restore configured operating mode on page 58).
- *Wait for Recovery Then Restore Original Role*
  On recovery, P1's effective HA operating mode resumes its configured primary role. This also means that S2 needs to give back the primary role to P1. This behavior may be useful if the cause of failure is temporary and rare, but may cause problems if the cause of failure is permanent or persistent.
  In the case, the S2 will send out another alert email similar to the following:
  This is the HA machine at 172.16.5.11.

  The following event has occurred
  'SLAVE asks us to switch roles (recovery after a restart)
  The state changed from 'MASTER' to 'SLAVE'

  After recovery, P1 also sends out an alert email similar to the following:
  This is the HA machine at 172.16.5.10.

  The following critical event was detected
  The system was shutdown!
- *wait for recovery then restore slave role*
  On recovery, P1's effective HA operating mode becomes *slave*, and S2 continues to assume the *master* role. P1 then synchronizes with the current primary unit, S2. For information on manually restoring the FortiVoice unit to acting in its configured HA mode of operation, see click HERE to restore configured operating mode on page 58.

Failover scenario 2: System reboot or reload of the primary unit

If you need to reboot or reload (not shut down) P1 for any reason, such as a firmware upgrade or a process restart, by using the CLI commands `execute reboot` or `execute reload`, or by clicking the *Restart* button under *Status > Dashboard > System Command* on the GUI:

- P1 will send a holdoff command to S2 so that S2 will not take over the primary role during P1's reboot.
- P1 will also send out an alert email similar to the following:
  This is the HA machine at 172.16.5.10.
  The following critical event was detected
  The system is rebooting (or reloading)!

- S2 will hold off checking the services and heartbeat with P1. Note that S2 will only hold off for about 5 minutes. In case P1 never boots up, S2 will take over the primary role.
- S2 will send out an alert email, indicating that S2 received the holdoff command from P1.
  This is the HA machine at 172.16.5.11.

  The following event has occurred
  'peer rebooting (or reloading)'
  The state changed from 'SLAVE' to 'HOLD_OFF'

After P1 is up again:

- P1 will send another command to S2 and ask S2 to change its state from holdoff to secondary and resume monitoring P1's services and heartbeat.
- S2 will send out an alert email, indicating that S2 received instruction commands from P1.
  This is the HA machine at 172.16.5.11.

  The following event has occurred
  'peer command appeared'
  The state changed from 'HOLD_OFF' to 'SLAVE'.
- S2 logs the event in the HA logs.

Failover scenario 3: System reboot or reload of the secondary unit

If you need to reboot or reload (not shut down) S2 for any reason, such as a firmware upgrade or a process restart, by using the CLI commands `execute reboot` or `execute reload`, or by clicking the *Restart* button under *Monitor* > *System Status* > *Status* on the GUI, the behavior of P1 and S2 is as follows:

- P1 will send out an alert email similar to the following, informing the administrator of the heartbeat loss with S2.
  This is the HA machine at 172.16.5.10.

  The following event has occurred
  'ha: SLAVE heartbeat disappeared'
- S2 will send out an alert email similar to the following:
  This is the HA machine at 172.16.5.11.

  The following critical event was detected
  The system is rebooting (or reloading)!
- P1 will also log this event in the HA logs.

Failover scenario 4: System shutdown of the secondary unit

If you shut down S2:

- No alert email is sent out from either P1 or S2.
- P1 will log this event in the HA logs.

Failover scenario 5: Primary heartbeat link fails

If the primary heartbeat link fails, such as when the cable becomes accidentally disconnected, and if you have not configured a secondary heartbeat link, the FortiVoice units in the HA group cannot verify that other units are operating and assume that the other has failed. As a result, the secondary unit (S2) changes to operating as a primary unit, and **both** FortiVoice units are acting as primary units.

Two primary units connected to the same network may cause address conflicts on your network. Additionally, because the heartbeat link is interrupted, the FortiVoice units in the HA group cannot synchronize configuration changes or voice data changes.

Even after reconnecting the heartbeat link, both units will continue operating as primary units. To return the HA group to normal operation, you must connect to the web-based manager of S2 to restore its effective HA operating mode to *slave* (secondary unit).

1. The FortiVoice HA group is operating normally.
2. The heartbeat link Ethernet cable is accidentally disconnected.
3. S2’s HA heartbeat test detects that the primary unit has failed.
   How soon this happens depends on the HA daemon configuration of S2.
4. The effective HA operating mode of S2 changes to *master*.
5. S2 sends an alert email similar to the following, indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.
   This is the HA machine at 172.16.5.11.

   The following event has occurred
   ‘MASTER heartbeat disappeared’
   The state changed from ‘SLAVE’ to ‘MASTER’
6. S2 records event log messages (among others) indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

Recovering from a heartbeat link failure

Because the hardware failure is not permanent (that is, the failure of the heartbeat link was caused by a disconnected cable, not a failed port on one of the FortiVoice units), you may want to return both FortiVoice units to operating in their configured modes when rejoining the failed primary unit to the HA group.

To return to normal operation after the heartbeat link fails

1. Reconnect the primary heartbeat interface by reconnecting the heartbeat link Ethernet cable.
   Even though the effective HA operating mode of S2 is *master*, S2 continues to attempt to find the other primary unit. When the heartbeat link is reconnected, S2 finds P1 and determines that P1 is also operating as a primary unit. So S2 sends a heartbeat signal to notify P1 to stop operating as a primary unit. The effective HA operating mode of P1 changes to *off*.
2. P1 sends an alert email similar to the following, indicating that P1 has stopped operating as the primary unit.
   This is the HA machine at 172.16.5.10

   The following event has occurred

   'SLAVE asks us to switch roles (user requested takeover)'

   The state changed from 'MASTER' to 'OFF'
3. P1 records event log messages (among others) indicating that P1 is switching to *off* mode.
   The configured HA mode of operation of P1 is *master* and the effective HA operating mode of P1 is *off*.

   The configured HA mode of operation of S2 is *slave* and the effective HA operating mode of S2 is *master*.
4. Connect to the web-based manager of P1, go to *System* > *High Availability* > *Status*.
5. Check for synchronization messages.
   Do not proceed to the next step until P1 has synchronized with S2.
6. Connect to the web-based manager of S2, go to *System* > *High Availability* > *Status* and select *click HERE to restore configured operating mode*.

The HA group should return to normal operation. P1 records the event log message (among others) indicating that S2 asked P1 to return to operating as the primary unit.

P1 and S2 synchronize again. P1 processes phone calls normally.

Failover scenario 6: Network connection between primary and secondary units fails (remote service monitoring detects a failure)

Depending on your network configuration, the network connection between the primary and secondary units can fail for a number of reasons. In the network configuration shown in Example active-passive HA group on page 65, the connection between port1 of primary unit (P1) and port1 of the secondary unit (S2) can fail if a network cable is disconnected or if the switch between P1 and S2 fails.

A more complex network configuration could include a number of network devices between the primary and secondary unit’s non-heartbeat network interfaces. In any configuration, remote service monitoring can only detect a communication failure. Remote service monitoring cannot determine where the failure occurred or the reason for the failure.

In this scenario, remote service monitoring has been configured to make sure that S2 can connect to P1. The *On failure* setting located in the HA main configuration section is *wait for recovery then restore slave role*. For information on the *On failure* setting, see On failure on page 60. For information about remote service monitoring, see Configuring service-based monitoring on page 64.

The failure occurs when power to the switch that connects the P1 and S2 port1 interfaces is disconnected. Remote service monitoring detects the failure of the network connection between the primary and secondary units. Because of the *On failure* setting, P1 changes its effective HA operating mode to *failed*.

When the failure is corrected, P1 detects the correction because while operating in failed mode P1 has been attempting to connect to S2 using the port1 interface. When P1 can connect to S2, the effective HA operating mode of P1 changes to *slave* and the voice data on P1 will be synchronized to S2. S2 can now deliver the calls. The HA group continues to operate in this manner until an administrator resets the effective HA modes of operation of the FortiVoice units.

1. The FortiVoice HA group is operating normally.
2. The power cable for the switch between P1 and S2 is accidentally disconnected.
3. S2’s remote service monitoring cannot connect to the primary unit.
   How soon this happens depends on the remote service monitoring configuration of S2.
4. Through the HA heartbeat link, S2 signals P1 to stop operating as the primary unit.
5. The effective HA operating mode of P1 changes to *failed*.
6. The effective HA operating mode of S2 changes to *master*.
7. S2 sends an alert email similar to the following, indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.
   This is the HA machine at 172.16.5.11.

   The following event has occurred
   ‘MASTER remote service disappeared’
   The state changed from ‘SLAVE’ to ‘MASTER’
8. S2 logs the event (among others) indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.
9. P1 sends an alert email similar to the following, indicating that P1 has stopped operating in HA mode.
   This is the HA machine at 172.16.5.10.

   The following event has occurred
   'SLAVE asks us to switch roles (user requested takeover)'

The state changed from 'MASTER' to 'FAILED'

10. P1 records the log messages (among others) indicating that P1 is switching to *Failed* mode.

Recovering from a network connection failure

Because the network connection failure was not caused by failure of either FortiVoice unit, you may want to return both FortiVoice units to operating in their configured modes when rejoining the failed primary unit to the HA group.

To return to normal operation after the heartbeat link fails

1. Reconnect power to the switch.
   Because the effective HA operating mode of P1 is *failed*, P1 is using remote service monitoring to attempt to connect to S2 through the switch.
2. When the switch resumes operating, P1 successfully connects to S2.
   P1 has determined the S2 can connect to the network and process calls.
3. The effective HA operating mode of P1 switches to *slave*.
4. P1 logs the event.
5. P1 sends an alert email similar to the following, indicating that P1 is switching its effective HA operating mode to *slave*.
   This is the HA machine at 172.16.5.10.
   The following event has occurred
   'SLAVE asks us to switch roles (user requested takeover)'
   The state changed from 'FAILED' to 'SLAVE'
6. Connect to the web-based manager of P1 and go to *System* > *High Availability* > *Status*.
7. Check for synchronization messages.
   Do not proceed to the next step until P1 has synchronized with S2.
8. Connect to the web-based manager of S2, go to *System* > *High Availability* > *Status* and select *click HERE to restore configured operating mode*.
9. Connect to the web-based manager of P1, go to *System* > *High Availability* > *Status* and select *click HERE to restore configured operating mode*.
   P1 should return to operating as the primary unit and S2 should return to operating as the secondary unit.
   P1 and S2 synchronize again. P1 can now process phone calls normally.

Configuring system time, system options, SNMP, email setting, GUI appearance, and call data storage

The *System* > *Configuration* submenu lets you configure the system time, system options, SNMP, email setting, GUI appearance, and call data storage.

This topic includes:

- Configuring the time and date on page 72
- Configuring system options on page 75
- Configuring SNMP queries and traps on page 76
- Configuring email Setting on page 82
- Customizing the GUI appearance on page 84
- Selecting the call data storage location on page 86

Configuring the time and date

The *System* > *Configuration* > *Time* tab lets you configure the system time and date of the FortiVoice unit.

You can either manually set the FortiVoice system time or configure the FortiVoice unit to automatically keep its system time correct by synchronizing with Network Time Protocol (NTP) servers.

For many features to work, including scheduling, logging, and certificate-dependent features, the FortiVoice system time must be accurate.
FortiVoice units support daylight savings time (DST), including recent changes in the USA, Canada and Western Australia.

To configure the system time

1. Go to *System* > *Configuration* > *Time*.
2. Configure the following:

GUI field	Description
System time	Displays the date and time according to the FortiVoice unit's clock at the time that this tab was loaded, or when you last selected the *Refresh* button.
Time zone	Select the time zone in which the FortiVoice unit is located. • *Automatically adjust clock for daylight saving time changes*: Enable to adjust the FortiVoice system clock automatically when your time zone changes to daylight savings time (DST) and back to standard time. When selecting time zone in CLI, use the command `config system time manual` and enter the code before the time zone in Time zone codes for CLI configuration {config system time manual} on page 73.
Set date	Select this option to manually set the date and time of the FortiVoice unit's clock, then select the *Year*, *Month*, *Day, Hour*, *Minute*, and *Second* fields before you click *Apply*. Alternatively, configure *Synchronize with NTP server*.
Synchronize with NTP Server	Select to use a network time protocol (NTP) server to automatically set the system date and time, then configure *Server* and *Sync Interval*. • *Server*: Enter the IP address or domain name of an NTP server. You can add a maximum of 10 NTP servers. The FortiVoice unit uses the first NTP server based on the selection mechanism of the NTP protocol. Click the + sign to add more servers. Click the - sign to remove servers. Note that you cannot remove the last server. To find the NTP servers that you can use, see http://www.ntp.org. • *Sync Interval*: Enter how often, in minutes, the FortiVoice unit should synchronize its time with the NTP server. For example, entering 1440 causes the FortiVoice unit to synchronize its time once a day. Depending on your network traffic, it may take some time for the FortiVoice unit to synchronize its time with the NTP server.

3. Click *Apply*.

Time zone codes for CLI configuration {`config system time manual`}

Code	Time Zone
0	(GMT-12:00) Eniwetok, Kwajalein
1	(GMT-11:00) Midway Island, Samoa
2	(GMT-10:00) Hawaii
3	(GMT-9:00) Alaska
4	(GMT-8:00) Pacific Time (US& Canada)
5	(GMT-7:00) Arizona
6	(GMT-7:00) Mountain Time (US& Canada)
7	(GMT-6:00) Central America
8	(GMT-6:00) Central Time
9	(GMT-6:00) Mexico City
10	(GMT-6:00) Saskatchewan
11	(GMT-5:00) Bogota, Lima, Quito
12	(GMT-5:00) Eastern Time (US & Canada)
13	(GMT-5:00) Indiana (East)
14	(GMT-4:30) Venezuela Standard Time
15	(GMT-4:00) Atlantic Time (Canada)
16	(GMT-4:00) Caracas, La Paz
17	(GMT-4:00) Santiago
18	(GMT-3:30) Newfoundland
19	(GMT-3:00) Brasilia
20	(GMT-3:00) Buenos Aires, Georgetown
21	(GMT-3:00) Greenland
22	(GMT-2:00) Mid-Atlantic
23	(GMT-1:00) Azores
24	(GMT-1:00) Cape Verde Is.
25	(GMT) Casablanca, Monrouia
26	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
27	(GMT+1:00) Amsterdam, Berlia, Bern, Rome, Stockholm, Vienna
28	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
29	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris
30	(GMT+1:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb
31	(GMT+1:00) West Central Africa

Code	Time Zone
32	(GMT+2:00) Athens, Istanbul, Minsk
33	(GMT+2:00) Bucharest
34	(GMT+2:00) Cairo
35	(GMT+2:00) Harare, Pretoria
36	(GMT+2:00) Helsinki, Riga, Tallinn
37	(GMT+2:00) Jerusalem
38	(GMT+3:00) Baghdad
39	(GMT+3:00) Kuwait, Riyadh
40	(GMT+3:00) Moscow, St.Petersburg, Volgograd
41	(GMT+3:00) Nairobi
42	(GMT+3:30) Tehran
43	(GMT+4:00) Abu Dhabi, Muscat
44	(GMT+4:00) Baku, Tbilisi, Yerevan
45	(GMT+4:30) Kabul
46	(GMT+5:00) Ekaterinburg
47	(GMT+5:00) Islamabad, Karachi, Tashkent
48	(GMT+5:30) Calcutta, Chennai, Mumbai, New Delhi
49	(GMT+5:45) Kathmandu
50	(GMT+6:00) Almaty, Novosibirsk
51	(GMT+6:00) Astana, Dhaka
52	(GMT+6:00) Sri Jayawardenepara
53	(GMT+6:30) Rangoon
54	(GMT+7:00)B angkok, Hanoi, Jakarta
55	(GMT+7:00) Krasnoyarsk
56	(GMT+8:00) Beijing, Chong Qing, Hong Kong, Urumgi
57	(GMT+8:00) Irkutsk, Ulaan Bataar
58	(GMT+8:00) Kuala Lumpur, Singapore
59	(GMT+8:00) Perth
60	(GMT+8:00) Taipei
61	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul
62	(GMT+9:00) Yakutsk
63	(GMT+9:30) Adelaide, Darwin
64	(GMT+10:00) Brisbane
65	(GMT+10:00) Canberra, Melbourne, Sydney

Code	Time Zone
66	(GMT+10:00) Guam, Port Moresby, Hobart, Vladivostok
67	(GMT+11:00) Magadan, Solomon Is., New Caledonia
68	(GMT+12:00) Auckland, Wellington
69	(GMT+12:00) Fiji, Kamchatka, Marshall Is.
70	(GMT+13:00) Nuku'alofa
71	(GMT-3:00) Montevideo
72	(GMT+3:00) Minsk

Configuring system options

The *System* > *Configuration* > *Options* tab lets you set the following global Setting:

- system idle timeout
- password enforcement policy
- administration ports on the interfaces

To view and configure the system options

1. Go to *System* > *Configuration* > *Option*.
2. Configure the following:

GUI field	Description
Idle timeout	Enter the amount of time that an administrator may be inactive before the FortiVoice unit automatically logs out the administrator. For better security, use a low idle timeout value, for example, 5 minutes.
Web action host/IP	Enter the host name or IP address from where a email notification is sent to you when a voice mail or fax is delivered to your extension. This IP address is included in the email notification. You can open the link to view or manage the voice mail or fax. If you leave this field empty, port1 IP will be used instead. The value entered here replaces the default *Url host* variable for customizing messages. See Customizing call report and notification email templates on page 106.
Administration Ports	Specify the TCP ports for administrative access on all interfaces. Default port numbers: HTTP: 80 HTTPS: 443 SSH: 22 TELNET: 23

3. Click *Apply*.

Configuring SNMP queries and traps

Go to *System* > *Configuration* > *SNMP* to configure SNMP to monitor FortiVoice system events and thresholds, or a high availability (HA) configuration for failover messages.

To monitor FortiVoice system information and receive FortiVoice traps, you must compile Fortinet proprietary MIBs as well as Fortinet-supported standard MIBs into your SNMP manager. RFC support includes support for most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II). For more information, see FortiVoice MIBs on page 81.

The FortiVoice SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiVoice system information and can receive FortiVoice traps.

The FortiVoice SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Before you can use its SNMP queries, you must enable SNMP access on the network interfaces that SNMP managers will use to access the FortiVoice unit. For more information, see Editing network interfaces on page 40.

This topic includes:

- Configuring an SNMP threshold on page 76
- Configuring email Setting on page 82
- Configuring an SNMP v3 user on page 79

Configuring an SNMP threshold

Configure under what circumstances an event is triggered.

To set SNMP thresholds

1. Go to *System* > *Configuration* > *SNMP.*
2. Configure the following:

GUI field		Description
SNMP agent enabled		Enable to activate the FortiVoice SNMP agent. This must be enabled to accept queries from SNMP managers or send traps from the FortiVoice unit.
Description		Enter a descriptive name for the FortiVoice unit.
Location		Enter the location of the FortiVoice unit.
Contact		Enter administrator contact information.
SNMP Threshold		To change a value in the four editable columns, select the value in any row. It becomes editable. Change the value and click outside of the field. A red triangle appears in the field’s corner and remains until you click *Apply*.
	Trap Type	Displays the type of trap, such as *CPU Usage*.
	Trigger	You can enter either the percent of the resource in use or the number of times the trigger level must be reached before it is triggered. For example, using the default value, if the mailbox disk is 90% or more full, it will trigger.

GUI field		Description
	Threshold	Sets the number of triggers that will result in an SNMP trap. For example, if the CPU level exceeds the set trigger percentage once before returning to a lower level, and the threshold is set to more than one, an SNMP trap will not be generated until that minimum number of triggers occurs during the sample period.
	Sample Period(s)	Sets the time period in seconds during which the FortiVoice unit SNMP agent counts the number of triggers that occurred. This value should **not** be less than the *Sample Freq(s)* value.
	Sample Freq(s)	Sets the interval in seconds between measurements of the trap condition. You will not receive traps faster than this rate, depending on the selected sample period. This value should be less than the *Sample Period(s)* value.
Community		Displays the list of SNMP communities (for SNMP v1 and v2c) added to the FortiVoice configuration. For information on configuring a community, see either Configuring email Setting on page 82 or Configuring an SNMP v3 user on page 79.
	Name	Displays the name of the SNMP community. The SNMP Manager must be configured with this name.
	Status	A green check mark icon indicates that the community is enabled.
	Queries	A green check mark icon indicates that queries are enabled.
	Traps	A green check mark icon indicates that traps are enabled.
User		Displays the list of SNMP v3 users added to the FortiVoice configuration. For information on configuring a v3 user, see Configuring an SNMP v3 user on page 79.
	Name	Displays the name of the SNMP v3 user. The SNMP Manager must be configured with this name.
	Status	A green check mark icon indicates that the user is enabled.
	Queries	A green check mark icon indicates that queries are enabled.
	Traps	A green check mark icon indicates that traps are enabled.
	Security Level	Displays the security level.

3. Click *Apply*.

Configuring an SNMP v1 and v2c community

An SNMP community is a grouping of equipment for SNMP-based network administration purposes. You can add up to three SNMP communities so that SNMP managers can connect to the FortiVoice unit to view system information and receive SNMP traps. You can configure each community differently for SNMP traps and to monitor different events. You can add the IP addresses of up to eight SNMP managers to each community.

To configure an SNMP community

1. Go to *System* > *Configuration* > *SNMP*.
2. Under *Community*, click *New* to add a community or select a community and click *Edit*.
   The *SNMP Community* page appears.
3. Configure the following:

GUI field		Description
Name		Enter a name to identify the SNMP community. If you are editing an existing community, you cannot change the name. You can add up to 16 communities.
Enable		Enable to send traps to and allow queries from the community's SNMP managers.
Community Hosts		Lists SNMP managers that can use the Setting in this SNMP community to monitor the FortiVoice unit. Click *Create* to create a new entry. You can add up to 16 hosts.
	IP Address	Enter the IP address of an SNMP manager. By default, the IP address is 0.0.0.0, so that any SNMP manager can use this SNMP community.
	Create (button)	Click to add a new default entry to the *Hosts* list that you can edit as needed.
	Delete (button)	Click to remove this SNMP manager.
Queries		Enter the *Port* number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiVoice unit. Mark the *Enable* check box to activate queries for each SNMP version.
Traps		Enter the *Local Port* and *Remote Port* numbers (162 local, 162 remote by default) that the FortiVoice unit uses to send SNMP v1 and SNMP v2c traps to the SNMP managers in this community. Enable traps for each SNMP version that the SNMP managers use. Enable each SNMP event for which the FortiVoice unit should send traps to the SNMP managers in this community. Since FortiVoice checks its status in a scheduled interval, not all the events will trigger traps. For example, FortiVoice checks its hardware status every 60 seconds. This means that if the power is off for a few seconds but is back on before the next status check, no system event trap will be sent.

4. Click *Create*.

Configuring an SNMP v3 user

SNMP v3 adds more security by using authentication and privacy encryption. You can specify an SNMP v3 user on FortiVoice so that SNMP managers can connect to the FortiVoice unit to view system information and receive SNMP traps.

To configure an SNMP v3 user

1. Go to *System* > *Configuration* > *SNMP*.
2. Under *User*, click *New* to add a user or select a user and click *Edit*.
   The *SNMPv3 User* page appears.
   You can add up to 16 users.

3. Configure the following:

GUI field		Description
User name		Enter a name to identify the SNMP user. If you are editing an existing user, you cannot change the name.
Enable		Enable to send traps to and allow queries from the user's SNMP managers.
Security level		Choose one of the three security levels: • *No authentication, no privacy*: This option is similar to SNMP v1 and v2. • *Authentication, no privacy*: This option enables authentication only. The SNMP manager needs to supply a password that matches the password you specify on FortiVoice. You must also specify the authentication protocol (either SHA1 or MD5). • *Authentication, privacy*: This option enables both authentication and encryption. You must specify the protocols and passwords. Both the protocols and passwords on the SNMP manager and FortiVoice must match.
	Authentication Protocol	For *Security level*, if you select either *Authentication* option, you must specify the authentication protocol and password. Both the authentication protocol and password on the SNMP manager and FortiVoice must match.
	Privacy protocol	For *Security level*, if you select *Privacy*, you must specify the encryption protocol and password. Both the encryption protocol and password on the SNMP manager and FortiVoice must match.
Notification Hosts		Lists the SNMP managers that FortiVoice will send traps to. Click *Create* to create a new entry. You can add up to 16 host.
	IP Address	Enter the IP address of an SNMP manager. By default, the IP address is 0.0.0.0, so that any SNMP manager can use this SNMP user.
	Create (button)	Click to add a new default entry to the *Hosts* list that you can edit as needed.
	Delete (button)	Click to remove this SNMP manager.
Queries		Double click the default port number (161) to enter the *Port* number that the SNMP managers use for SNMP v3 queries to receive configuration information from the FortiVoice unit. Select the *Enable* check box to activate queries.
Traps		Double click the default local port (162) and remote port number (162) to enter the *Local Port* and *Remote Port* numbers that the FortiVoice unit uses to send SNMP v3 traps to the SNMP managers. Select the *Enable* check box to activate traps.

GUI field	Description
	Enable each SNMP event for which the FortiVoice unit should send traps to the SNMP managers. Not all events trigger traps because the FortiVoice unit checks its status at a scheduled interval. For example, FortiVoice checks its hardware status every 60 seconds. This means that if the power is off for a few seconds but is back on before the next status check, no system event trap will be sent.

4. Click *Create*.

FortiVoice MIBs

The FortiVoice SNMP agent supports Fortinet proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiVoice unit configuration.

The FortiVoice MIBs are listed in FortiVoice MIBs on page 81. You can obtain these MIB files from Fortinet technical support. To communicate with the SNMP agent, you must compile these MIBs into your SNMP manager.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database. If the standard MIBs used by the Fortinet SNMP agent are already compiled into your SNMP manager you do not have to compile them again.

FortiVoice MIBs

MIB file name	Description
FortiVoice.mib	Displays the proprietary Fortinet MIB includes detailed FortiVoice system configuration information. Your SNMP manager requires this information to monitor FortiVoice configuration Setting. For more information, see MIB fields on page 81.

FortiVoice traps

The FortiVoice unit's SNMP agent can send traps to SNMP managers that you have added to SNMP communities. To receive traps, you must load and compile the FortiVoice trap MIB into the SNMP manager.

All traps sent include the trap message as well as the FortiVoice unit serial number and host name.

MIB fields

Trap	Description
fvTrapStorageDiskHighThreshold	Trap sent if log disk usage and mailbox disk usage become too high.
fvTrapSystemEvent	Trap sent when system shuts down, reboots, upgrades, etc.
fmlTrapHAEvent	Trap sent when an HA event occurs.

The Fortinet MIB contains fields reporting current FortiVoice unit status information. The tables below list the names of the MIB fields and describe the status information available for each. You can view more details about the information available from all Fortinet MIB fields by compiling the MIB file into your SNMP manager and browsing the MIB fields.

System session MIB fields

MIB field	Description
fvSysModel	FortiVoice model number, such as 400 for the FortiVoice-400.
fvSysSerial	FortiVoice unit serial number.
fvSysVersion	The firmware version currently running on the FortiVoice unit.
fvSysCpuUsage	The current CPU usage (%).
fvSysMemUsage	The current memory utilization (%).
fvSysLogDiskUsage	The log disk usage (%).
fvSysStorageDiskUsage	The storage disk usage (%).
fvSysEventCode	System component events.
fvSysload	Current system load.
fvSysHA	• fvHAMode: Configured HA operating mode. • fvHAEffectiveMoce: Effective HA operating mode.
fmlHAEventId	HA event type ID.
fmlHAUnitIp	Unit IP address where the event occurs.
fmlHAEventReason	The reason for the HA event.

Configuring email Setting

You can configure the FortiVoice unit to send email notifications to phone users when they miss a phone call or receive a voicemail or fax.

For phone users to receive the notifications, you need to add their email addresses when configuring the extensions. See Configuring Extensions on page 156.

To configure email Setting

1. Go to *System > Configuration > Mail Setting*.
2. Configure the following:

GUI field	Description
Local Host	

GUI field		Description
	Host name	Enter the host name of the FortiVoice unit, such as `fortivoice-200D`.
	Local domain name	Enter the local domain name of the FortiVoice unit, such as `example.com`.
Mail Queue		
	Maximum time for email in queue (1-240 hours)	Enter the maximum number of hours that deferred email messages can remain in the deferred email queue, during which the FortiVoice unit periodically retries to send the message. After it reaches the maximum time, the FortiVoice unit sends a final delivery status notification (DSN) email message to notify the sender that the email message was undeliverable.
	Time interval for retry (10-120 minutes)	Enter the number of minutes between delivery retries for email messages in the deferred mail queues.
Relay Server		Configure an SMTP relay, if needed, to which the FortiVoice unit will relay outgoing email. This is typically provided by your Internet service provider (ISP), but could be a mail relay on your internal network.
	Relay server name	Enter the domain name of an SMTP relay.
	Relay server port	Enter the TCP port number on which the SMTP relay listens. This is typically provided by your Internet service provider (ISP).
	Use SMTPs	Enable to initiate SSL- and TLS-secured connections to the SMTP relay if it supports SSL/TLS. When disabled, SMTP connections from the FortiVoice unit's built-in MTA or proxy to the relay will occur as clear text, unencrypted. This option must be enabled to initiate SMTPS connections.

	Authentication Required	Select the checkbox and click the arrow to expand the section and configure:
		• *User name*: Enter the name of the FortiVoice unit's account on the SMTP relay.
		• *Password*: Enter the password for the FortiVoice unit's user name.
		• *Authentication type*: Available SMTP authentication types include:
		    • *AUTO* (automatically detect and use the most secure SMTP authentication type supported by the relay server)
		    • *PLAIN* (provides an unencrypted, scrambled password)
		    • *LOGIN* (provides an unencrypted, scrambled password)
		    • *DIGEST-MD5* (provides an encrypted hash of the password)
		    • *CRAM-MD5* (provides an encrypted hash of the password, with hash replay prevention, combined with a

GUI field	Description
	challenge and response mechanism)
Customize Email Template	View and reword the default email history report and notification email templates. For more information, see Customizing call report and notification email templates on page 106.

3. Click *Apply*.

Customizing the GUI appearance

The *System* > *Configuration* > *Appearance* tab lets you customize the default appearance of the web-based manager and voicemail interface with your own product name, product logo, corporate logo, and language.

To customize the GUI appearance

1. Go to *System* > *Configuration* > *Appearance*.
2. Click the arrow to expand *Administration interface* and *Voicemail interface*.

3. Configure the following change appearance:

GUI field	Description
Administration interface	
Product name	Enter the name of the product. This name will precede *Administrator Login* in the title on the login page of the web-based manager.
Product icon	Click *Change* to browse for the product icon. The icon should be in .ico format, and 16 pixels wide x16 pixels tall in size.
Top logo	Click *Change* to upload a graphic that will appear at the top of all pages in the web-based manager. The image's dimensions must be 460 pixels wide by 36 pixels tall. For best results, use an image with a transparent background. Non-transparent backgrounds will not blend with the underlying theme graphic, resulting in a visible rectangle around your logo graphic. Uploading a graphic overwrites the current graphic. The Fort iVoice unit does not retain previous or default graphics. If yo u want to revert to the current graphic, use your web browser to save a backup copy of the image to your management co mputer, enabling you to upload it again at a later time. Click *Reset* to return to the default setting.
Default UI language	Select the default language for the display of the web-based manager. You can configure a separate language preference for each administrator account. For details, see Configuring administrator accounts on page 46.
Default theme	Select the default theme for the web-based manager GUI.
Voicemail interface	
Voicemail login	Enter a word or phrase that will appear on top of the web user portal login page, such as Voicemail Login.
Login user name hint	Enter a hint for the user name, such as Your Email Address. This hint will appear as a mouse-over display on the login name field.
Voicemail theme	Select a theme for the web user portal GUI.
Default UI language	Select the language in which web user portal pages will be displayed. By default, the FortiVoice unit will use the same language as the web-based manager
Voicemail top logo	Click *Change* to upload a graphic that will appear at the top of all web user portal pages. The image's dimensions must be 460 pixels wide by 36 pixels tall. For best results, use an image with a transparent background. Non-transparent backgrounds will not blend with the underlying theme graphic, resulting in a visible rectangle around your logo graphic.

GUI field	Description
	Uploading a graphic overwrites the current graphic. The FortiVoice unit does not retain previous or default graphics. If you want to revert to the current graphic, use your web browser to save a backup copy of the image to your management computer, enabling you to upload it again at a later time. Click *Reset* to return to the default setting.

4. Click *Apply* to save changes or *Reset* to return to the default Setting.

Selecting the call data storage location

The *System* > *Configuration* > *Storage* tab lets you configure local or remote storage of call data such as the recorded calls, faxes, and voice mails.

FortiVoice units can store call data either locally or remotely. FortiVoice units support remote storage by a network attached storage (NAS) server using the network file system (NFS) protocol.

NAS has the benefits of remote storage which include ease of backing up the call data and more flexible storage limits. Additionally, you can still access the call data on the NAS server if your FortiVoice unit loses connectivity.

If the FortiVoice unit is a member of an active-passive HA group, and the HA group stores call data on a remote NAS server, disable call data synchronization to prevent duplicate call data traffic. For details, see Configuring the HA mode and group on page 59.

If you store the call data on a remote NAS device, you cannot back up the data. You can only back up the call data stored locally on the FortiVoice hard disk. For information about backing up call data, see Backing up configuration on page 100.

Tested and Supported NFS servers

- Linux NAS (NFS v3/v4)
  - Red Hat 5.5
  - Fedora 16/17/18/19
  - Ubuntu 11/12/13
  - OpenSUSE 13.1
- FreeNAS
- Openfiler
- EMC VNXe3150 (version 2.4.2.21519(MR4 SP2))
- EMC Isilon S200 (OneFS 7.1.0.3)

Untested NFS servers

- Buffalo TeraStation
- Cisco Linksys NAS server

Non-Supported NFS Servers

- Windows 2003 R2 /Windows 2008 Service for NFS

To configure call data storage

1. Go to *System* > *Configuration* > *Storage*.
2. Configure the following:

GUI field		Description
Local		Select to store call data on the FortiVoice unit's local disk or RAID.
NAS		Select to store call data on a remote network attached storage (NAS) server.

	Storage type	Select a type of the NAS server:
		• *NFS*: To configure a network file system (NFS) server. For this option, enter the following information:
		  ◦ *Hostname/IP address*: the IP address or fully qualified domain name (FQDN) of the NFS server.
		  ◦ *Port*: the TCP port number on which the NFS server listens for connections.
		  ◦ *Directory*: the directory path of the NFS export on the NAS server where the FortiVoice unit will store call data.
		• *iSCSI Server*: To configure an Internet SCSI (Small Computer System Interface) server. For this option, enter the following information:
		  ◦ *Initiator name as username:* Select to use the iSCSI initiator node name as the user name of the FortiVoice unit's account on the iSCSI server.
		  ◦ *Username*: the user name of the FortiVoice unit's account on the iSCSI server.
		  ◦ *Password*: the password of the FortiVoice unit's account on the iSCSI server.
		  ◦ *Hostname/IP address*: the IP address or fully qualified domain name (FQDN) of the iSCSI server.
		  ◦ *Port*: the TCP port number on which the iSCSI server listens for connections.
		  ◦ *Encryption key*: the key that will be used to encrypt data stored on the iSCSI server. Valid key lengths are between 6 and 64 single-byte characters.
		  ◦ *iSCSI ID*: the iSCSI identifier in the format expected by the iSCSI server, such as an iSCSI Qualified Name (IQN), Extended Unique Identifier (EUI), or T11 Network Address Authority (NAA).
		Status: When available, it indicates if the iSCSI share was successfully mounted on the FortiVoice unit's file system. This field appears only after you configure the iSCSI share and click *Apply*. *Status* may take some time to appear if the iSCSI server is slow to respond.

GUI field	Description
	If *Not mounted* appears, the iSCSI share was not successfully mounted. Verify that the iSCSI server is responding and the FortiVoice unit has both read and write permissions on the iSCSI server.
Test (button)	Click to verify the NAS server Setting are correct and that the FortiVoice unit can access that location. The test action basically tries to discover, login, mount, and unmount the remote device. This button is available only when *NAS server* is selected.
Click here to format this device Click here to check file system on this device	These two links appear when you configure an iSCSI server and click *Apply*. Click a link to initiate the described action (that is, format the device or check its file system). A message appears saying the action is being executed. Click OK to close the message and click *Refresh* to see a *Status* update. If the ISCSI disk has never been formatted, the FortiVoice unit needs to format it before it can be used. If the disk has been formatted before, you do not need to format it again. unless you want to wipe out the data on it.

Configuring advanced phone system settings

The *System* > *Advanced* submenu lets you configure SIP setting, SIP phone auto-provisioning, prompt languages, phone management, and system capacity.

This topic includes:

- Configuring SIP settings on page 88
- Configuring the internal ports on page 90
- Configuring external access on page 90
- Configuring SIP phone auto-provisioning on page 91

Configuring SIP settings

FortiVoice units support SIP communications.

To configure FortiVoice SIP Setting

1. Go *System* > *Advanced* > *SIP.*
2. Configure the following:

GUI field		Description
SIP Transport/Internal Ports		SIP communication commonly uses TCP or UDP port 5060 and/or 5061. Port 5060 is used for nonencrypted SIP signaling sessions and port 5061 is typically used for SIP sessions encrypted with Transport Layer Security (TLS). Enter the ports as required.
RTP Setting		
	Port	Enter the starting Real-time Transport Protocol (RTP) port that the FortiVoice unit will use for phone call sessions. If the unit is behind a firewall, these ports should be open. Ensure there is a reasonable port range so that you have enough ports for all open calls. The default port is 5000. Enter the end RTP port that the FortiVoice unit will use for phone call sessions. Ensure there is a reasonable port range so that you have enough ports for all open calls. The default port is 30000.
	Timeout	Enter the amount of time in seconds during an active call that the extension will wait for RTP packets before hanging up the call. 0 means no time limit. The default is 60.
	Hold timeout	Enter the amount of time in seconds that the extension will wait on hold for RTP packets before hanging up the call. 0 means no time limit. The default is 300.
Registration/Subscription Interval		If this is a dynamic account with the VoIP provider, enter the registration interval as required by the VoIP provider. After each registration interval, the FortiVoice unit renews the registration of the account with the VoIP provider.
	Extension registration/subscription interval range	To keep the extensions' registration status with the FortiVoice unit, enter the range of extension registration time interval as required by the FortiVoice unit in minutes. An extension's registration timeout setting is overridden by the FortiVoice unit's extension registration time interval range if it is out of the range. The default range is 1-480. The start of the range is 1-60 and the end of the range is 30-1440.
	Internal extension registration/subscrip tion interval	Enter the default registration time interval for the extensions on your subnet as required by the FortiVoice unit in minutes. The default is 30 and the range is 10-480. Set a proper value for this option. If it is too low, the performance of the FortiVoice unit is compromised due to frequent registration. If it is too high, the connection between the FortiVoice unit and the extension may terminate.

GUI field		Description
	External extension registration/subscription interval	Enter the default registration time interval for the extensions on other subnets as required by the FortiVoice unit in seconds. The default is 30 and the range is 10-1800. Set a proper value for this option. The FortiVoice unit requires that external extensions register more frequently with it to keep the connection. However, if the value is set too low, the performance of the FortiVoice unit is compromised due to frequent registration. If it is too high, the connection between the FortiVoice unit and the extension may terminate.
Security		By default, the FortiVoice unit screens out incoming calls from unauthenticated source. If you want to change this default setting, select *Accept unauthenticated incoming call*.
Advanced Setting		*SIP session helper*: Select if you do not want the FortiVoice unit to apply NAT or other SIP session help features to SIP traffic. With the SIP session helper disabled, the FortiVoice unit can still accept SIP sessions if they are allowed by a security policy, but the FortiVoice unit will not be able to open pinholes or NAT the addresses in the SIP messages. *Internal network*: Identify the internal networks designated for phone calls on the FortiVoice unit. When a call reaches the public IP address of the FortiVoice unit, it will be routed to one of the internal networks. Note that modifying internal networks terminate ongoing calls. This option is only available if you select *SIP session helper.*

3. Click *Apply*.

Configuring the internal ports

System > *Advanced* > *Service* lets you configure the FortiVoice unit listening ports for network communications.

To configure internal port Setting

1. Go to *System* > *Advanced* > *Service.*
2. Change the default *HTTP* and *HTTPS* port numbers if required.
3. Enable *TFTP* port if required.
   TFTP connection is **not** secure, and can be intercepted by a third party.
4. Other ports are predefined and cannot be changed.
5. Click *Apply*.

Configuring external access

System > *Advanced* > *External Access* lets you configure the FortiVoice unit external hostname/IP and ports through which it can be accessed by other devices through the internet.

When external extensions connect to the FortiVoice unit, they get the basic PBX configurations including the external access IP and ports through auto provisioning. They can then use the information to register with the FortiVoice unit. For more information, see Configuring SIP phone auto-provisioning on page 91.

Extensions are defined as external in extension configuration. For more information, see Configuring IP extensions on page 156.

To configure external access

1. Go to *System* > *Advanced* > *External Access* and configure the following:

GUI field	Description
SIP server external hostname/IP address	Enter the hostname/IP for your SIP server external access.
SIP External Ports	Enter the external access ports for SIP transport. WSS (WebSocket Secure) is used to support FortiFone desktop application.
Other service external hostname/IP address	If you have another service for external access, enter the hostname/IP.
Service External Ports	Enter the external access ports for the other service.

2. Click *Apply*.

Configuring SIP phone auto-provisioning

System > *Advanced* > *Auto Provisioning* allows the FortiVoice unit to discover the SIP phones on your network and send the configuration files to them.

With auto-provisioning configured, when a supported FortiFone is connected to the network and powered on, it is automatically discovered and receives the configuration file from the FortiVoice unit. The FortiFone will then reboot with the pushed-in configuration file and register with the FortiVoice unit.

The FortiVoice unit can only auto provision the supported FortiFones.

To configure auto-provisioning Setting

1. Go to *System* > *Advanced* > *Auto Provisioning* and configure the following:

GUI field		Description
Auto Provisioning		
	Enabled	Select to activate the SIP phone auto-provisioning function for auto discovering the phones.
	Unassigned phone (Generate default configuration for unassigned Desktop FortiFone)	Select to generate basic phone configuration files for the supported unassigned SIP Desktop FortiFones. For details, see Viewing desktop FortiFones on page 27. With this option selected, once a supported FortiFone connects to the FortiVoice unit and is auto-discovered, the FortiVoice unit sends the basic PBX setup information to it for registering with the FortiVoice unit to be assigned an extension. If you want to upgrade your phone system and keep the current phone configuration, ***do not*** select this option. Otherwise your existing phone configuration will be overridden by the upgraded FortiVoice configuration.
	Provisioning protocol	Select the protocol for the phones to retrieve the configuration file from the FortiVoice unit.
	Server Setting for Phone Configuration	If you use different servers for SIP, NTP, and LDAP, select to configure the Setting of each server for the supported phones. The servers' port information reflect the FortiVoice unit's network interfaces. For details, see Configuring the network interfaces on page 39. • *SIP server:* Select or click *Override*to enter the current public IP address or public domain name of the server. The SIP phones connect to this server to register. • *NTP server*: Select or click *Override* to enter the current public IP address or public domain name of the server. The SIP phones connect to this server to synchronize time. • *LDAP contact*: Select or click *Override* to enter the current public IP address or public domain name of the server. The SIP phones connect to this server to receive phone directories. • *Provisioning server*: If you use a specific server to send PBX setup information to the phones, select or click *Override* to enter the current public IP address or public domain name of the server. The SIP phones connect to this server to receive the full PBX setup information.
Auto Discovery		If phone auto discovery is required, enable SIPPnP multicast function for the connected phones to find the provisioning server contained in its message for the phones.

GUI field		Description
		You can also click the DHCP server link to select or add a server that contains provisioning server information in its message for the phones to look for. For more information, see Configuring DHCP server on page 44. SIPPnP multicast and DHCP server do not conflict although SIPPnP has priority. Phones can retrieve provisioning server information from either of the two.
Other Setting		
	Secondary account (Enable secondary account for Desktop FortiFone)	In addition to the main account, secondary accounts can be added on the same FortiVoice unit. Select this option in order to add a secondary account when configuring extensions. For details, see Advanced on page 159
	Administrator PIN to provision phone	Click and enter a global password to be used by an administrator to connect a FortiFone to the FortiVoice unit to set mobile extension number. This password is also used by the administrator to override schedules. For details, see Configuring system capacity on page 107. For example, you can press the default Configure Phone feature code *17 (See Modifying feature access codes on page 271) on any FortiFone that connects to the FortiVoice unit and enter this password. You can then enter an existing extension to set it as the extension of this phone.
	Phone firmware upgrade schedule	Select a schedule profile to upgrade phone firmware. For more information, see Scheduling the FortiVoice unit on page 131. This is the same configuration as in Managing firmwares on page 151. If the upgrade schedule is changed in one place, both places are affected.
	Backward support of legacy FortiFone (FON 360/460/560) (Obsolescent)	If you have legacy FortiFones, select this option for backward provisioning support.

2. Click *Apply*.

Managing certificates

This section explains how to manage X.509 security certificates using the FortiVoice web-based manager. Using the *Certificate* submenu, you can generate certificate requests, install signed certificates, import CA root certificates and certificate revocation lists, and back up and restore installed certificates and private keys.

The FortiVoice unit uses certificates for PKI authentication in secure connections. PKI authentication is the process of determining if a remote host can be trusted with access to network resources. To establish its trustworthiness, the remote host must provide an acceptable authentication certificate by obtaining a certificate from a certification authority (CA).

You can manage the following types of certificates on the FortiVoice unit:

Certificate type	Usage
Server certificates	The FortiVoice unit must present its local server certificate for the following secure connections: • the web-based manager (HTTPS connections only) • phone user web interface (HTTPS connections only) • phone and FortiVoice unit (TLS and SRTP connections only), see Configuring SIP profiles on page 115. For details, see Managing local certificates on page 94.
CA certificates	The FortiVoice unit uses CA certificates to authenticate the PKI users, including administrators and phone users. For details, see Managing certificate authority certificates on page 99.
Personal certificates	Phone users' personal certificates are used for S/MIME encryption.

This section contains the following topics:

- Managing local certificates on page 94
- Obtaining and installing a local certificate on page 95
- Managing certificate authority certificates on page 99
- Managing the certificate revocation list on page 99

Managing local certificates

System > Certificate > Local Certificate displays both the signed server certificates and unsigned certificate requests.

On this tab, you can also generate certificate signing requests and import signed certificates in order to install them for local use by the FortiVoice unit.

FortiVoice units require a local server certificate that it can present when clients request secure connections, including:

- the web-based manager (HTTPS connections only)
- phone user web interface (HTTPS connections only)

To view local certificates, go to *System > Certificate > Local Certificate*.

GUI field	Description
View	Select a certificate and click *View* to display its issuer, subject, and range of dates within which the certificate is valid.
Generate	Click to generate a local certificate request. For more information, see Generating a certificate signing request on page 95.
Download	Click the row of a certificate file or certificate request file in order to select it, then click this button and select either: • *Download*: Download a certificate (.cer) or certificate request (.csr) file. You can send the request to your certificate authority (CA) to obtain a signed certificate for the FortiVoice unit. For more information, see Downloading a certificate signing request on page 97. • *Download PKCS12 File*: Download a PKCS #12 (.p12) file. For details, see

GUI field	Description
	Downloading a PKCS #12 certificate on page 99.
Assign to	Click the row of a certificate in order to select it, then click this button to assign it to a service.
Import	Click to import a signed certificate for local use. For more information, see Importing a certificate on page 98.

Obtaining and installing a local certificate

There are two methods to obtain and install a local certificate:

- If you already have a signed server certificate (a backup certificate, a certificate exported from other devices, and so on), you can import the certificate into the FortiVoice unit. For details, see Importing a certificate on page 98
- Generate a certificate signing request on the FortiVoice unit, get the request signed by a CA, and import the signed certificate into the FortiVoice unit.

For the second method, follow these steps:

- Generating a certificate signing request on page 95
- Downloading a certificate signing request on page 97
- Submitting a certificate request to your CA for signing on page 97
- Importing a certificate on page 98

Generating a certificate signing request

You can generate a certificate request file, based on the information you enter to identify the FortiVoice unit. Certificate request files can then be submitted for verification and signing by a certificate authority (CA).

For other related steps, see Obtaining and installing a local certificate on page 95.

To generate a certificate request

1. Go to *System >Certificate > Local Certificate*.
2. Click *Generate*.
   A dialog appears.
3. Configure the following:

GUI field		Description
Certification name		Enter a unique name for the certificate request, such as fvlocal.
Subject Information		Information that the certificate is required to contain in order to uniquely identify the FortiVoice unit.
	Certification name	Select the type of identifier to be used in the certificate to identify the FortiVoice unit: • *Host IP* • *Domain name* • *E-mail*

GUI field		Description
		Which type you should select varies by whether or not your FortiVoice unit has a static IP address, a fully-qualified domain name (FQDN), and by the primary intended use of the certificate. For example, if your FortiVoice unit has both a static IP address and a domain name, but you will primarily use the local certificate for HTTPS connections to the web-based manager by the domain name of the FortiVoice unit, you might prefer to generate a certificate based on the domain name of the FortiVoice unit, rather than its IP address. • *Host IP* requires that the FortiVoice unit have a static, public IP address. It may be preferable if clients will be accessing the FortiVoice unit primarily by its IP address. • *Domain name* requires that the FortiVoice unit have a fully-qualified domain name (FQDN). It may be preferable if clients will be accessing the FortiVoice unit primarily by its domain name. • *E-mail* does not require either a static IP address or a domain name. It may be preferable if the FortiVoice unit does not have a domain name or public IP address.
	IP	Enter the static IP address of the FortiVoice unit. This option appears only if *ID type* is *Host IP*.
	Domain name	Type the fully-qualified domain name (FQDN) of the FortiVoice unit. The domain name may resolve to either a static or, if the FortiVoice unit is configured to use a dynamic DNS service, a dynamic IP address. For more information, see Configuring the network interfaces on page 39 and Configuring DNS on page 43. If a domain name is not available and the FortiVoice unit subscribes to a dynamic DNS service, an `unable to verify certificate` message may appear in the user's browser whenever the public IP address of the FortiVoice unit changes. This option appears only if *ID type* is *Domain name*.
	E-mail	Type the email address of the owner of the FortiVoice unit. This option appears only if *ID type* is *E-mail*.
Optional Information		Information that you may include in the certificate, but which is not required.
	Organization unit	Type the name of your organizational unit, such as the name of your department. (Optional) To enter more than one organizational unit name, click the + icon, and enter each organizational unit separately in each field.
	Organization	Type the legal name of your organization. (Optional)
	Locality (City)	Type the name of the city or town where the FortiVoice unit is located. (Optional)

GUI field		Description
	State/Province	Type the name of the state or province where the FortiVoice unit is located. (Optional)
	Country	Select the name of the country where the FortiVoice unit is located. (Optional)
	E-mail	Type an email address that may be used for contact purposes. (Optional)
Key type		Displays the type of algorithm used to generate the key. This option cannot be changed, but appears in order to indicate that only RSA is currently supported.
Key size		Select a security key size of *512 Bit*, *1024 Bit*, *1536 Bit* or *2048 Bit*. Larger keys are slower to generate, but provide better security.

4. Click *Create*.
   The certificate is generated, and can be downloaded to your management computer for submission to a certificate authority (CA) for signing. For more information, see Downloading a certificate signing request on page 97.

Downloading a certificate signing request

After you have generated a certificate request, you can download the request file to your management computer in order to submit the request file to a certificate authority (CA) for signing.

For other related steps, see Obtaining and installing a local certificate on page 95.

To download a certificate request

1. Go to *System >Certificate > Local Certificate*.
2. Click the row that corresponds to the certificate request in order to select it.
3. Click *Download*, then select *Download* from the pop-up menu.
   Your web browser downloads the certificate request (.csr) file.

Submitting a certificate request to your CA for signing

After you download the certificate request file, you can submit the request to you CA for signing.

For other related steps, see Obtaining and installing a local certificate on page 95.

To submit a certificate request

1. Using the web browser on the management computer, browse to the website for your CA.
2. Follow your CA’s instructions to place a Base64-encoded PKCS #12 certificate request, uploading your certificate request.
3. Follow your CA’s instructions to download their root certificate and Certificate Revocation List (CRL), and then install the root certificate and CRL on each remote client.
4. When you receive the signed certificate from the CA, install the certificate on the FortiVoice unit. For more information, see Importing a certificate on page 98.

Importing a certificate

You can upload Base64-encoded certificates in either privacy-enhanced email (PEM) or public key cryptography standard #12 (PKCS #12) format from your management computer to the FortiVoice unit.

DER encoding is not supported in FortiVoice version 2.0 GA.

Importing a certificate may be useful when:

- restoring a certificate backup
- installing a certificate that has been generated on another system
- installing a certificate, after the certificate request has been generated on the FortiVoice unit and signed by a certificate authority (CA)

If you generated the certificate request using the FortiVoice unit, after you submit the certificate request to CA, the CA will verify the information and register the contact information in a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA will then sign the certificate and return it to you for installation on the FortiVoice unit. To install the certificate, you must import it. For other related steps, see Obtaining and installing a local certificate on page 95.

If the FortiVoice unit's local certificate is signed by an intermediate CA rather than a root CA, before clients will trust the FortiVoice unit's local certificate, you must demonstrate a link with trusted root CAs, thereby proving that the FortiVoice unit's certificate is genuine. You can demonstrate this chain of trust either by:

- installing each intermediate CA's certificate in the client's list of trusted CAs
- including a signing chain in the FortiVoice unit's local certificate

To include a signing chain, before importing the local certificate to the FortiVoice unit, first open the FortiVoice unit's local certificate file in a plain text editor, append the certificate of each intermediate CA in order from the intermediate CA who signed the FortiVoice unit's certificate to the intermediate CA whose certificate was signed directly by a trusted root CA, then save the certificate. For example, a local certificate which includes a signing chain might use the following structure:

```
-----BEGIN CERTIFICATE-----
<FortiVoice unit's local server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<certificate of intermediate CA 1, who signed the FortiVoice certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<certificate of intermediate CA 2, who signed the certificate of intermediate CA
   1 and whose certificate was signed by a trusted root CA>
-----END CERTIFICATE-----
```

To import a local certificate

1. Go to *System >Certificate > Local Certificate*.
2. Click *Import*.
3. Select the type of the import file or files:
   - *Local Certificate*: Select this option if you are importing a signed certificate issued by your CA. For other related steps, see Obtaining and installing a local certificate on page 95.
   - *PKCS12 Certificate*: Select this option if you are importing an existing certificate whose certificate file and private key are stored in a PKCS #12 (.p12) password-encrypted file.
   - *Certificate*: Select this option if you are importing an existing certificate whose certificate file (.cert) and key file (.key) are stored separately. The private key is password-encrypted.
     The remaining fields vary by your selection in *Type*

4. Configure the following:
   - *Certificate name:* Enter the name of the certificate.
   - *Certificate file*: Enter the location of the previously .cert or .pem exported certificate (or, for PKCS #12 certificates, the .p12 certificate-and-key file), or click *Import* to locate the file.
   - *Key file*: Enter the location of the previously exported key file, or click *Import* to locate the file.
   - This option appears only when *Type* is *Certificate*.
   - *Password*: Enter the password that was used to encrypt the file, enabling the FortiVoice unit to decrypt and install the certificate.
     This option appears only when *Type* is *PKCS12 certificate* or *Certificate*.
5. Click *OK*.

Downloading a PKCS #12 certificate

You can export certificates from the FortiVoice unit to a PKCS #12 file for secure download and import to another platform, or for backup purposes.

To download a PKCS #12 file

1. Go to *System* > *Certificate* > *Local Certificate*.
2. Click the row that corresponds to the certificate in order to select it.
3. Click *Download*, then select *Download PKCS12 File* on the pop-up menu.
   A dialog appears.
4. In *Password* and *Confirm password*, enter the password that will be used to encrypt the exported certificate file. The password must be at least four characters long.
5. Click *OK*.
6. If your browser prompts you for a location to save the file, select a location.
7. Your web browser downloads the PKCS #12 (.p12) file. For information on importing a PKCS #12 file, see Importing a certificate on page 98.

Managing certificate authority certificates

Go to *System* > *Certificate* > *CA Certificate* to view and import certificates for certificate authorities (CA).

Certificate authorities validate and sign other certificates in order to indicate to third parties that those other certificates may be trusted to be authentic.

CA certificates are required by connections that use transport layer security (TLS), and by S/MIME encryption. Depending on the configuration of each PKI user, CA certificates may also be required to authenticate PKI users.

To view the list of CA certificates, go to *System* > *Certificate* > *CA Certificate*. You can remove, view, download, or import a CA certificate.

Managing the certificate revocation list

The *Certificate Revocation List* tab lets you view and import certificate revocation lists.

To ensure that your FortiVoice unit validates only valid (not revoked) certificates, you should periodically upload a current certificate revocation list, which may be provided by certificate authorities (CA).

To view remote certificates, go to *System >Certificate > Certificate Revocation List*. You can remove, view, download, or import a certificate revocation list.

Maintaining the system

The *System > Maintenance* submenu allows you to perform scheduled maintenance.

This topic includes:

- Maintaining the system configuration on page 100
- Downloading a trace file on page 101

Maintaining the system configuration

The *System > Maintenance > Configuration* tab contains features for use during scheduled system maintenance: updates, backups, restoration, and centralized administration.

Backing up configuration

Before installing FortiVoice firmware or making significant configuration changes, back up your FortiVoice configuration. Backups let you revert to your previous configuration if the new configuration does not function correctly. Backups let you compare changes in configuration.

You can back up system configuration or user configuration. System configuration includes the configurations that make the FortiVoice unit work. User configuration includes user-configured Setting, such as voicemail greetings, in addition to system configuration.

In addition to backing up your configuration manually, you can also configure a schedule to back up the configuration automatically to the FortiVoice local hard drive or a remote FTP/SFTP server.

To back up the configuration file

1. Go to *System > Maintenance > Configuration*.
2. In the *Backup* area, select *System configuration* or *User data*.
   If you choose to back up user data and the user data files are not updated, select the files to be updated and click *Prepare* first before proceeding to the next step.
3. Click *Backup*.
   Your management computer downloads the configuration file. Time required varies by the size of the file and the speed of your network connection. You can restore the backup configuration later when required. For details, see Restoring the configuration on page 101.

To schedule a configuration backup

1. Go to *System > Maintenance > Configuration*.
2. Under *Scheduled Backup*, configure the schedule time and the maximum backup number. When the maximum number is reached, the oldest version will be overwritten.
3. Enable *Local backup* if you want to back up locally.
4. Enable *Remote backup* and configure the FTP/SFTP server credentials if you want to back up remotely.
5. Click *Apply*.

Restoring the configuration

In the *Restore Configuration* area under *System* > *Maintenance* > *Configuration* > *Trace Log*, you can restore the backup FortiVoice configuration from your local PC. For details, see Restoring the configuration on page 298.

Restoring the firmware

In the *Restore Firmware* area under *System* > *Maintenance* > *Configuration* > *Trace Log*, you can install a FortiVoice firmware from your local PC. For details, see Installing firmware on page 295.

Downloading a trace file

If Fortinet Technical Support requests a trace log for system analysis purposes, you can download one using the web-based manager.

Trace logs are compressed into an archive (.gz), and contain information that is supplementary to debug-level log files.

To download a trace file

1. Go to *System* > *Maintenance* > *Configuration* > *Trace Log*.
2. Configure *Trace Log* Setting.
3. Click *Prepare* to make the trace log file ready before downloading it.
4. Click *Download trace log*.
   Your web browser downloads trace.log.gz.

Configuring Phone System

The *Phone System* menu lets you configure the FortiVoice PBX Setting and other features for managing phone calls.

This topic includes:

Configuring phone system settings

Phone System > *Setting* let you configure the FortiVoice unit's location, number management, speed dial, email notification templates and system capacity.

You need to inform the users about some of the Setting that affect them, such as number Setting and speed dial Setting.

This topic includes:

Setting PBX location and contact information

Identify the FortiVoice unit's location and its number.

To set the PBX location

1. Go to *Phone System* > *Setting* > *Location*.
2. Configure the following:

GUI field	Description
Country/Region	Select the country/region where the FortiVoice unit is in.
Emergency number	Click the default number (911) to enter the emergency call number of the selected country.

GUI field	Description
Long-distance prefix	Click the default number (1) to enter the prefix for dialing long-distance calls.
International prefix	Click the default number (011) to enter the prefix for dialing international calls.
Outside line prefix	Click the default number (9) to enter the prefix for making outbound calls.
Area code	Click the default number (613) to enter the *Area code* for the main number of the FortiVoice unit. This code is provided by your PSTN service provider.
Required when dialing local numbers	Select this option if the area code needs to be dialed for local phone calls.
Main display name	Enter the name displaying on the FortiVoice unit. This name is provided by your PSTN service provider.
Main number	Enter the main number of the FortiVoice unit. This number is provided by your PSTN service provider.
Default prompt language	Select a new default prompt language for the FortiVoice unit. The default is English. This setting affects all of the FortiVoice unit's voice prompts, such as auto attendant and voice mail. However, if you change the sound file for an individual component, such as auto attendant, to use a different language, it will override the default prompt language for this component. For information on adding prompt languages, see Managing phone audio settings on page 110.
Default emergency zone	Select the default emergency contact or click + to add a new one. For more information, see Configuring emergency zone profiles on page 131.
Default time zone	Select a new default time zone for the FortiVoice unit. The default is Pacific Time.
Contact Information	Optionally, enter your contact information.
Emergency Setting	Configure to send an alert email when an emergency call is made. You can add up to 30 email addresses. Select *Do nothing* if you don't want the FortiVoice unit to send an alert email. Otherwise, select *Send Alert Email* and enter the email address. Click *Customize Email Template* if you want to modify the notification email template. For more information, see Customizing call report and notification email templates on page 106.

3. Click *Apply*.

Configuring PBX options

The *Phone System* > *Setting* > *Option* tab lets you configure the pattern and number of digits you want the FortiVoice unit to use for phone numbers, speed dials, and prefixes as well as the default FortiVoice system Setting. These Setting apply to all extensions unless you change them when configuring the extensions. For details, see Setting up local extensions on page 156.

The FortiVoice unit supports the following pattern-matching syntax:

Syntax	Description
X	Matches any single digit from 0 to 9.
Z	Matches any single digit from 1 to 9.
N	Matches any single digit from 2 to 9.
[15-7]	Matches a single character from the range of digits specified. In this case, the pattern matches a single 1, as well as any number in the range 5, 6, 7.
.	Wildcard match; matches one or more characters, no matter what they are.
!	Wildcard match; matches zero or more characters, no matter what they are.
, ; or (space)	These pattern delimiters allow you to enter multiple pattern strings at a time. For example, you can enter NXXX,6XXXX;[3-5]X

Pattern-matching examples

Pattern	Description
NXXX	Matches any four-digit number, as long as the first digit is 2 or higher.
NXXNXXXXXX	This pattern matches with areas with 10-digit dialing.
1NXXNXXXXXX	Matches the number 1, followed by an area code between 200 and 999, then any seven-digit number. In the North American Numbering Plan calling area, you can use this pattern to match any long-distance number.
011.	Matches any number that starts with 011 and has at least one more digit.

To configure PBX options

1. Go to *Phone System* > *Setting* > *Option*.
2. Configure the following:

GUI field		Description
Number Management		
	Extension number pattern	Enter the extension number pattern. For example, NXXX is any four-digit number as long as the first digit is 2 or higher and 7XXX is a four-digit number that always starts with 7. This pattern will be followed when creating extensions. See Configuring IP extensions on page 156.

GUI field		Description
	Speed dial pattern	Enter the speed dial number pattern. For example, *3XX is any three-digit number that starts with 3. This pattern will be followed when configuring speed dials. See Mapping speed dials on page 255.
	System prohibited prefix	Enter the phone number prefix that you want to ban, such as 900. Click the + sign to add up to 10.
	System unrestricted prefix	Enter the allowed phone number prefix, such as 800. Click the + sign to add up to 10.
	Operator extension	Enter the extension for the operator of the FortiVoice unit.
	Supporting extension	Enter the extension for technical support of the FortiVoice unit.
Default Setting		
	Default SIP user password	Enter your own password or let the FortiVoice unit generate one for you. This password is used for configuring your SIP phone from the phone or the Web. You need the phone's IP to access it from the Web. This password appears when you add an extension. For details, see Configuring IP extensions on page 156. • *Specified*: Enter the password. The password cannot be blank, must be 8 or more characters, must contain at least one uppercase character, one lowercase character and one number. Non-alphanumeric characters, like (- $, are not supported in the password field. The default password is voice#321. • *Generated*: Select to have a system-generated password.
	Default user password	Enter your own password or let the FortiVoice unit generate one for you. This password is for user web portal access. This password appears when you add an extension. For details, see Configuring IP extensions on page 156. • *Specified*: Enter the password. The password cannot be blank, must be 8 or more characters, must contain at least one uppercase character, one lowercase character and one number. Non-alphanumeric characters, like (- $, are not supported in the password field. The default password is voice#321. • *Generated*: Select to have a system-generated password.
	Default Voicemail PIN	Enter your own password or let the FortiVoice unit generate one for you. This password is for the extension user to access voice mail and the user web portal. This password appears when you add an extension. For details, see Configuring IP extensions on page 156. If you select *Specified*, the default password is 123123.

GUI field		Description
	User ID prefix	Enter the prefix for the extension user ID. When you add a new extension, the FortiVoice unit will generate a user ID with this prefix plus the extension number. For details, see Configuring IP extensions on page 156.
	Default ring duration	Enter the time, in seconds, for a phone connected to the FortiVoice unit to ring before the call is processed (for example, the call is sent to voice mail). The default is 20.
	Internal calls ring pattern	Select the system defined distinctive ring pattern.
	External calls ring pattern	Select the system defined distinctive ring pattern.

3. Click *Apply*.

Customizing call report and notification email templates

Go to *Phone System* > *Setting* > *Custom Message* to view and reword the default call report and notification email templates.

The FortiVoice unit sends out call reports based on your call report configuration (see Configuring report email notifications on page 1) and notification email when, for example, you have a new voicemail or fax in your mailbox or missed a call. You can customize the email templates for the call report and email notifications.

You can change the content of the email template by editing the text and HTML codes and by working with email template variables. For descriptions of the default email template variables, open a template and select *Edit Variable*.

To customize call report and email templates

1. Go to *Phone System* > *Setting* > *Custom Message.*
2. Open *Report* or *Email template* to display the default templates.
3. To edit a template, double-click it or select it and click *Edit*.
4. To format template in HTML, use HTML tags, such as `<b>some bold text</b>`.
   There is a limit of 250 characters for the *Subject* field, 60 characters for the *From* field, and 4000 characters for *Htmlbody* and *Textbody* messages each in the *Content body* field.
5. To add a variable:
   - Select *Insert Variables* next to the area to insert a variable. A pop-up window appears.
   - Place your mouse cursor in the text message at the insertion point for the variable.
   - Click the name of the variable to add. It appears at the insertion point.
   - To add another variable, click the message area first, then click the variable name.
   - Click the Close (X) icon to close the window.
6. To insert a color:
   - Click *Insert Color Code.* A pop-up window of color selection appears.
   - Place your mouse cursor in the text at the insertion point for the color code, or highlight an existing color code to change.

- Click a color in the color selection pop-up window.
  For example, to replace the color code in the HTML tag <tr bgcolor="#3366ff">, you can highlight "#3366ff", then select the color you want from the color palette.
  To add a new color code, include it with HTML tags as applicable, such as <tr bgcolor="#3366ff">.

7. To determine if your HTML and color changes are correct, click *Preview*. The replacement message appears in HTML format.
8. Click *OK*, or click *Reset To Default* to revert the replacement message to its default text.

Configuring system capacity

The *Phone System* > *Setting* > *Miscellaneous* tab lets you set the PIN used by the administrator to override schedules, *configure* voicemail greeting and message length, set phone directory options, configure CDR Setting, and configure queue logs.

To configure system capacity

1. Go to *System* >*Setting* > *Miscellaneous.*
2. Configure the following:

GUI field		Description
PBX Setting		
	Administrator PIN	Enter the password used by the administrator to override schedules. This global password is also used by an administrator to connect a FortiFone to the FortiVoice unit to set mobile extension number. For details, see Configuring SIP phone auto-provisioning on page 91.
	PBX identification	Enter a unique name for the FortiVoice unit.
	User portal local authentication type	Select the method to access the user web portal. By default, both personal password and voicemail (user) PIN can be used. Personal password and voicemail (user) PIN are set when configuring extensions. Usually numbers are used as voicemail PIN which are very easy to guess and can be cracked using some HTTP password guess tool within minutes. That is why a separate personal password is added which can be much longer and stronger to mitigate the risk of password guess attack and preserve the voicemail PIN for phone access only. For more information, see Configuring IP extensions on page 156. • *User password or voicemail PIN*: Both personal password and user PIN can be used to access the user web portal. • *User password only:* Use personal password to access the user web portal.
	Notification expiry	Enter the email notification expiry time in hours. The range is 1-2160 hours.

GUI field		Description
	QR code expiry	Enter the QR code expiry time in hours. The range is 1- 2160 hours.
Business Group		Select *Disabled* to hide business group in *Extensions* and select *Automatic* to show it. For more information, see Creating business groups on page 187.
Schedule Override		Select *Allow admin user to override schedule* if required. An administrator with the privilege can dial *821, *822, or *823 followed by the administrator PIN to temporarily replace the original schedule with one of the three default ones. You may also modify the temporary schedule. Dial *820 to go back to the original schedule.
Voicemail		Enter the maximum message length, greeting length, and voicemail volume you want.
Directory		Set phone directory options.
	Dial-by-name option	Select how a caller can check the directory by dialing a name.
	Dial-by-name digits	Enter the number of letters allowed for a caller to dial someone by name. The range is 3-9. This feature enables a caller to reach a specific person quickly by dialing, for example, the first three letters of their first or last name from any phone.
	Read back number	Select if you want a person's extension number to be read out after you check the directory by dialing the person's first or last name.
Internet of Things		
	Amazon Alexa	Select to enable configuring your FortiVoice unit's integration with Amazon Alexa. For more information, see Configuring Internet of Things (IoT) on page 276.
CDR		Enter the time in month that you want to keep the call log/call detail record and the maximum number of CDR records. For information about call log/CDR, see Viewing call records on page 31.
Queue Log		Enter the time in month that you want to keep the queue log and the maximum number of log records. For information about queue logs, see Viewing log messages on page 32.

3. Click *Apply*.

Creating contacts

The *Phone System* > *Contact* menu lets you view and set up phone directories.

You can also configure speed dial rules.

To view the phone directory

1. Go to *Phone System > Contact > Directory.*
   All extensions on this FortiVoice unit are displayed. You can download all contacts or the search result.

To create a contact

1. Go to *Phone System > Contact > Business Contact.*
2. Click *New* and configure the following:

GUI field	Description
Display name	The name displaying on the caller's phone. This is usually the name of the contact.
Main number	Enter the phone number mainly used by the contact.
Mobile number	Enter the contact's cellphone number.
Home number	Enter the contact's home phone number.
Description	Enter any notes for the address book.

3. Click *Create*.

To export a contact

1. Go to *Phone System > Contact > Business Contact.*
2. Select one or more records.
3. Click *Other Actions > Export*.
4. Open or save the file.
5. Click *OK*.

To import a contact

1. Go to *Phone System > Contact > Business Contact.*
2. Click *Other Actions > Import*.
3. Browse for the file you want.
4. Click *OK*.

Configuring speed dials

For fast and efficient dialing, use the speed dial pattern to map the phone numbers, mostly outbound numbers.

For information on setting speed dial number pattern, see Configuring PBX options on page 103.

To map speed dials

1. Go to *Phone System > Contact > Speed Dial Rule*.
2. Click *New*.
3. Enter a name for the speed dial mapping.
4. For *Dialed Pattern*, enter the number based on the speed dial number pattern you set. For example, 333.
5. For *Mapped Pattern*, enter the phone number to map to the speed dial pattern.
   You can enter digits 0–9, space, dash, comma, # and *.
   Speed dial pattern accepts # as the lead digit (Eg. #XX or #613XXX).

If you want to enter an auto attendant number followed by an extension, you can use comma (,) or semicolon (;) to pause the automatic dialing.
A comma pauses dialing for two seconds, for example, 1-123-222-1234, 5678#. In this case, once pressing the speed dial code you set, auto attendant 1-123-1234 is reached, and after two seconds, extension 5678 is automatically dialed.
A semicolon pauses dialing for one second, for example, 1-123-222-1234; 5678#. In this case, once pressing the speed dial code you set, auto attendant 1-123-1234 is reached, and after one second, extension 5678 is automatically dialed.

6. Optionally, enter a note for the mapping, such as “This is for customer A”.
7. Click *Create*.

Managing phone audio settings

The *Phone System* > *Audio* > *Prompt/Music On Hold* menu lets you upload, record, and play phone sound files such as voicemail greetings and announcements. It also lets you choose the sound files to play while a call is on hold.

There are default sound files ready to use.

The sound files can be used when configuring music on hold, conference calls, and auto attendants. See To configure music on hold on page 111 and Configuring Call Features on page 250.

The *Phone System* > *Audio* > *Prompt Language* menu lets you configure the prompt language that affects all of the FortiVoice unit’s voice prompts, such as auto attendant and voicemail. Prompt languages are used when configuring the PBX Setting. For more information, see Setting PBX location and contact information on page 102.

However, if you change the sound file for an individual component, such as auto attendant, to use a different language, it will override the default prompt language for this component.

The default prompt language is English.

For information on generating a prompt language file, see Recording in FortiVoice audio format on page 111.

To manage a sound file

1. Go to *Phone System* > *Audio* > *Prompt*.
2. Click *New*.
3. Enter a name and ID for the file.
4. Select a file type.
5. Optionally, enter a description for the file.
6. For *Voice language*, configure the following:
   If you select *Prompt sound file* for the profile type, you can click *Upload* to get an existing sound file, *Record* to make a sound file, *Download* to save a a sound file, and *Play* to listen to an uploaded or recorded file (with speakers or earphones) for the language you select.
   a. To record a sound file, click *Record*.
   b. On the *Send Voice Recording Call* dialog box, enter the extension that you will use to record the file, and click *Send* to dial the extension. You can edit the extension or add a new one. For details, see Configuring IP extensions on page 156.
   c. When the extension rings, record the sound file and hang up.
   d. On the FortiVoice web-based manager, click *Yes* on the *Voice recording request sent to specified extension* dialog box.

If you select *Music on hold* for the profile type, you can click *Upload* to get an existing sound file, *Record* to make a sound file, *Download* to save a sound file, and *Play* to listen to a uploaded or recorded file (with speakers or earphones).

7. Click *Create*.

To configure music on hold

1. Go to *Phone System* > *Audio* > *Music On Hold*.
2. Click *New*.
3. Configure the following:

GUI field		Description
Name		Enter a name for the music on hold file.
Mode		
	Files	If you select to use existing sound files, do the following: • For *Sound files*, select the *Available* sound files and click -> to move them into the *Selected* field. You can use the *Up* and *Down* buttons to reorder the files. • For *Play mode*, if you want to play the selected sound files randomly, select *Random*. If you want to play the files according to the order in the *Selected* field, select *Sequential*.
	Stream	If you select to use streaming files, in the *Stream URL* field, enter the URL where the streaming music is, such as a radio station. This way, the music is delivered to the FortiVoice unit and played virtually straight away. You can click *Test stream* to see if the URL is added successfully. Before doing so, make sure to only use the legal stream sources.
	Volume	Set the music sound volume.
	Description	Optionally, enter a description for the file.

4. Click *Create*.

To add a prompt language

1. Go to *Phone System* > *Audio* > *Prompt Language*.
2. Click *New*.
3. Click *Upload* to browse and upload the language file in FortiVoice language package format (*.fvl) provided by Fortinet Technical Support.
4. Click *Create*.

Recording in FortiVoice audio format

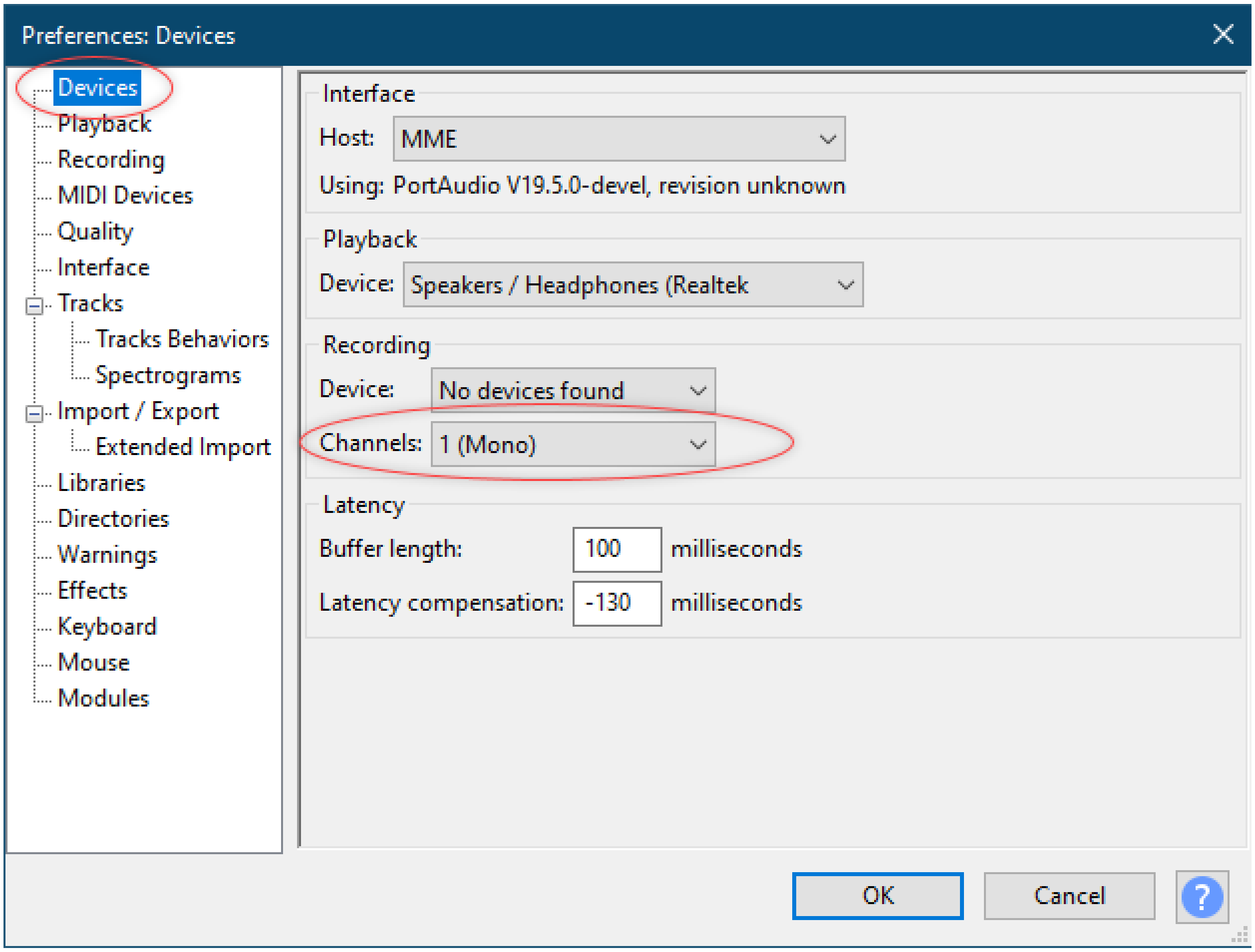
A prompt language file must be recorded in the FortiVoice language package format. This can be accomplished by using the free and robust audio program called Audacity and a microphone.

Once this program has been installed, and the microphone connected, then the file can be recorded.

Audacity cannot natively record in the format that FortiVoice unit requires. Therefore, some adjustments need to be made in the software as described in the following procedure.

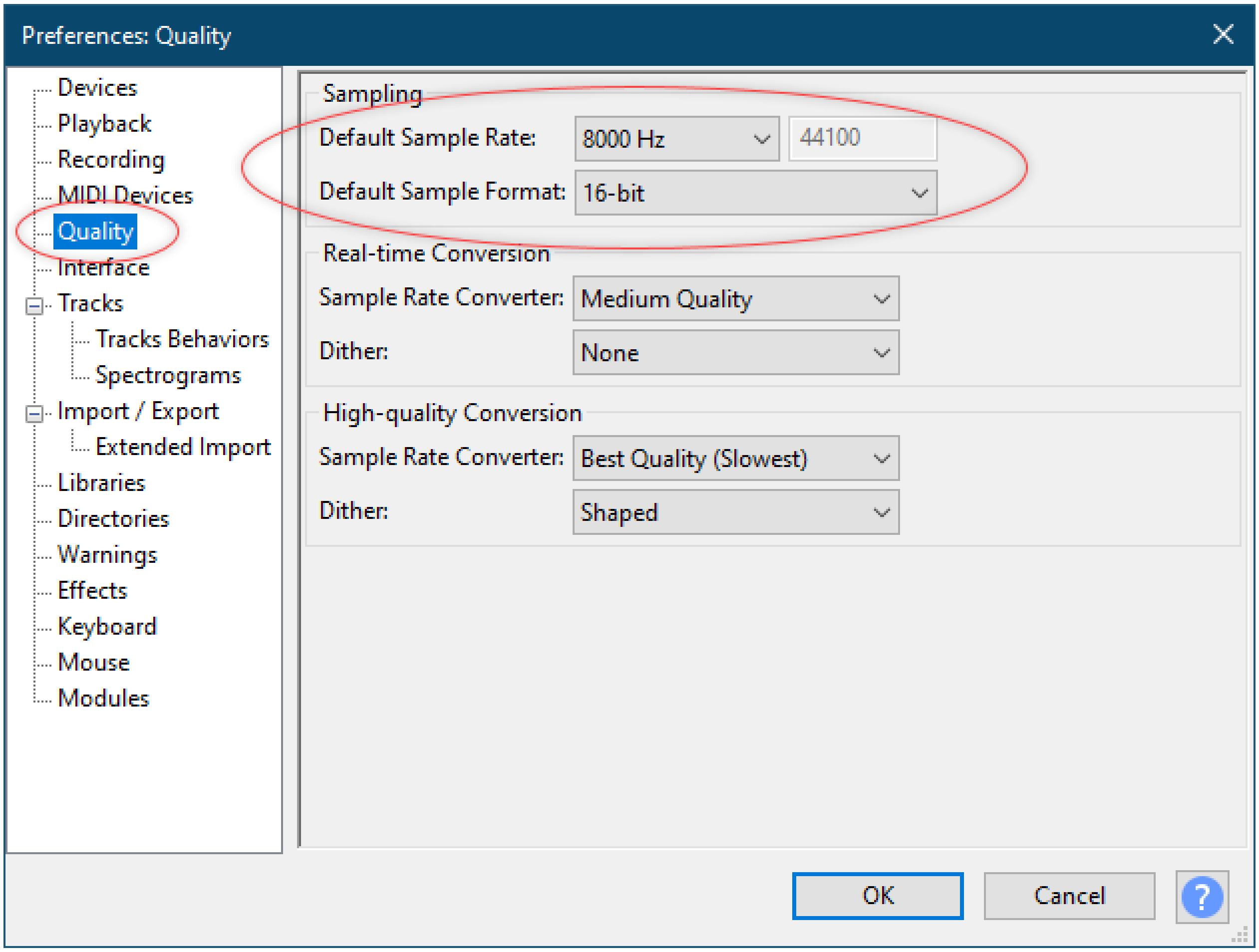
To generate a prompt language file

1. On Audacity, go to *Edit > Preferences*.
2. Click the *Devices* menu.
3. In *Channels*, select *1(Mono)*.



4. Click the *Quality* menu.
5. In *Default Sample Rate*, select 8000 Hz.

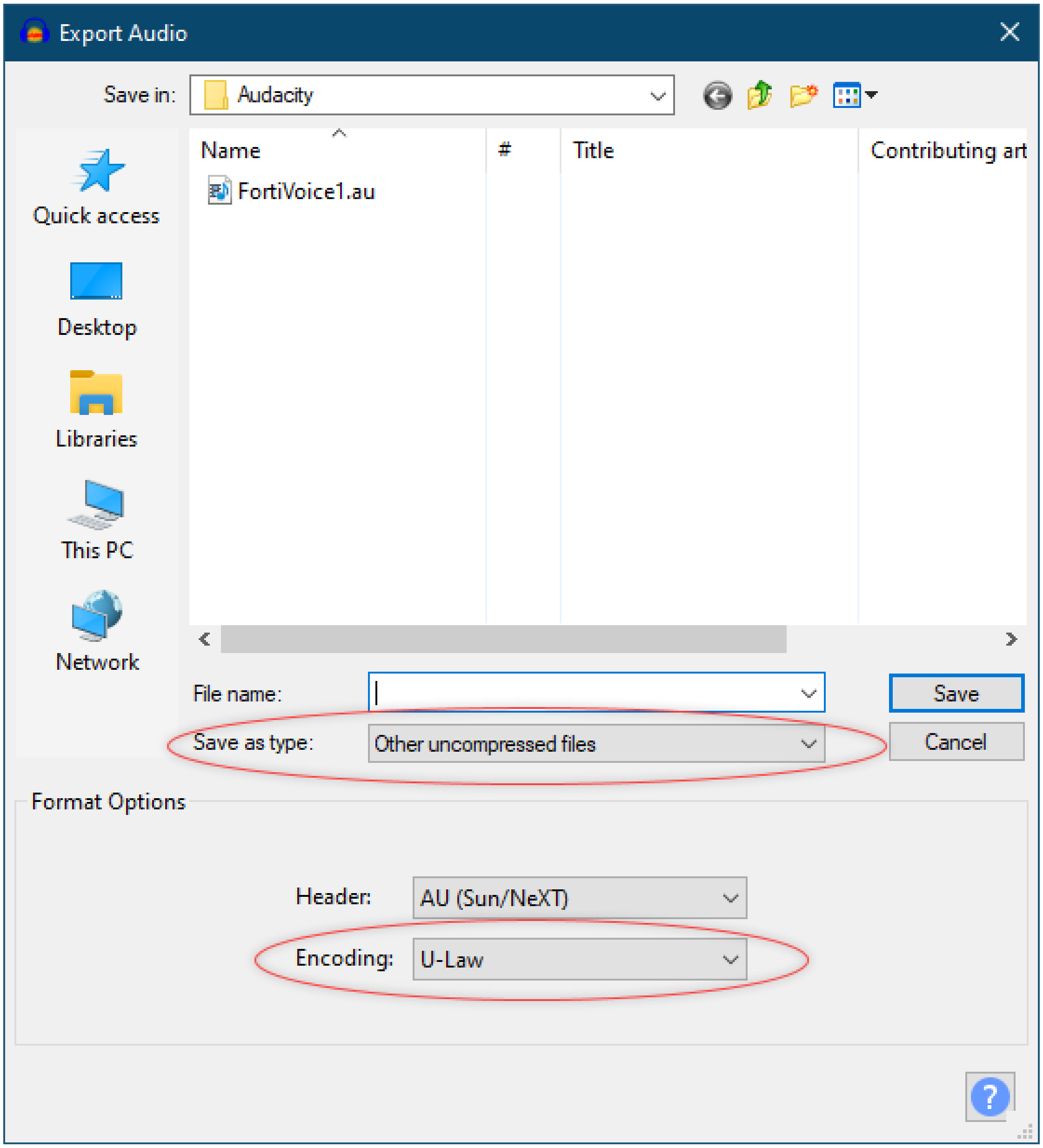
6. In *Default Sample Format*, select 16 bit.



7. Click *OK*.
8. When you are ready, record your prompt language message.

9. Save the file in a format that works with the FortiVoice unit.

a. Go to *File* > *Export* > *Export Audio*.



b. In *Save in*, select the directory where you want to save the file.

c. In *File name*, enter the required file name. The correct file extension is automatically added at the end of the file name according to the format that you select in *Save as type*.

d. In *Save as type*, select *Other uncompressed files*.

e. In *Encoding*, select *U-Law*.

f. Click *Save*.

g. If the Edit Metadata tags dialog appears, you can add tags and click *OK*.
The recording is now in a format that you can load onto the FortiVoice unit.

Working with FortiVoice profiles

The *Phone System* > *Profile* tab lets you create user privileges and SIP profiles for configuring extensions and SIP trunks. It also allows you to modify caller IDs, schedule the FortiVoice unit, and configure phone and LDAP profiles.

This topic includes:

Configuring SIP profiles

Configure the supported phone features and codecs and apply them to the extensions and SIP trunks.

Communicate with your VoIP service provider because the profile Setting are subject to the capabilities of the VoIP service provider. For example, if some of your features and codecs are not supported by your VoIP service provider, they will not work even if they are enabled or selected in the SIP profile.

The default SIP profiles can be edited but cannot be deleted.

For information on extensions, see Configuring Extensions on page 156.

For information on SIP trunks, see Configuring Trunks on page 190.

To configure a SIP profile

1. Go to *Phone System* > *Profile* > *SIP* and click *New.*
2. Configure the following:

GUI field	Description
Name	Enter a name for this profile.
DTMF	Select the dual-tone multi-frequency (DTMF) method used by the VoIP provider. Options are RFC2833, Inband, Info, Shortinfo, and Auto. Auto means the VoIP provider’s server and the FortiVoice unit will negotiate to select a DTMF method. You could also select a specific DTMF method if required.
Keep alive	Enter the time interval in seconds for the FortiVoice unit to talk to the SIP server of your service provider to keep the connectivity and check its capability. 0 means no checking by the FortiVoice unit.

GUI field	Description
NAT	Select if the VoIP service provider supports SIP NAT translation.
T.38	Select if the VoIP service provider supports fax over VoIP network.
Transport	*Transport*: SIP commonly uses TCP or UDP port 5060 and/or 5061. Port 5060 is used for non-encrypted SIP signaling sessions and port 5061 is typically used for SIP sessions encrypted with Transport Layer Security (TLS). Enable the protocols as required. This option, if applied to a user, overrides the system-wide transport Setting. For more information, see Configuring SIP settings on page 88. *Secure RTP*: Select to provide encryption, message authentication and integrity, and replay protection to the FortiVoice Real-time Transport Protocol data.
Codec	Select the codecs supported by the VoIP service provider. Among the selected ones, choose the preferred one for the VoIP provider. The preferred codec is usually the most used one in your area and provides the best quality of communication. If your preferred codec is different from that of your VoIP service provider, the service provider's codec will be used as long as it is one of your supported codecs.

3. Click *Create*.

Modifying caller IDs

You can change the phone number, caller's name, or both that will appear on the destination phone.

Caller ID modifications are used when configuring dial plans. For more information, see Configuring Call Routing on page 205.

To modify a caller ID

1. Go to *Phone System* > *Profile* > *Caller ID Modification.*
2. Click *New* and configure the following:

GUI field	Description
Name	Enter the name for this caller ID modification record.
Map to new number	Enter the extension number or number pattern you want to modify. For example, you can enter 8134 to modify a single extension, or 81xx to modify all the four-digit numbers starting with 81.
Number Modification	If you have entered a number or number pattern in *Map to new number* field, configure the following values to modify it: • *Strip*: Enter a number to hide the starting part of an extension from displaying. 0 means no action. For example, if your *Match number* is 8134 and *Strip* is 2, only 34 will be displayed as caller ID. • *Truncate*: Enter a number to hide the ending part of an extension from

GUI field	Description
	displaying. 0 means no action. For example, if your *Match number* is 8134 and *Truncate* is 2, only 81 will be displayed as caller ID. • *Prefix*: Add a number before an extension. For example, if your *Match number* is 8134 and *Prefix* is 5, the caller ID will be 58134. • *Postfix*: Add a number after an extension. For example, if your *Match number* is 8134 and *Postfix* is 5, the caller ID will be 81345.
Match option	Select the way to match a call with caller name and number in order to modify call number or caller ID. • *Match Number or Name*: If the number is matched, modifications will be done based on *Number Modification* configuration. If the name is matched, modifications will be done based on *Map to new caller ID name* configuration. • *Match Number then Name*: If the number is matched, modifications will be done based on *Number Modification* configuration. If both the number and name are matched, modifications will be done based on *Map to new caller ID name* configuration. • *Match Name then Number*: If the *Name* is matched, modification will be done based on *Map to new caller ID name* configuration. If both the name and number are matched, modifications will be done based on *Number Modification* configuration. • *Match Number and Name*: If both the number and name are matched, modifications will be done based on *Number Modification* and *Map to new caller ID name* configurations.
Match caller ID name	Enter the caller ID that you want to map to another one. Caller IDs are created when configuring SIP extensions. See Configuring IP extensions on page 156.
Map to new caller ID name	Enter the new caller ID name to which you want to map the one entered in the field.
Block caller ID	Select to stop your caller ID from displaying on the destination phone.

3. Click *Create*.

Mapping a group of extensions to a caller ID name

If you want to map a group of extensions to a caller ID name, you can use the pattern for the extensions to do so.

For example, if you have a technical support team that has 10 extensions (8100-8110), instead of displaying each extension when making calls, you can just display one caller ID name “Support” for the whole team.

To map a group of extensions to a caller ID name

1. Go to *Phone System > Profile > Caller ID Modification.*
2. Click *New*.

3. In the *Map to new number* field, enter the pattern of the extensions, such as 81xx in the example.
4. In the *Map to new caller ID name* field, enter the caller ID name to which you want to map, such as “Support”.
5. Click *Create*.

Configuring phone profiles

Phone profiles contain the phone configurations that are mostly used and customized, such as the programmable phone keys. Phone profiles make extension configuration more flexible because phone users are allowed to choose the profile they want. In addition, any changes the administrator makes to a profile is automatically applied to the extensions that use the profile. For more information, see Configuring IP extensions on page 156.

The phone profiles configured here appear as *Admin defined* profiles when you configure a SIP extension.

To configure a phone profile

1. Go to *Phone System* > *Profile* > *Phone.*
2. Click *New* and configure the following:

GUI field	Description
Name	Enter a name for the profile.
Phone model	Select a phone model for the profile.
Time format	Select the time display format on the phone. *North American*: mm/dd/yyyy *International*: dd/mm/yyyy
Phone book	Select *Local only* to include the phone directory on this FortiVoice unit, and *Global* to include the phone directories of any remote FortiVoice units connected to this unit. For information on phone directories, see The Fax Queue tab lists the faxes waiting to be sent on the FortiVoice unit. For more information about fax, see Configuring fax on page 263. on page 36.
Phone language	Select the language display on the phone.
Description	Enter any notes you have for this profile.
VLAN	You may need to deploy phones using the existing IT infrastructure which only has one network drop for each employee. The network switch supports 802.1Q VLAN tagging and LLDP-MED. Some phones such as FortiFones have two network ports: LAN and PC. The recommended solution is to connect FortiFones to the switch using LAN port and connect the computer to the PC port of FortiFones. VLAN tag needs to be enabled to segregate FortiFone voice network and PC data network.
Option	If you select *Manual*, configure the following: *Enable VLAN tagging for voice*: Select to enable VLAN tagging to segregate FortiFone voice network and PC data network. *Voice VLAN ID*: Enter your organization’s VLAN ID for voice.

GUI field		Description
		Priority for voice: Enter the traffic service level recommended by the IEEE. Each number represents a traffic type. The range is from 0-7, with 7 being the highest. • 0: Background • 1: Best Effort • 2: Excellent Effort • 3: Critical Applications • 4: Video, < 100 ms latency and jitter • 5: Voice, < 10 ms latency and jitter • 6: Internetwork Control • 7: Network Control *Enable VLAN tagging for data*: Select to enable VLAN tagging to segregate PC data network and FortiFone voice network. *Voice VLAN ID*: Enter your organization's VLAN ID for data. *Priority for data*: Enter the traffic service level recommended by the IEEE. Each number represents a traffic type. The range is from 0-7, with 7 being the highest. • 0: Background • 1: Best Effort • 2: Excellent Effort • 3: Critical Applications • 4: Video, < 100 ms latency and jitter • 5: Voice, < 10 ms latency and jitter • 6: Internetwork Control • 7: Network Control If you select *LLDP* (Link Layer Discovery Protocol), the FortiVoice unit automatically generates the configuration file. You need to enable LLDP support on your network switch.
Automatic Configuration		
	Display option	Select what to display on the extension: the extension user's name only or name and number.
	Digit map pause timer	Enter the digit map timeout in seconds which defines the waiting time between the completion of dialing number entering and initiating the call. For example, if you enter 5 and use the default digit map syntax, the phone will initiate a call 5 seconds after you finish entering the dialing number.
	Intercom barge	If you select FortiFone-175, 375, or 475 for *Phone model*, you can enable intercom barge to allow intercom drop-in in a phone conversation.
	Screensaver timer	If you select FortiFone-175, 375, 475, 570, or 575 for *Phone model*, you can set the phone screen saving timer in seconds. The screensaver time for FortiFone-175, 375, and 475 can be set between 0-3600 seconds.

GUI field		Description
		The screensaver time on FortiFone-570 and 575 can only be set to the following increments: • 15 seconds • 30 seconds • 1 minute • 2 minutes • 5 minutes • 10 minutes • 30 minutes • 1 hour • 2 hours • 3 hours • 6 hours
	Button transparency	If you select FortiFone-570 for *Phone model*, select the percentage of phone buttons' background color transparency.
	Backlight time	Set the phone backlight time to illuminate the screen in low light conditions.
Hotel		If you select FortiFone-H35 for *Phone model*, enter the hotel contact information and instructions on how to dial rooms, local, long distance, and international number. You may also select the font color for the call display.

3. Click *Create*.

Configuring programmable keys profiles

The *Programmable Keys* submenu lets you configure the programmable keys for FortiFones. For FortiFones with expansion modules or multiple key pages, you can select the module or page to program the keys.

Once a programmable keys profile is applied to an extension, the keypad programming is always the same regardless of the phone for the extension.

To configure a programmable keys profile

1. Go to *Phone System* > *Profile* > *Programmable Keys*.
2. Click *New*.
3. Enter the profile name, select a phone type, enter any notes you have for the profile, and click *Create*.

4. Double-click the profile you created and configure the following:

GUI field	Description
Provisioning lines	Select the phone lines you want to reserve. For example, if you select 2 for this phone, number 1 and 2 on the keypad become reserved for phone lines.
Number of expanded modules	Select the number of expanded modules for the keypad. This option only appears for certain FortiFone models.
Number of pages to be used on this phone	Select the number of pages for the keypad. This option only appears for certain FortiFone models.
Base/Page/Expanded Module	Fields display depending on the phone model.
Option	The keypad number of the phone.
Mode	Select *User* to allow users to configure the programmable keys on the web user portal. Select *Admin* to configure the programmable keys here.
Function	Select the function assigned to this key.
Resource	For some functions, you need to enter the information in this field based on your phone configuration. For example, if you select function *Line appearance* for key 3, select what the line is for in this field.
Label	For some functions, you can add a explanatory label for the key.

5. Click *OK*.

Configuring LDAP profiles

The *LDAP* submenu lets you configure LDAP profiles which can query LDAP servers for authentication.

Before using an LDAP profile, verify each LDAP query and connectivity with your LDAP server. When LDAP queries do not match with the server's schema and/or contents, unintended phone call processing behaviors can result.

LDAP profiles each contains one or more queries that retrieve specific configuration data, such as user groups, from an LDAP server. The LDAP profile list indicates which queries you have enabled in each LDAP profile.

To view the list of LDAP profiles, go to *Phone System* > *Profile* > *LDAP*.

GUI field	Description
Profile Name	The name of the profile.
Server	The domain name or IP address of the LDAP server.
Port	The listening port of the LDAP server.

GUI field	Description
Auth	Indicates whether *User Authentication Options* is enabled.
Cache	Indicates whether query result caching is enabled.
(Green dot in column heading)	Indicates whether the entry is currently referred to by another item in the configuration. If another item is using this entry, a red dot appears in this column, and the entry cannot be deleted.

You can add an LDAP profile to define a set of queries that the FortiVoice unit can use with an LDAP server. You might create more than one LDAP profile if, for example, you have more than one LDAP server, or you want to configure multiple, separate query sets for the same LDAP server.

After you have created an LDAP profile, LDAP profile options will appear in other areas of the FortiVoice unit's configuration. These options let you to select the LDAP profile where you might otherwise create a reference to a configuration item stored locally on the FortiVoice unit itself. These other configuration areas will only allow you to select applicable LDAP profiles — that is, those LDAP profiles in which you have enabled the query required by that feature. For example, if a feature requires a definition of user groups, you can select only from those LDAP profiles where *Group Query Options* are enabled.

To configure an LDAP profile

1. Go to *Phone System > > Profile > LDAP*.
2. Click *New* to add a profile or double-click a profile to modify it.

GUI field	Description
Profile name	For a new profile, enter its name.
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of the LDAP server. *Port*: Enter the port number where the LDAP server listens. The default port number varies by your selection in *Use secure connection*: port 389 is typically used for non-secure connections, and port 636 is typically used for SSL-secured (LDAPS) connections.
Fallback server name/IP	Optional. Enter the fully qualified domain name (FQDN) or IP address of an alternate LDAP server that the FortiVoice unit can query if the primary LDAP server is unreachable. *Port*: Enter the port number where the fallback LDAP server listens. The default port number varies by your selection in *Use secure connection*: port 389 is typically used for non-secure connections, and port 636 is typically used for SSL-secured (LDAPS) connections.
Use secure connection	Select whether to connect to the LDAP servers using an encrypted connection. • *none*: Use a non-secure connection. • *SSL*: Use an SSL-secured (LDAPS) connection. Click *Test LDAP Query* to test the connection. A pop-up window appears. For details, see Testing LDAP profile queries on page 125.
Base DN	Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiVoice unit will search for user objects, such as `ou=People,dc=example,dc=com`.

GUI field	Description
	User objects should be child nodes of this location.
Bind DN	Enter the bind DN, such as `cn=FortiVoiceA,dc=example,dc=com`, of an LDAP user account with permissions to query the *Base DN*. This field may be optional if your LDAP server does not require the FortiVoice unit to authenticate when performing queries.
Bind password	Enter the password of the *Bind DN*. Click *Browse* to locate the LDAP directory from the location that you specified in *Base DN*, or, if you have not yet entered a *Base DN*, beginning from the root of the LDAP directory tree. Browsing the LDAP tree can be useful if you need to locate your *Base DN*, or need to look up attribute names. For example, if the *Base DN* is unknown, browsing can help you to locate it. Before using, first configure *Server name/IP*, *Use secure connection*, *Bind DN*, *Bind password*, and *Protocol version*, then click *Create* or *OK*. These fields provide minimum information required to establish the directory browsing connection.

3. Configure the following sections:
   - Configuring authentication options on page 123
   - Configuring advanced options on page 124
4. Click *Create, OK* or *Apply*.
   The LDAP profile appears in the LDAP profile list. To apply it, select the profile in features that support LDAP queries, such as protected domains and policies.
   Before using the LDAP profile in other areas of the configuration, verify the configuration of each query that you have enabled in the LDAP profile. Incorrect query configuration can result in unexpected phone processing behavior. For information on testing queries, see Testing LDAP profile queries on page 125.

Configuring authentication options

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 121.

1. Go to *Phone System > Profile > LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *User Authentication Options* section.
4. Configure the following:

GUI field	Description
Try Common Name with Base DN as Bind DN	Select to form the user's bind DN by prepending a common name to the base DN. Also enter the name of the user objects' common name attribute, such as `cn` or `uid` into the field.

Search User and Try Bind DN	Select to form the user's bind DN by using the DN retrieved for that user by *configuring the following:*
	• *LDAP user query*: Enter an LDAP query filter that selects a set of user objects from the LDAP directory.
	The query string filters the result set, and should be based upon any attributes that are common to all user objects but also exclude non-user objects.
	For example, if user objects in your directory have two distinguishing characteristics, their `objectClass` and `extension` attributes, the query filter might be:
	`(& (objectClass=inetOrgPerson) (telephonenumber=$u))`
	where `$u` is the FortiVoice variable for a user's extension.
	This option is preconfigured and read-only if you have selected from *Schema* any schema style other than *User Defined*.
	• *Schema*: If your LDAP directory's user objects use a common schema style:
	  • InetOrgPerson
	  • Active Directory
	Select the schema style. This automatically configures the query string to match that schema style.
	If your LDAP server uses any other schema style, select *User Defined*, then manually configure the query string.
	• *Scope*: Select which level of depth to query, starting from *Base DN*.
	  • *One level*: Query only the one level directly below the Base DN in the LDAP directory tree.
	  • *Subtree*: Query recursively all levels below the *Base DN* in the LDAP directory tree.
	• *Derefer*: Select the method to use, if any, when dereferencing attributes whose values are references.
	  • *Never*: Do not dereference.
	  • *Always*: Always dereference.
	  • *Search*: Dereference only when searching.
	  • *Find*: Dereference only when finding the base search object.

Configuring advanced options

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see Configuring LDAP profiles on page 121.

1. Go to *Phone System > Profile > LDAP*.
2. Click *New* to create a new profile or double click on an existing profile to edit it.
3. Click the arrow to expand the *Advanced Options* section.
4. Configure the following:

GUI field	Description
Timeout (seconds)	Enter the maximum amount of time in seconds that the FortiVoice unit will wait for query responses from the LDAP server.
Protocol version	Select the LDAP protocol version used by the LDAP server.
Enable cache	Enable to cache LDAP query results. Caching LDAP queries can introduce a delay between when you update LDAP directory information and when the FortiVoice unit begins using that new information, but also has the benefit of reducing the amount of LDAP network traffic associated with frequent queries for information that does not change frequently. If this option is enabled but queries are not being cached, inspect the value of TTL. Entering a TTL value of 0 effectively disables caching.
TTL (minutes)	Enter the amount of time, in minutes, that the FortiVoice unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiVoice unit to query the LDAP server, refreshing the cache. The default TTL value is `1440` minutes (one day). The maximum value is `10080` minutes (one week). Entering a value of `0` effectively disables caching. This option is applicable only if *Enable cache* is enabled.
Enable user password change	Enable if you want to allow FortiVoice web portal users to change their password.
Password schema	Select your LDAP server's user schema style, either *OpenLDAP* or *Active Directory*.

Testing LDAP profile queries

After you have created an LDAP profile, you should test each enabled query in the LDAP profile to verify that the FortiVoice unit can connect to the LDAP server, that the LDAP directory contains the required attributes and values, and that the query configuration is correct.

When testing a query in an LDAP profile, you may encounter error messages that indicate failure of the query and how to fix the problem.

To verify user authentication options

1. Go to *Phone System > Profile > LDAP*.
2. Double-click the LDAP profile whose query you want to test.
3. Click *Test LDAP Query*.
   A pop-up window appears allowing you to test the query.
4. From *Select query type*, select *Authentication*.

5. In *User name*, enter the user name or extension of a user on the LDAP server, such as `jdoe` or `1234`, depending your selection of *User Authentication Options*.
6. In *Password*, enter the current password for that user.
7. Click *Test*.
   The FortiVoice unit performs the query, and displays either success or failure for each operation in the query, such as the search to locate the user record, or binding to authenticate the user.

Clearing the LDAP profile cache

You can clear the FortiVoice unit's cache of query results for any LDAP profile.

This may be useful after, for example, you have updated parts of your LDAP directory that are used by that LDAP profile, and you want the FortiVoice unit to discard outdated cached query results and reflect changes to the LDAP directory. After the cache is emptied, any subsequent request for information from that LDAP profile causes the FortiVoice unit to query the updated LDAP server, refreshing the cache.

e**To clear the LDAP query cache**

1. Go to *Phone System* > *Profile* > *LDAP*.
2. Double-click the LDAP profile whose query cache you want to clear.
3. Click *Test LDAP Query*.
4. From *Select query type*, select *Clear Cache*.
   A warning appears at the bottom of the window, notifying you that the cache for this LDAP profile will be cleared if you proceed. All queries will therefore be new again, resulting in decreased performance until the query results are again cached.
5. Click *Ok*.
   The FortiVoice unit empties cached LDAP query responses associated with that LDAP profile.

Configuring user privileges

A user privilege includes a collection of phone services and restrictions that can be applied to each extension user.

The default user privilege configurations can be edited but cannot be deleted.

For information on extensions, see Configuring Extensions on page 156.

To configure a user privilege

1. Go to *Phone System* > *Profile* > *User Privilege* and click *New.*
2. Configure the following:

GUI field		Description
Name		Enter a name for this profile.
Basic Setting		
	Auto provisioning	Select to enable auto-provisioning for the extension. For more information, see Configuring SIP phone auto-provisioning on page 91.

GUI field		Description
		Once a FortiFone or supported DHCP-enabled phone connects to the FortiVoice unit and is auto-discovered, the FortiVoice unit assigns an IP address to the FortiFone and sends the basic PBX setup information to it. The full PBX configuration file will only be sent to the phone if this option is selected in the user privilege applied to the extension associated with the phone.
	List in directory	Select to put the user's name in the dial-by-name directory which allows a caller to find a user's extension number, and connect to their local extension or remote extension. This way the caller can reach their party without speaking to the receptionist.
	Configure programmable phone feature key/PFK	Select to enable configuring the feature access codes. For more information, see Modifying feature access codes on page 271.
	Softclient API login	Select to enable FortiVoice softclient to log into the FortiVoice unit.
	Lookup directory	Select to enable a user to view the phone directory of the local office. For more information, see The Fax Queue tab lists the faxes waiting to be sent on the FortiVoice unit. For more information about fax, see Configuring fax on page 263. on page 36.
	Lookup directory in remote office(s)	Select to enable a user to view the phone directories of remote offices. For more information, see The Fax Queue tab lists the faxes waiting to be sent on the FortiVoice unit. For more information about fax, see Configuring fax on page 263. on page 36.
	Twinning	Select to enable twinning function on an extension. The twinning feature allows you to use an external telephone (often a smartphone or home phone) to replicate your internal office extension (often your desk phone), so that when your desk phone rings, so does the "twin" phone. Once you return to your desk, you may press the Twinning key on the phone to terminate the twinning. This is useful when you are away from your desk but still want to receive calls to your desk phone. With this feature selected, you can configure twinning. For more information, see Setting extension user preferences on page 173.
	Internet of Things	Select to enable configuring your FortiVoice unit's integration with Amazon Alexa. For more information, see Configuring Internet of Things (IoT) on page 276.
Operator Role		Select to enable an extension user to process phone calls using the FortiVoice user web portal.

GUI field		Description
		You can select the four options to handle calls in each category. When the user privilege with this option selected is applied to an extension, an *Operator Console* button will appear on the top of the extension user’s FortiVoice web portal. Clicking the button lets the user to process phone calls on the Web.
Voicemail		Select to enable the voicemail service.
	Maximum messages	Enter the number of voice mails allowed.
	Voicemail retention days	Enter the number of days to keep the voicemails.
Music		
	Music on hold	Select a music on hold file. For details, see Managing phone audio settings on page 110.
	Early media	Early media is the exchange of information between the PBXes before the establishment of a phone connection, such as the ring tone. You can select a music file for early media. For details, see Managing phone audio settings on page 110.
Fax		Select to set the fax rules for users. For information on fax, see Configuring fax on page 263.
	Max incoming messages	Enter the number of incoming faxes allowed.
	Max incoming fax retention days	Enter the number of days to keep the incoming faxes.
	Max outgoing messages	Enter the number of outgoing faxes allowed.
	Max outgoing fax retention days	Enter the number of days to keep the outgoing faxes.
Call Restriction		Select call dialing restrictions for international, long distance, local, and internal calls. • *Forbidden*: Call is not allowed. • *Allowed*: Call is allowed. • *Allowed with Account Code*: Call is allowed by entering the system account/exempt code. For information on account code, see Configuring account codes on page 154. Not applicable to internal calls. • *Allowed with Personal Code*: Call is allowed by entering an extension’s account/exempt code. For more information, see Configuring account codes on page 154. Not applicable to internal calls. • *Allowed with Account and Personal Code*: Call is allowed by entering the system and extension account/exempt codes. Not applicable to internal calls.

GUI field		Description
	Other Restricted Area Code	You can specify area codes to which an extension is allowed or denied to make phone calls. **1.** Click *New*. **2.** Enter a name for this call restriction. **3.** Select *Enabled* to activate this restriction. **4.** Enter the area code that you want to set restriction. **5.** Select the permission for the area code. For more information, see Call Restriction on page 128. **6.** Click *Create*.
	Miscellaneous	*The max number of concurrent calls*: Set the maximum number of concurrent incoming and outgoing calls on the extension. The range is 1-10. The default is 4.
Monitor/Recording		Configure monitoring and recording outgoing and incoming calls of an extension to which this user privilege is applied.
	Personal recording	Select to allow users to configure personal recording of their incoming and outgoing calls on the user web interface.
	System recording	Select to allow users to configure system recording of their incoming and outgoing calls on the user web interface.
	Allow being barged	Select to allow monitoring an extension to which this user privilege is applied.
	Allow barging	Select to allow the extension to which this user privilege is applied to monitor other extensions. To barge a call, you need to enter your user PIN. For information on user PIN, see Voicemail PIN on page 163.
	Call barge option	If you select *Allow barging*, choose a barging method.
Hot-desking		Hot desking enables users to log into another phone. However, unlike using Follow Me or Call Forwarding which simply redirect a user's calls to another user's phone, hot desking takes total control of another phone by applying all of the user's own phone Setting to that phone until the user logs out. Each user can log into another phone by pressing *11 and enter his extension number and user PIN following the prompts. To log out, a user can press *12. You can view hot desking configurations by going to Viewing activity details of hot desking extensions on page 29. • *Enable hot-desking login*: Select to enable the hot-desking login function. • *Automatic logout hours*: Enter the time in hours for the phone to automatically log out of hot-desking. • *Enable hosting hot-desking*: Select if you want to log into a regular phone with the hot-desking phone authentication (by pressing *11 and enter your extension number and user PIN following the prompts).

GUI field		Description
		By doing so, the regular phone keeps its configuration and extension number. However, outgoing calls display the hot-desking number. The regular phone logs out of hot-desking when the time set in *Automatic logout hours* expires. If the two phones use different programmable phone keys, the host phone will reboot. For information on programmable phone keys, see Configuring phone profiles on page 118.
User Portal		Enable or disable the web portal and select the features of the user web portal. Only the selected ones will appear for the extension to which this user privilege is applied.
Advanced Setting		
	Conference number	Select the permission for conference calls: • *Allow All:* Select to allow the extension to join all conference calls. • *Disallow All:* Select to prohibit the extension from joining all conference calls. • *Allow All with Exempt:* If you select this option, click *New* to enter the conference call number(s) that the extension is banned to join. • *Disallow All with Exempt:* If you select this option, click *New* to enter the conference call number(s) that the extension is allowed to join. For more information, see Configuring auto attendants on page 250.
	Paging/Intercom	Select the permission for paging/intercom: • *Allow All:* Select to allow the extension to page/intercom all paging numbers. • *Disallow All:* Select to prohibit the extension to page/intercom all paging numbers. • *Allow All with Exempt:* If you select this option, click *New* to enter the paging/intercom number(s) that the extension is banned to page/intercom. • *Disallow All with Exempt:* If you select this option, click *New* to enter the paging/intercom number(s) that the extension is allowed to page/intercom. For more information on paging, see Configuring auto attendants on page 250.
	Trusted hosts	Enter the IP address and netmask of the subnet that can register with the SIP server. Only extensions on the specified subnet can register with the SIP server. You can add multiple trusted hosts.

GUI field		Description
	Permitted outgoing rules	Enable or disable all available outbound calling rules. For more information on calling rules, see Configuring outbound dial plans on page 211.

3. Click *Create*.

Configuring emergency zone profiles

You configure an emergency zone profile to include the detailed contact information in case of emergencies.

To configure an emergency zone profile

1. Go to *Phone System* > *Profile* > *Emergency Zone*.
2. Click *New* and configure the following:

GUI field	Description
Name	For a new profile, enter its name.
Emergency caller ID	Enter the caller ID to display on the destination phone when you dial the emergency number, such as 911. If an extension in this profile already has an emergency caller ID, this ID is overridden by the extension's own ID. See Emergency caller ID on page 174.
Description	Enter any notes you have for this profile.
Emergency setting	Configure to send an alert email when an emergency call is made. Select *Do nothing* if you don't want the FortiVoice unit to send an alert email. Otherwise, select *Send alert email* and enter the email address.
Contact Information	Enter the emergency contact information for the profile.

3. Click *Create*.

Scheduling the FortiVoice unit

You can schedule the FortiVoice operation time and use the schedules when configuring dial plans, virtual numbers, or call management. The default schedules, namely *after_hour, any_time*, *business_hour,* and *holiday*, can be modified but cannot be deleted.

Depending on your preference, you can create either a standard or a calendar-based schedule.

For information on dial plan, see Configuring Call Routing on page 205.

For information on virtual numbers, see Working with virtual numbers on page 188.

For information on call management, see Setting extension user preferences on page 173.

To configure a standard schedule

1. Go to *Phone System* > *Profile* > *Schedule* and click *New.*
2. Enter a profile name and select *Standard* for *Mode*.

3. Click *Create*.
4. In the schedule list, select the profile name you created and click *Edit*.
5. For *Week Day*, select the days to include in the schedule and set the AM and PM time or select *Full Day*.
6. For Holiday, click *New* to set the holidays. For example, select 01/01/12 in the *Date* field and enter New Year's Day in the *Description* field, and click *Create*.
7. Click *OK*.

To configure a calendar-based schedule

1. Go to *Phone System* > *Profile* > *Schedule* and click *New*.
2. Enter a profile name and select *Calendar* for *Mode*.
3. Click *Create*.
4. In the schedule list, select the profile name you created and click *Edit*.
5. Double-click a date to schedule an event.
6. Click *OK*.

Configuring devices

Phone System > *Device* allows you to configure desktop FortiFones (including Cisco CP-7841 and CP-8841 phones with version number 12.X) and FortiFone 870i in a central place for easy management.

This topic includes:

- Configuring desktop FortiFones on page 132
- Configuring FortiFone-870i on page 134

Configuring desktop FortiFones

You can configure desktop FortiFones to include their MAC addresses, phone model, phone profiles, names, and statuses. You may also assign a phone to an extension, to FortiFone-870i, or to an extension as an auxiliary.

To view the list of desktop FortiFones, go to *Phone System* > *Device* > *Desktop FortiFone*.

GUI field	Description
Delete	Select one or more SIP phone records and click this button to remove them all at once.
Action	• *Assign to New Extension*: Select a SIP phone in *Not Assigned* status and click this option to add an extension and assign this phone to the extension at the same time. For more information, see To assign a new extension user to an unassigned phone on page 133. • *Assign to Existing Extension:* Select an unassigned phone and click this option to assign this phone to an existing extension. The phone record disappears from the *Unassigned Phone* list. For more information, see To assign an existing extension user to an unassigned phone on page 134. • *Assign to Multi-cell Device*: Select a multi-cell device (for example, FortiFone 870i) in *Not Assigned* status and click this option to add an

GUI field	Description
	extension and assign this phone to the extension at the same time. For more information, see To assign a new extension user to an unassigned phone on page 133 and Configuring FortiFone-870i on page 134. • *Assign as Auxiliary to Existing Extension:* Select a SIP phone in *Not Assigned* status and click this option to assign it to an existing extension as an auxiliary device. For more information, see To assign a new extension user to an unassigned phone as an auxiliary device on page 134 and Auxiliary Device on page 160. • *View Phone Configuration*: Select a SIP phone in *Assigned* status and click this option display its configuration file. • *Export*: Select to save the SIP phone list in `csv` format.
MAC Address	The Media Access Control address (MAC address) of the SIP phone.
Phone Model	The phone brand and model.
Phone Profile	The profile for this phone. See Configuring SIP profiles on page 115.
Management	Displays if the phone has been assigned to an extension.
Number	The extension number of the phone.
Display Name	The name displaying on the extension. This is usually the name of the extension user.
Status	Displays if the phone is registered with the FortiVoice unit. A registered phone is assigned an IP address and basic PBX setup information.
IP	The IP address of the phone assigned by the FortiVoice unit.
Phone Info	The model, MAC address, and firmware version of the phone for this extension.

To add a desktop FortiFone

1. Go to *Phone System > Device > Desktop FortiFone*.
2. Click *New* and configure the following:

GUI field	Description
MAC Address	Enter the MAC address of the phone you want to add.
Phone model	Select the phone brand and model.
Phone Profile	Select the profile for this phone. You may also create a profile or edit an existing one. For more information, see Configuring SIP profiles on page 115.
Status	Displays if the phone is registered with the FortiVoice unit. A registered phone is assigned an IP address and basic PBX setup information. This field is auto-populated based on the phone information you have entered.
Description	Enter any notes about the phone.

3. Click *Create*.

To assign a new extension user to an unassigned phone

1. Go to *Phone System* > *Device* > *Desktop FortiFone*.
2. Select a phone in *Not assigned* status.
3. Click *Action* and select *Assign to New Extension.*
4. Enter the extension details and click *Next*. For details, see Configuring IP extensions on page 156.
5. Review the phone details and click *Next*.
6. Review the summary and click *Finish*.

To assign an existing extension user to an unassigned phone

1. Go to *Phone System* > *Device* > *Desktop FortiFone*.
2. Select a phone in *Not assigned* status.
3. Click *Action* and select *Assign to Existing Extension.*
4. Select the extension to associate with the unassigned phone and click *Next*.
5. Review the extension details and click *Next*. For details, see Configuring IP extensions on page 156.
6. Review the phone details and click *Next*.
7. Review the summary and click *Finish*.

To assign a new extension user to an unassigned phone as an auxiliary device

1. Go to *Phone System* > *Device* > *Desktop FortiFone*.
2. Select a phone in *Not assigned* status.
3. Click *Action* and select *Assign as Auxiliary to Existing Extension.*
4. Select the extension to associate with the unassigned phone and click *Next*.
5. Review the extension details and click *Next*. For details, see Configuring IP extensions on page 156.
6. Review the phone details and click *Next*.
7. Review the summary and click *Finish*.

Configuring FortiFone-870i

Each base FortiFone-870i can support up to 15 handsets. You can configure a FortiFone-870i to work with the FortiVoice unit by adding a primary phone (base) and multiple secondary phones (bases).

The following prerequisites must be met for the FortiFone-870i configuration to work:

- FortiVoice v6.0 build 127 or later
- FortiVoice auto provisioning is enabled (see Configuring SIP phone auto-provisioning on page 91)
- FortiFone-870i firmware 3.23 or later
- Network connectivity available between FortiFone-870i and the FortiVoice unit

Follow the FortiFone-870i guide to configure the phone first. Once you connect the phone to the network, you can configure it on the FortiVoice unit.

To configure the FortiFone-870i

1. Go to *Phone System* > *Device* > *Multi-cell Device* and click *New.*
2. Enter the MAC address of the intended primary station.
3. Select *Enable*.
4. In *Device role*, set the station as primary with chain ID. The chain ID should be numbers up to 5 digits. Enter any description as needed and click *Create*.

You can now add extensions to the primary station. You only need to apply the extension configuration to the primary. All secondary stations can obtain the extension information from the primary.

5. Go to *Phone System > Device > Desktop FortiFone.*
6. Select the primary station just created, click *Action,* and select *Assign to New Extension* or *Assign to Existing Extension*.
7. For *Assign to New Extension*, see To assign a new extension user to an unassigned phone on page 133.
8. For *Assign to Existing Extension*, see To assign an existing extension user to an unassigned phone on page 134.
9. Add more extensions as needed with a different handset IDs. Upon completion, you should see all the extensions listed for the primary station.
10. Since the primary station is provisioned, proceed to provision the secondary stations. Factory reset the intended secondary station and connect it to the network. If the network and the FortiVoice unit are configured properly, it should appear under *Phone System > Device > Desktop FortiFone*.
11. Select the unassigned FortiFone 870i station, click *Action > Assign to Multi-cell Device.*
12. In *Device role*, set the base station as secondary and select *Prime* (primary station) from the drop down list. Type any description as needed.
13. Click *OK*.
14. On the secondary phone configuration, remove the temporary extension setting and reboot the station. See the phone guide for more information.
    Note that the temporary extension is used for initial configuration of the base and has to be removed for the phone to work with the FortiVoice unit.

Reviewing system configuration

Phone System > Review provides a snapshot of the FortiVoice system configuration. You may also modify some items.

The items to be reviewed or modified include:

- Extension numbers (For modification information, see Configuring IP extensions on page 156.)
- New voice mail check
- Network summary
- DID handling information
- Call queues (For modification information, see Creating call queues on page 216.)
- Agents (For modification information, see Configuring agents on page 225.)
- Extensions that are used by other objects and their roles in the objects.

Managing FortiVoice Gateways, Local Survivability, and Firmwares

A managed gateway is one of the FortiVoice Gateways that either contains FXS, FXO, or PRI ports that handles calls for the FortiVoice phone system. Gateway Management enables auto-discovery of other FortiVoice gateways on the network and offers remote device management from a centralized FortiVoice phone system. Gateways will still need to be configured for network Setting and administrator passwords, but all other configurations will be received from the FortiVoice unit.

For information on gateway auto-discovery, see Viewing unmanaged gateways on page 29.

FVE-100E and larger systems can manage gateways.

FVE models and supported number of gateways

FVE model	Number of gateways supported
100E & VM100	5
200F & VM200	5
300E	10
VM500	15
500E & 500F	15
1000E & VM1000	25
200D	25
2000E, 2000F & VM2000	50
3000E & VM3000	50
5000F & VM5000	100
VM10000	100
VM50000	200

The FortiVoice Local Survivable solution is designed to provide branch resiliency for centralized deployments with multi-sites. It is delivered and supported by a selected line of enterprise-class appliances through a firmware upgrade and enables system administrators to seamlessly connect multiple locations with an easy-to-deploy solution.

Firmwares of the FortiVoice units and FortiFones can be managed in a single place.

For information on local survivable gateway deployment, see FortiVoice Local Survivable Gateway Deployment Guide.

This topic includes:

Managing FXO gateways

FXO Gateways connect your IP phone system to an outside telephone line. It allows you to connect the FXS port to the FXO port of the gateway, which then translates the analog phone line to a VoIP call.

The FortiVoice FVG-GO08 gateways can be auto discovered by the FortiVoice unit once they connect to it. You can also manually add gateways to be managed by the FortiVoice unit.

This topic includes:

- Viewing and adding gateways on page 137
- Creating multiple trunk gateways on page 138

Viewing and adding gateways

To view the list of added GO08 gateways, go to *Managed System* > *Gateway* > *FXO Gateway*.

GUI field	Description
Apply configuration	Select a gateway from the list and click this option to apply the FortiVoice FXO gateway configuration file to this gateway and reboot the gateway immediately.
View configuration	Select a gateway from the list and click this option to display the configuration file applied to this gateway.
Unmanaged Gateway	Click to display the gateways auto discovered by the FortiVoice unit. For more information, see Viewing unmanaged gateways on page 29.
Fetch Device Info	Select a branch FortiVoice unit from the list and click this option to retrieve its information.
Upgrade	Select a gateway and select this option to upgrade it now or later.

To add a gateway

1. Go to *Managed System* > *Gateway* > *FXO Gateway*.
2. Click *New* and do the following:

GUI field	Description
Name	Enter a unique name for the gateway.
Enable	Select to activate the gateway if required.
Display name	The name displaying on the gateway, such as ABC Company Gateway.
Hostname/IP address	Enter the hostname or IP address of LAN1 of the gateway. If you are using a different network interface, enter its IP. If the gateway has been configured to use a different HTTPS port, enter the port number after the IP address. • *Get device information*: Click to get the serial number, device type, and Mac address of the gateway. This will confirm the systems are able to communicate with each other and that the password entered is valid. If preconfiguring the system before deployment, manually enter in the serial

GUI field	Description
	number and MAC address of the gateway. • *Connect Device*: Click to go to the Web GUI of the gateway.
Admin user name	Enter the user name for logging into the gateway.
Admin password	Enter the password for logging into the gateway.
Serial number	The serial number of the gateway.
Type	Select the gateway brand and model.
MAC address	Enter the Mac address of the gateway.
Manage Trunk	See Creating multiple trunk gateways on page 138
Description	Enter any comments for the gateway.

3. Click *Create*.

Creating multiple trunk gateways

A GO08 gateway has 8 FXO ports. By default, all 8 ports are mapped to a single trunk. However, you may reassign the ports to multiple trunks if required. For example, you can have 4 trunks with 2 ports in each. Before adding any port to a trunk, you need to reduce the port number in the default trunk accordingly.

After creating a trunk gateway, you can manually add it into the dial plan to make it work. For more information, see Configuring inbound dial plans on page 205 and Configuring outbound dial plans on page 211.

To add a trunk gateway

1. Go to *Managed System* > *Gateway* > *FXO Gateway.*
2. Select a gateway for which you want to add a trunk and click *Edit*.
3. Click *Manage trunk*.
4. Double click the default gateway.
5. For *Mapped FXO ports*, reduce the number based on the number of ports you want to map to the new trunk. For example, if you want to map ports 6-8 to a new trunk, enter 1-5.
6. Click *OK*.

7. Click *New* and do the following:

GUI field	Description
Trunk gateway	Enter a unique name for the trunk gateway.
Enabled	Select to activate the trunk gateway if required.
Display name	The name displaying on the trunk gateway, such as ABC Company Gateway.
Main number	Enter the main number assigned to this trunk gateway. If you just have DIDs and no main number, you can select one of the DIDs as the main number.
Mapped FXO ports	Enter the ports to be mapped to this trunk gateway using a hyphen for a continuous range or a coma separating individual ports. For example 1-4,6.
Gateway device	Select the gateway for which the trunk is created.
Gateway SIP address	Enter the SIP address of the gateway. A SIP address is what you get when you register for a SIP account.
Gateway SIP port	Enter the port number for the gateway. It is either 5060 or 5061.
Caller ID modification	Select to allow caller ID modification configurations. You can associate multiple caller ID modification configurations with a dial plan. For more information on caller ID modification, see "Modifying caller IDs on page 116".
Off hook only	If the managed GO08 is connected with a third-party paging system that provides a dial tone before accepting DTMF digits from the gateway, you can select this option to stop the gateway from sending any DTMF digits after the dial tone is detected. In this case, when paging users dial the paging number, the gateway triggers the paging system to play dial tone and waits for digits from the paging users. If you have upgraded from an old phone system and want to keep its paging system, with this change at the system level, users' paging behavior is not affected regardless if this option is selected.
Description	Enter any comments for the trunk gateway.

8. Click *Create*.

Managing FXS gateways

FXS gateways connect traditional PBX phone lines to a VoIP phone system or provider. To connect the FXO ports to the Internet or a VoIP system, you need an FXS gateway in between.

The FortiVoice FVG-GS16 gateways can be auto discovered by the FortiVoice unit once they connect to it. You can also manually add gateways to be managed by the FortiVoice unit.

This topic includes:

- Viewing and adding gateways on page 140
- Editing gateway extensions on page 140

Viewing and adding gateways

To view the list of added GS16 gateways, go to *Managed System > Gateway > FXS Gateway.*

GUI field	Description
Apply configuration	Select a gateway from the list and click this option to apply the FortiVoice FXS gateway configuration file to this gateway and reboot the gateway immediately.
View configuration	Select a gateway from the list and click this option to display the configuration file applied to this gateway.
Unmanaged Gateway	Click to display the gateways auto discovered by the FortiVoice unit. For more information, see Viewing unmanaged gateways on page 29.
Fetch Device Info	Select a branch FortiVoice unit from the list and click this option to retrieve its information.
Upgrade	Select a gateway and select this option to upgrade it now or later.

To add a gateway

1. Go to *Managed System > Gateway > FXS Gateway.*
2. Click *New* and do the following:

GUI field	Description
Name	Enter a unique name for the gateway.
Enable	Select to activate the gateway if required.
Display name	The name displaying on the gateway, such as ABC Company Gateway.
Hostname/IP address	Enter the hostname or IP address of the gateway. • *Get device information*: Click to get the serial number, device type, and MAC address of the gateway. • *Connect Device*: Click to go to the Web GUI of the gateway.
Admin user name	Enter the user name for logging into the gateway.
Admin password	Enter the password for logging into the gateway.
Serial number	The serial number of the gateway.
Type	Select the gateway brand and model.
MAC address	Enter the Mac address of the gateway.
Manage extension	See Editing gateway extensions on page 140
Description	Enter any comments for the gateway.

3. Click *Create*.

Editing gateway extensions

A GS16 gateway has 16 FXS ports. Each port has an extension number.

To modify a gateway extension

1. Go to *Managed System > Gateway > FXS Gateway.*
2. Select a gateway of which you want to modify the extension and click *Edit*.
3. Click *Manage extension*.
4. Double click any extension to modify it.

GUI field		Description
Number		Enter the extension number following the extension number pattern. See Configuring PBX options on page 103
Edit Preference		See Setting extension user preferences on page 173
User ID		This is the system-generated ID based on the user ID prefix you set (see User ID prefix on page 106) and the extension number. This option is view only and only appears when you edit an extension. You can add a new user ID through the CLI.
Enable		Select to activate the extension.
Display name		Enter the name displaying on the extension. This is usually the name of the extension user. You can click *Expand to modify caller ID* to add a caller ID for external calls or emergency calls.
Description		Enter any comments for the extension.
Device Setting		
	Gateway device	This is the system-generated ID based on the user ID prefix you set (see User ID prefix on page 106) and the extension number. This option is view only and only appears when you edit an extension. You can add a new user ID through the CLI.
	Gateway fxs port	This is the analog port number assigned to the extension. This is read only.
	Direct call	If you want the phone to perform a direct call to a specified number after you pick up the phone, enable this option. *Number*: Enter the phone number for the direct call. *After*: Enter the wait period in seconds before the phone dials the specified phone number. The default is 0. The wait period range is from 0 to 30.
User Setting		
	Management	Configure the extension's role in other Setting. *User privilege*: Select the services for the extension. Click *Edit* to modify the current user privilege or click *New* to configure a new one. For more information on user privilege, see Configuring user privileges on page 126.

5.

GUI field		Description
		Department: Select the department that the extension belongs to. Click *Edit* to modify the current department or click *New* to configure a new one. For more information on extension department, see Configuring agents on page 225.
	Web Access	Configure web user portal and soft client access from mobile or desktop devices. *Authentication type*: Select the extension’s authentication type: Local or LDAP. *User password*: Enter the password for user web portal access which can be much longer and stronger to mitigate the risk of password guess attack and preserve the User PIN for phone access only. Control of using personal password or voicemail PIN to access user web portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 107. You can check the password strength. See Reviewing system configuration on page 135. Click *Generate* to generate a strong password automatically. Select *View password* to display the password. This option is only available when you select *Local* for *Authentication Type*.
	LDAP profile	If you select *LDAP* for *Authentication type*, select an LDAP profile to apply to this extension. For information on LDAP profile, see Configuring LDAP profiles on page 121. You can click *New* to create a new profile or *Edit* to modify the selected one.
	Authentication ID	If you select *Try common name with base DN as bind DN* as the user authentication option in the authentication profile you select, enter the authentication ID based on the user objects’ common name attribute you entered in the *Common name ID* field of the profile, such as jdoe. If you select *Search user and try bind DN* as the user authentication option in the authentication profile you select, leave this field blank. This option is only available if you select *LDAP* for *Authentication type*.
	Phone Access	Configure voicemail access by phone or access to restricted phone calls.

GUI field	Description
	Voicemail PIN: Enter the password for the extension user to access voicemail and the user web portal. Selection of using personal password or voicemail PIN to access user web portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 107. You can check the PIN strength. See Reviewing system configuration on page 135. Click *Generate* to generate a strong password automatically. Select the view PIN icon to display the password. If you have configured the default user PIN (see Default Voicemail PIN on page 105), the password appears here. However, you can change it. *Personal code*: Enter the extension specific account code that can be used to restrict calls. This code is needed to make some restricted calls. You can click *Generate* to get a code.

6. For more information, see Configuring IP extensions on page 156.
7. Click *Close*.

Managing PRI gateways

VoIP PRI gateways seamlessly connect your legacy telephony infrastructure, made up of PRI (T1, E1) or BRI lines, to IP networks. Businesses with legacy phone equipment (such as a TDM PBX) can use PRI gateways to connect to SIP trunking services without having to spend money altering their current network infrastructure.

The FortiVoice FVG-GT01 and GT02 gateways can be auto discovered by the FortiVoice unit once they connect to it. You can also manually add gateways to be managed by the FortiVoice unit.

This topic includes:

- Viewing and adding gateways on page 143
- Creating multiple trunk gateways on page 144

Viewing and adding gateways

To view the list of added GT01/02 gateways, go to *Managed System > Gateway > PRI Gateway*.

GUI field	Description
Apply configuration	Select a gateway from the list and click this option to apply the FortiVoice FXS gateway configuration file to this gateway and reboot the gateway immediately.

GUI field	Description
View configuration	Select a gateway from the list and click this option to display the configuration file applied to this gateway.
Unmanaged Gateway	Click to display the gateways auto discovered by the FortiVoice unit. For more information, see Viewing unmanaged gateways on page 29.
Fetch Device Info	Select a branch FortiVoice unit from the list and click this option to retrieve its information.
Upgrade	Select a gateway and select this option to upgrade it now or later.

To add a gateway

1. Go to *Managed System > Gateway > PRI Gateway*.
2. Click *New* and do the following:

GUI field	Description
Name	Enter a unique name for the gateway.
Enable	Select to activate the gateway if required.
Display name	The name displaying on the gateway, such as ABC Company Gateway.
Hostname/IP address	Enter the hostname or IP address of the gateway. • *Get device information*: Click to get the serial number, device type, and MAC address of the gateway. • *Connect Device*: Click to go to the Web GUI of the gateway.
Admin user name	Enter the user name for logging into the gateway.
Admin password	Enter the password for logging into the gateway.
Serial number	The serial number of the gateway.
Type	Select the gateway brand and model.
MAC address	Enter the MAC address of the gateway.
Description	Enter any comments for the gateway.

3. Click *Create*.

Creating multiple trunk gateways

A GT01/02 gateway has 1 span (PRI port). By default, the single span is mapped to one trunk. However, you may reassign the span to multiple trunks if required. Before adding any span to a trunk, you need to free the span in the default trunk accordingly.

After creating a trunk gateway, you can manually add it into the dial plan to make it work. For more information, see Configuring inbound dial plans on page 205 and Configuring outbound dial plans on page 211.

To add a trunk gateway

1. Go to *Managed System > Gateway > PRI Gateway*.
2. Select a gateway for which you want to add a trunk and click *Edit*.

3. Click *Manage trunk*.
4. Double click the default gateway.
5. For *Span*, move the span to the *Available* field.
6. Click *OK*.
7. Click *New* and do the following:

GUI field	Description
Trunk gateway	Enter a unique name for the gateway.
Enabled	Select to activate the trunk gateway if required.
Type	Select PRI for the trunk gateway.
Display name	The name displaying on the trunk gateway, such as ABC Trunk.
Main number	Enter the main number assigned to this trunk gateway. If you just have DIDs and no main number, you can select one of the DIDs as the main number.
Edit span	Select the span to be modified.
Span	Move the span to the *Selected* field to assign it to the trunk gateway.
Gateway device	Select the gateway for which the trunk is created.
Gateway SIP address	Enter the SIP address of the gateway. A SIP address is what you get when you register for a SIP account.
Gateway SIP port	Enter the port number for the gateway. It is either 5060 or 5061.
Caller ID modification	Select to allow caller ID modification configurations. You can associate multiple caller ID modification configurations with a dial plan. For more information on caller ID modification, see “Modifying caller IDs on page 116”.
Description	Enter any comments for the trunk.

8. Click *Create*.

Configuring local survivability

FortiVoice local survivability solution is designed to provide branch resiliency for centralized deployments with multi-sites. The FortiVoice unit at the central office sends the configuration files to the FortiVoice units and extensions at the branch offices. The central office handles all inbound calls thereby consolidating the number of lines required for an organization.

With this solution, you have one place to look for the routing rules, logs, call records, and call recordings. You can see the whole setup, make changes, or modify records on the fly. If an extension is added, it is operational immediately. Any users at any location will be able to call that new extension right away without waiting for configurations to sync up, or new policies required to be set at each location.

If the communication between the FortiVoice unit at the central office and the FortiVoice units and extensions at the branch offices is down, the FortiVoice units at the branch offices (survivability branches) will kick in to provide access to lines until the communication is restored between the central unit and the extensions.

A survivability branch is a local FortiVoice unit containing local extensions that is part of a centralized deployment.

FortiVoice models 300E and up and FortiVoice VM models 500 and up provide central management.

FVE-20E2, FVE-20E4, FVE-50E6, FVE-200F8, FVE-500F, and GS16 can serve as local survivability (survivability branch) models.

FVE models and supported number of survivability branches

FVE Model	Number of gateways supported
300E	10
VM500	15
500E & 500F	15
1000E & VM1000	20
200D	20
2000E, 2000F & VM2000	40
3000E & VM3000	40
5000F & VM5000	100
VM10000	100
VM50000	200

This topic includes:

- Local survivability deployment on page 146
- Adding, configuring, and viewing survivability branches on page 147

Local survivability deployment

Follow these recommended general steps to deploy your local survivability network:

- Set up HA on the central unit
  It is important to get your HA up and running and the correct virtual IP set as it is used throughout the local survivability setup. For information on setting up HA, see Using high availability on page 53.
- Add or import extensions to the central unit
  Once each branch unit has been added, you can add or import their extensions to the central unit. For more information, see Configuring IP extensions on page 156.
- Add and configure each branch unit:
  - Log in and choose a survivability management mode. See Adding, configuring, and viewing survivability branches on page 147.
  - Configure network and administration Setting – configure the network address, route and admin password as well as location Setting. See Configuring System Setting on page 37.
- Apply branch configuration from central unit
  Once the branch unit is set to the correct IP address, you can apply the configuration from the central system to each branch. See Adding, configuring, and viewing survivability branches on page 147.
- Add phones to network at branch offices
  Once the branch unit has received the configuration file, add the phones to the network. They will automatically detect the branch unit and be redirected to the central office to get their configuration file.

Adding the phones to the network too early will result in receiving an unassigned phone configuration file from the branch system. The phones need to be set to factory default for them to go to the central unit to get their configuration file.

Adding, configuring, and viewing survivability branches

Managed System > *Survivability* > *Survivability Branch* allows you to view and add survivability branches.

To view the list of added survivability branches

1. Go to *Managed System* > *Survivability* > *Survivability Branch*.

GUI field	Description
Apply configuration	Select a branch FortiVoice unit from the list and click this option to apply the FortiVoice configuration file to this branch unit and reboot the unit immediately.
View configuration	Select a branch FortiVoice unit from the list and click this option to display the configuration file applied to this unit.
Fetch Device Info	Select a branch FortiVoice unit from the list and click this option to retrieve its information.
Upgrade	Select a branch FortiVoice unit and select this option to upgrade it now or later.

To add a survivability branch on the central unit

1. Go to *Managed System* > *Survivability* > *Survivability Branch.*
2. Click *New* and configure the following:

GUI field	Description
Name	Enter a unique name for the branch unit.
Enable	Select to activate the branch unit if required.
Display name	Not required. You can leave this field empty.
Hostname/IP address	Enter the hostname or IP address of the branch unit. If the branch unit is configured to use a non-default HTTPS port, then add `:<port number>` after the IP address. For example, `172.16.5.11:4430`. *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 provisioned branch unit and get the serial number, type, and MAC address of the branch unit. This action can confirm that the systems can communicate and that the password is valid. *Connect Device*: Click to go to the Web GUI of the branch unit.

GUI field		Description
Admin user name		Enter the user name of the administrator account used for logging in to the branch unit. The default is admin.
Admin password		Enter the password associated with the Admin user name.
Serial number		The serial number of the branch unit that you are adding to this survivability branch. If you are configuring the survivability branch before deploying the branch unit, then manually update the serial number, type, and MAC address.
Type		Select the branch unit brand and model.
MAC address		Enter the MAC address of the branch unit.
Description		Enter any comments for the branch unit.
Survivability		Click to configure the branch unit details.
	Management mode	Make sure to select *Fully Managed*. **Fully managed - without branch paging** With the fully managed mode and without branch paging configured, the main office pushes the following configurations to the branch unit. • Extension user • Extension preferences • Global system Setting • PBX setting • Profile location • Survivability branch • System auto-provisioning • System PSTN channels • Trunk PSTN **Fully managed - with branch paging** With the fully managed mode and branch paging configured, the main office pushes the following configurations to the branch unit. • Call handling • Dialplan FXO gateway mapping • Dialplan outbound • Extension user • Extension preferences • Global system Setting • PBX account code • PBX setting • Profile location • Survivability branch • System auto-provisioning • System PSTN channels • Trunk PSTN

GUI field		Description
		• Trunk SIP peer
	Heartbeat server address	Select the heartbeat server on the central unit used to monitor the status of each branch unit in the network and enable communication between the main office unit and the branch unit. *Internal provisioning address*: The SIP server IP address of the main office unit which the branch unit sends OPTIONS SIP message to. *External host IP*: The external static IP address of the main office unit which the branch unit sends OPTIONS SIP messages to.
	Branch SIP server	Enter the branch unit's SIP server hostname or IP address for local extensions (phones) to reach.
	Branch SIP port	Enter the SIP server port number of the branch unit which local extensions (phones) can reach. The range is from 1 to 65535. The default is 5060.
	SIP phone registration interval	To keep the extensions' registration status with the central unit, enter the extension registration time interval in minutes as required by the FortiVoice unit. The range is from 1 to 120 minutes. The default is 5 minutes.
	Emergency call	Choose the branch or central unit to handle emergency calls. It is recommended to choose the branch unit to ensure the call is routed to the correct locations due to regional or international boundaries. *Handled by Branch*: The branch office intercepts the EMS call and sends it out on one of the local lines. *Handled by Central*: The main office handles the EMS call based on its configuration.
	Central trunk fallback to branch	Select if you want the branch unit to handle the call locally if the central unit fails to handle the calls, for example, when SIP trunk is down.
	External caller ID option	Choose the system default or branch specific caller ID for outgoing calls originating from branch offices instead of the FortiVoice main number (see Main number on page 103) or the trunk phone number (see Phone Number on page 194).
	External caller ID	If you choose *Use branch caller ID* for *External caller ID option,* enter the caller ID.
	Phone directory option	Choose the system default or branch phone directory.
	Branch failover trunk FXO ports	This option only activates when you edit a survivability branch. Enter the FXO failover port in the event of internet failure or a network crash by connecting the branch unit to an outside telephone line.

GUI field		Description
		For a port range, enter the starting and ending ports separated by a dash. For separate ports, use a comma. Port list example: 1-4,6.
	Branch extensions	Select the extensions to add to the branch.
	Gateway	The FortiVoice survivability branch solution can support a FortiVoice FXS gateway at the branch office. To link the branch unit with a deployed FortiVoice FXS gateway, select the FortiVoice FXS gateway from the *Available* list and use the right arrow to move it to the *Selected* list.
Branch Paging		Use branch paging to broadcast an audio message to branch extensions (phones) or an overhead paging system.
	FXO port	This option only activates when you edit a survivability branch. Enter the FXO port that the paging system is plugged in to at the branch office, if applicable.
	Max duration	Enter the maximum time period in seconds for each overhead paging session. When the maximum duration is reached, the branch paging session automatically ends. The duration range is from 0 to 64800 seconds.
	Number	This option only activates when you edit a survivability branch. Enter the number to engage the paging system. For example, 0110.
	Accept same branch paging	Select to allow all extensions at the same branch to connect to the paging system without a user privilege and complete a paging call.
	Reject paging by default	Select to allow extensions at the same branch to connect to the paging system using a user privilege and account code, and complete a paging call.
	Accept failover local paging	If the main office is down and you want to do paging from the branch office, select this option. *with authentication code*: This code is not required.
Speed Dial Rule		This option is only available when you edit a branch. Click to add a speed dial rule for the branch. For details, see Mapping speed dials on page 255.

Click *Create* and *Create*.

Managing firmwares

Managed System > *Firmware* allows you to manage firmwares of the FortiVoice units and FortiFones.

FortiVoice units refer to the FortiVoice devices managed by this FortiVoice unit, such as gateways.

FortiFones are those connect to this FortiVoice unit.

To manage FortiFone firmware

1. Go to *Managed System* > *Firmware* > *FortiFone Firmware.*

GUI field	Description
Upload	Click to upload a firmware file.
Download	Select a firmware file and click this button to download it.
Action	Select a firmware file and click this button to schedule or disable a firmware upgrade for the FortiFones managed by this FortiVoice unit. If you schedule an upgrade, the firmware will be pushed to the managed FortiFones at the scheduled time.
Statistics	Click to display the information of the managed FortiFones.
Upgrade schedule	Select a schedule profile to do the FortiFone firmware upgrade. For more information, see Scheduling the FortiVoice unit on page 131.

To manage FortiVoice firmware

1. Go to *Managed System* > *Firmware* > *FortiVoice Firmware.*

GUI field	Description
Upload	Click to upload a firmware file.
Upgrade	Select a firmware file to do the FortiVoice firmware upgrade now or at a scheduled time.

Configuring Security Setting

You can enhance the FortiVoice unit security by configuring intrusion detection, password policies, user privileges, and extension blocking.

This topic includes:

Configuring intrusion detection

Security > Intrusion Detection lets you manually add IPs to be exempted from being blocked, remove system added exempt IPs if you find them suspicious, and configure intrusion detection Setting.

The manually added IPs are usually from the sources that you trust. For example, IPs from external customer devices can be added.

IPs of the devices that are registered to the FortiVoice unit are automatically added to the exempt list.

To add an exempt IP

1. Go to *Security > Intrusion Detection > Exempt IP.*
2. Click *New*.
3. Enter the IP.
4. Click *Create*.

To remove an auto exempt IP

1. Go to *Security > Intrusion Detection > Auto Exempt IP.*
2. Select an IP you want to remove and click *Delete*.

To configure intrusion detection settings

1. Go to *Security > Intrusion Detection > Setting.*
2. Configure the following:

GUI field	Description
Status	• *Disable*: Select to stop the intrusion detection activities. • *Monitor Only*: Select to only track the intrusion detection activities. • *Enable*: Select to activate the intrusion detection activities.
Access tracking	Select the method to track the traffic access (and IPs) to the FortiVoice unit.

GUI field	Description
Initial block period	Enter the time in minutes to initially block every new device/IP trying to access the FortiVoice unit. This is to screen out spammers or attackers because they normally will not try again after being blocked initially.

3. Click *Apply*.

Setting password policies

Security > Password Policy lets you set the SIP password and user PIN policy for administrators and extension users. For information on setting SIP password and user PIN, see Configuring IP extensions on page 156.

You can also edit extension user passwords.

To set password policies

1. Go to *Security > Password Policy > Password/PIN Policy*.
2. Configure the following:

GUI field	Description

Password / PIN Policy	• *Minimum password length*: Set the minimum acceptable length (8) for passwords.
	• *Password must contain*: Select any of the following special character types to require in a password. Each selected type must occur at least once in the password.
	  • *Upper-case-letter* — A, B, C, ... Z
	  • *Lower-case-letter* — a, b, c, ... z
	  • *Number* — 0 ... 9
	  • *Non-alphanumeric* — punctuation marks, @,#, ... %
	• *Apply password policy to*: Select where to apply the password policy:
	  • *Admin user* — Apply to administrator web GUI passwords. If any password does not conform to the policy, require that administrator to change the password at the next login.
	  • *SIP users* — Apply to FortiVoice SIP phone users' passwords. If any password does not conform to the policy, require that user to change the password at the next login.
	  • *User passwords*: Apply to user web portal access passwords. If any password does not conform to the policy, require that user to change the password at the next login.
	• *Minimum PIN length*: Set the minimum acceptable length (6) for the user PIN.
	• *PIN must contain:*
	  • *Number*: to include a number (0-9) in the PIN.
	  • *PIN special*: Select to include special characters in the PIN.
	• *Apply PIN policy to*: Select *Voicemail users* to apply the policy to

GUI field	Description
	FortiVoice phone users' user PIN. If any PIN does not conform to the policy, require that user to change the PIN at the next login.
Allow empty admin password	Select to allow leaving the admin password field empty when logging in to the system.

3. Click *Apply*.

To edit extension user passwords

1. Go to *Security > Password Policy > Password Auditor.*
2. Double-click an extension of which you want to edit the user passwords.
3. Under *User Setting*, change the passwords as required. For more information, see Configuring IP extensions on page 156.
4. Click *OK*.

Configuring user privileges

A user privilege includes a collection of phone services and restrictions that can be applied to each extension user.

For more information, see Configuring user privileges on page 126.

Configuring account codes

You can set account codes to restrict long-distance and international calls, for instance. Users must dial these codes first before making long-distance or international calls.

You apply the account codes in user privileges. For details, see Configuring user privileges on page 126.

To set an account code

1. Go to *Call Security > User Privilege > Account Code.*
2. Click *New* and configure the following:

GUI field	Description
Name	Enter an account code name.
Description	Enter any notes you may have for the account code.
Shared	Select to use this code on any extension.
Represented in CDR	Select to display the account code by code or name in CDR. For information about CDR, see Viewing call records on page 31.
Access Code Set	Click *New* to enter the account code such as 69, display name for the code such as Finance, and any notes for the code. Click *Create*.

3. Click *Create*.

Blocking extensions

For security reasons, if you find any extension has been suffering from attacks by other devices, you may block it to stop the attacks.

To block a number

1. Go to *Security > Blocked Number*.
2. Click *New*.
3. Enter the extension you want to block.
4. Click *Create*.

To unblock a number

1. Go to *Security > Blocked Number*.
2. Select a blocked number in the list.
3. Click *Delete*.

Configuring Extensions

The *Extension* menu lets you configure local and remote extensions, extension groups, general voicemail, and virtual numbers.

This topic includes:

- Setting up local extensions on page 156
- Creating extension groups on page 180
- Setting up general voice mailboxes on page 187
- Working with virtual numbers on page 188

Setting up local extensions

You can configure IP phone extensions, edit analog extension, and choose extension preferences.

This topic includes:

- Configuring IP extensions on page 156
- Modifying managed extensions on page 166
- Modifying analog extension (200D-T, 1000E-T, and 20E2 models only) on page 167
- Setting up remote extensions on page 169
- Configuring fax extensions on page 170
- Setting extension user preferences on page 173

Configuring IP extensions

An IP extension is an IP phone connected through a network to a system. An internal IP extension is a phone connected on the same LAN as the system. An external IP extension is a phone connected outside the LAN.

To view the local IP extensions, go to *Extension* > *Extension* > *IP Extension*.

GUI field	Description
Other Actions	• *Export*: Select to save a copy of the extension list or download as a sample list with or without user ID in CSV format. • *Import*: Select to upload a copy of the extension list in CSV format. For details, see Importing a list of extensions on page 165. • *View Phone Configuration file:* Select a FortiFone extension and click this option to view the phone's configuration file. When a phone is associated with an extension, the FortiVoice unit generates a configuration file for the phone. For details, see To create or edit an IP extension on page 158. • *Apply Phone Configuration*: If you have edited an extension configuration and want to apply it to the phone associated with this extension, select the

GUI field	Description
	extension and click this option. The selected phones will reboot and only the phones that meet the following conditions will receive the new configuration: • Phones supported by and registered to the FortiVoice unit. For the list of supported phones and auto provisioning prerequisites, see Configuring SIP phone auto-provisioning on page 91. • Phone type and MAC address is correctly configured. See To create or edit an IP extension on page 158. • Auto-provisioning is enabled for the extension associated with the phone through the user privilege applied to it. See Configuring user privileges on page 126. • *Check the password strength of SIP accounts*: See Auditing SIP extension password on page 164. • *Number Auditor*: Auditing extension numbers and MAC addresses on page 164 • *Send Softclient QR Code by Email*: If you have added a FortiFone-SoftClient to an extension and entered your email address as a notification option, select this option to send a QR code to the email address. The QR code will also appear on the *Preferences* page of the extension's user web portal. See Auxiliary Device on page 160 and Notification Options on page 174. • *Maintenance*: Select an extension and click this button to manage a user's voicemail box. You can check the size of the box and empty the box. Click *Back* to return to the *SIP* tab.
Configure View (icon)	Click to display or hide columns you want. You can also save the customized view or set it back to default.
Enabled	Select to activate an extension.
Number	The extension number.
Display Name	The name displaying on the extension. This is usually the name of the extension user.
Phone Model	The brand and model of the phone.
Emergency Zone	The emergency zone profile for this extension. For more information, see Configuring emergency zone profiles on page 131.
Survival Branch	If the extension belongs to a FortiVoice survivability branch, the branch information is listed. For information on survivability branch, see Configuring local survivability on page 145.
Department	If the extension belongs to an extension department, the department information is listed. For information on departments, see Creating extension departments on page 180.
Business Group	If the extension belongs to a business group, the group information is listed. For information on business groups, see Creating business groups on page 187.

GUI field	Description
Status	The extension statuses, including: • *Idle*: The extension is not in use. • *In Use*: The extension is in use. • *Busy*: The extension is busy. • *Ringing*: The extension is ringing. • *On Hold*: The extension has an on-hold call. • *Admin down*: The trunk of the extension is disabled. Under this status, the extension remains registered with the FortiVoice unit. • *Not registered*: The extension is not registered with the FortiVoice unit and is not in service. • *Unavailable*: The extension is not reachable. • *Alarm detected*: There is a problem with the phone line. • *Other*: The status other than the above.
IP	The link to the IP address of the phone using the extension number.
Phone Profile	Displays the phone profile applied to the extension. For information on phone profile, see Configuring phone profiles on page 118.
Phone Info	The model, MAC address, and firmware version of the phone for this extension.

To create or edit an IP extension

1. Go to *Extension* > *Extension* > *IP Extension.*
2. Click *New* or double-click an existing extension.
3. Configure the following:

GUI field	Description
Number	Enter the extension number following the extension number pattern. See Configuring PBX options on page 103. Click *Edit Preference* to configure the extension user preferences. See Setting extension user preferences on page 173. This option is only available when you edit an extension.
User ID	This is the system-generated ID based on the user ID prefix you set (see User ID prefix on page 106) and the extension number. This option is view only and the ID only appears when you edit an extension. You can add a new user ID through the CLI.
Enable	Select to activate the extension.
Display name	Enter the name displaying on the extension. This is usually the name of the extension user. You can click *Expand to modify caller ID* to add a caller ID for external calls or emergency calls.

GUI field			Description
Description			Enter any notes for the extension.
Device Setting			Extension SIP devices include desktop phones, soft phones, and auxiliary devices.
	Desktop Phone		
		Type	Select the desktop phone type.
		Device	Select the specific phone model. Click the *New* icon to add a new device. See Configuring desktop FortiFones on page 132. Click the *Edit* icon to modify a selected device. See Configuring desktop FortiFones on page 132. Click the *Select* icon to choose an existing device. This option is only available if you select FortiFone type.
		SIP Setting	Select the SIP profile for the phone. Click the *New* icon to add a new profile. See Configuring SIP profiles on page 115. Click the *Edit* icon to modify a selected profile. See Configuring desktop FortiFones on page 132.
		Emergency zone	Select the emergency zone profile for the phone. Click the *New* icon to add a new profile. See Configuring emergency zone profiles on page 131. Click the *Edit* icon to modify a selected profile. See Configuring emergency zone profiles on page 131.
		Programmable keys	Select the keypad profile for the phone. Click the *New* icon to add a new profile. See Configuring programmable keys profiles on page 120. Click the *Edit* icon to modify a selected profile. See Configuring programmable keys profiles on page 120. This option is only available if you select FortiFone type.
		Advanced	• *SIP password*: Enter the password used for configuring your SIP phone from the phone or the Web. You need the phone's IP to access it from the Web. You can check the password strength. See Reviewing system configuration on page 135. Click *Generate* to generate a strong password automatically. Select *View password* to display the password. If you have configured the default SIP user password (see Default SIP user password on page 105), the password appears here. However, you can change it. • *Location*: Select *Internal* if the phone does not traverse through Network Address Translation (NAT) to connect to the FortiVoice unit, and *External* if the phone does.

GUI field		Description
		These are system defined locations. • *MWI* (Message Waiting Indication): Enable or disable MWI on the phone. • *Auto answer*: Enable or disable automatic answering on the phone. • *Direct call*: Enable or disable direct calling on the phone. • *Secondary accounts*: If you enabled the option to add a secondary account for desktop FortiFones, do it here by selecting the FortiFone extension and move it to the *Selected* field. For more information, see Secondary account (Enable secondary account for Desktop FortiFone) on page 93.
Soft Phone		
	License allocation	Select the number of softphone licenses for use on this extension.
	Mobile	Click *View Login Information* and log in onto the phone using the extension’s user name and password.
	Desktop	Click *View Login Information* and log in onto the phone using the extension’s user name and password.
	SIP Setting	• *Android/iPhone*: If the soft phone is on an Android phone or iPhone, select a SIP profile for it. Click *Edit* to modify the current profile or *New* to configure a new one. For more information, see Configuring SIP profiles on page 115. • *Windows/MacOS*: If the soft phone is on a Windows or Mac device, select a SIP profile for it. Click *Edit* to modify the current profile or *New* to configure a new one. For more information, see Configuring SIP profiles on page 115.
Auxiliary Device		Click *New* to add SIP devices to the extension. This is known as SIP forking. For more information, see Desktop Phone on page 159. SIP forking allows you to have your desk phone ring at the same time as your softphone or a SIP phone on your mobile. For example, you can use SIP forking to ring your desk phone and your Android SIP phone at the same time, allowing you to take the call from either device easily. No forwarding rules would be necessary as both devices would ring. In the same manner, SIP forking can be used in an office and allow the secretary to answer calls to the extension of his/her boss when he is away or unable to take the call.

GUI field			Description
			For more information, see Configuring SIP forking on page 165. Select a device and click *Other Actions* to apply extension configuration to the device or view the extension or SIP configuration file. The selected devices will reboot and only the devices that meet the following conditions will receive the new configuration: • Devices supported by and registered to the FortiVoice unit. For the list of supported phones and auto provisioning prerequisites, see Configuring SIP phone auto-provisioning on page 91. • Device type and MAC address is correctly configured. See To create or edit an IP extension on page 158. • Auto-provisioning is enabled for the extension associated with the device through the user privilege applied to it. See Configuring user privileges on page 126.
User Setting			
	Management		Configure the extension's role in other Setting.
		User privilege	Select the services for the extension. Click *Edit* to modify the current user privilege or click *New* to configure a new one. For more information on user privilege, see Configuring user privileges on page 126.
		Department	Select the department that the extension belongs to. Click *Edit* to modify the current department or click *New* to configure a new one. For more information on extension department, see Configuring agents on page 225.
		Survival branch	Select the local survival branch FortiVoice unit for the extension if the extension is in a local survivability network. Click *Edit* to modify the current branch unit. For more information, see Configuring local survivability on page 145.
		Voicemail	Configure the extension's voice mailbox. In some cases, you may want other users or groups to share this voice mailbox. For example, a supervisor wants his/her co-workers to access his/her voice mailbox while he/she is away. *Main voice mailbox:* Select the extension's own voice mailbox (*Default*) or that of another extension as the voice mailbox of this extension. Typically, you use the default mailbox.

GUI field			Description
			If you select the voice mailbox of another extension, you can click *Edit* to modify that extension. *Users/Groups*: The FortiVoice unit turns on the message waiting light on the phones of a user or user group to notify the user or group of a new voice message stored in the voice mailbox associated with this extension. To select users or user groups, under *User(s)* and *Group(s)*, select the users/groups from the *Available* field and click -> to move them to the *Selected* field. To listen to the message after being notified, the user can dial *97 or the code you set (see Modifying feature access codes on page 271) and enter the user's own user PIN. For information on creating user groups, see Creating extension groups on page 180.
	Web Access		Configure web user portal and soft client access from mobile or desktop devices.
		Authentication type	Select the extension's authentication type: *Local* or *LDAP*.
		User password	Enter the password for user web portal access which can be much longer and stronger to mitigate the risk of password guess attack and preserve the User PIN for phone access only. Control of using personal password or voicemail PIN to access user web portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 107. You can check the password strength. See Reviewing system configuration on page 135. Click *Generate* to generate a strong password automatically. Select *View password* to display the password. This option is only available when you select *Local* for *Authentication Type*.
		LDAP profile	If you select *LDAP* for *Authentication type*, select an LDAP profile to apply to this extension. For information on LDAP profile, see Configuring LDAP profiles on page 121. You can click *New* to create a new profile or *Edit* to modify the selected one.
		Authentication ID	If you select *Try common name with base DN as bind DN* as the user authentication option in the authentication profile you select, enter the authentication ID based on the user objects' common name attribute you entered in the *Common name ID* field of the profile, such as `jdoe`.

GUI field	Description
	If you select *Search user and try bind DN* as the user authentication option in the authentication profile you select, leave this field blank. This option is only available if you select *LDAP* for *Authentication type*.
Phone Access	Configure voicemail access by phone or access to restricted phone calls.
Voicemail PIN	Enter the password for the extension user to access voicemail and the user web portal. Selection of using personal password or voicemail PIN to access user web portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 107. You can check the PIN strength. See Reviewing system configuration on page 135. Click *Generate* to generate a strong password automatically. Select the view PIN icon to display the password. If you have configured the default user PIN (see Default Voicemail PIN on page 105), the password appears here. However, you can change it.
Personal code	Enter the extension specific account code that can be used to restrict calls. This code is needed to make some restricted calls. You can click *Generate* to get a code.
Call Center	This option appears if your FortiVoice unit has a call center license. Select to configure the departments that a call center agent manages, queues that the agent belongs to, skill sets, and skill levels. Click *Create* (for new extension) or *OK* (for editing extension) and configure the following: • *Agent profile*: Select the profile for the agent. You can also create a new one or modify an existing one. For more information about agent profiles, see Configuring agent profiles on page 236. • *Management departments*: An agent manager may need to monitor call queues in certain departments. For information on setting up departments, see Creating extension departments on page 180. Click >> to select the departments to be monitored and then click *Done*. • *Member of Queues*: Click to select the call queues to join. • *Main/Outgoing queue*: This option is for collecting the outgoing calls from all queues by this agent and

GUI field	Description
	displaying them in Working with call queue statistics on page 238. You can select any queue of which this agent is a member for that purpose except *None* which will not collect agent's outgoing call information. • *Queues*: Select the queues of which you want the extension/agent to be a member, and click *Apply*. • *Skill Sets*: Click *New* to select the skill set for the agent, including skill and level, and click *Create*. For more information about agent skills and levels, see Adding agent skill sets on page 235 and Creating agent skill levels on page 235. Click *OK*.

4. Click *Create* (for new extension) or *OK* (for editing extension).

Auditing SIP extension password

You can verify the strength of SIP extension passwords. For information on setting SIP extension password, see Configuring IP extensions on page 156.

To audit a SIP extension password

1. Go to *Extension* > *Extension* > *IP Extension.*
2. Under *Actions*, click *Check the password strength f SIP accounts*.
   The *Password Auditor* page opens.
3. If a password policy warning (red check mark) appears, click the warning to view the password policy. To set the policy, see Configuring system options on page 75.
4. If the password strength of an extension shows the *Weak* (black check mark) icon, you can click the password and change it based on the policy until the password strength shows the *Strong* (green check mark) icon.
5. Click *Close*.

Auditing extension numbers and MAC addresses

You can find and modify the duplicate extension numbers and conflicting MAC addresses.

Duplicate numbers occur when there are more than one extension with the same number.

Conflicting MACs occur when there are more than one extension associated with a MAC address.

To audit SIP extension numbers

1. Go to *Extension* > *Extension* > *IP Extension.*
2. Under *Actions*, click *Number Auditor* > *Numbers*.
   The *Number* page opens and lists the duplicate numbers.
3. Select the number you want to remove and click *Edit*.
   The duplicate number's configuration page displays.
4. Remove the duplicate number in the *Number* field and click *OK*.
   For information on extension numbers, see Configuring IP extensions on page 156.

To audit extension MAC addresses

1. Go to *Extension* > *Extension* > *IP Extension.*
2. Under *Actions*, click *Number Auditor* > *MACs*.
   The *Conflict MAC* page opens and lists the multiple extensions on a single MAC address.
3. Select the number you want to remove and click *Edit*.
4. On the *IP Extension* page, go to *Device Setting* > *Device*.
5. Click the *Select* icon and click *Select None* at the bottom of the page.

Importing a list of extensions

The import feature provides a simple way to add a list of new extensions in one operation. You can create a CSV file in any spreadsheet and import the data as long as the columns match the FortiVoice format.

Your CSV file must have a headline containing the column names such as *User ID, Extension, Display name, Phone type, Mac address, and Phone profile.* Otherwise, the import will fail.

To import extension records

1. On the *IP Extension* tab, click *Actions* > *Import.*
2. Browse for the extension list file.

Configuring SIP forking

SIP forking allows you to have your desk phone ring at the same time as your softphone or a SIP phone on your mobile.

When a device is added, it inherits your master phone’s user privileges except hot-desking and fax.

You can add two SIP extensions and one external phone number.

To add a SIP device

1. Go to *Extension* > *Extension* > *IP Extension.*
2. *Double-click an extension and go to Device Setting* > *Auxiliary Devices.*

3. Click *New* and configure the following:

GUI field	Description

Type	If your device is a FortiFone, configure the following:
	• *Device*: Click the *Select* icon to choose a FortiFone and click *OK*. The phones are configured for SIP inventory. See Configuring desktop FortiFones on page 132.
	You may also add a new phone or edit an existing one.
	• *Phone model*: After you select a device, the device model appears.
	• *Setting*: If you select *Custom*, configure the following:
	  • *SIP Setting*: Select the SIP profile for the extension. Click Edit to modify the current profile or New to configure a new one. For more information, see Configuring SIP profiles on page 115.
	  • *Emergency Zone*: Select the emergency zone profile for this extension. Click *Edit* to modify the current profile or *New* to configure a new one. For more information, see Configuring emergency zone profiles on page 131.
	  • *Location*: Select *Internal* if the phone does not traverse through Network Address Translation (NAT) to connect to the FortiVoice unit, and *External* if the phone does. These are system defined locations.
	  • *Handset ID*: If the device is a FortiFone-870i that supports multiple handsets, enter or click *Generate* to identify the handset.
	  • *MWI* (Message Waiting Indication): Enable or disable MWI on the phone.
	  • *Auto answer*: Enable or disable automatic answering on the phone.
	  • *Direct call*: Enable or disable direct calling on the phone.
	• *Secondary accounts*: If you enabled the option to add a secondary account for desktop FortiFones, do it here by selecting the FortiFone extension and move it to the *Selected* field. For more information, see Secondary account (Enable secondary account for Desktop FortiFone) on page 93.

	If your device is a Generic phone, configure the following: • SIP Setting: Select the SIP profile for the extension. Click Edit to modify the current profile or New to configure a new one. For more information, see Configuring SIP profiles on page 115. • *Emergency Zone*: Select the emergency zone profile for this extension. Click *Edit* to modify the current profile or *New* to configure a new one. For more information, see Configuring emergency zone profiles on page 131.

4. Click *Create*.

Modifying managed extensions

FVG-GS16 is a FXS gateway with 16 ports. Once it is added to the FortiVoice unit, 16 extensions are generated. You can modify each of the 16 extensions.

You can also view the local survivability branch paging numbers and change its password.

For information on adding the gateway, see Managing FXS gateways on page 139.

For information on configuring local survivability branches, see Configuring local survivability on page 145

To edit a GS16 or local survivability branch extension

1. Go to *Extension* > *Extension* > *Managed Extension.*
2. In *Gateway device*, select:
   - the GS16 gateway of which you want to modify the extension, or
   - the local survivability branch of which you want to modify the paging number.
3. Select the extension or paging number and click *Edit*.
4. If you selected a local survivability branch paging number, you can view the information and enter the display name and change the password. If you selected a GS16 gateway extension, configure the following:

GUI field	Description
Number	Enter the extension number following the extension number pattern. See Configuring PBX options on page 103.
User ID	This is the system-generated ID based on the user ID prefix you set (see User ID prefix on page 106) and the extension number. This option is view only and only appears when you edit an extension. You can add a new user ID through the CLI.
Enable	Select to activate the extension.
Display name	Enter the name displaying on the extension. This is usually the name of the extension user. Click the + sign if you want to add caller IDs: • *External caller ID*: Enter the external caller ID that displays on a called phone when you make a call. Use the `name<phone_number>` format, such as `HR<222134>`. • *Emergency caller ID*: Enter the emergency caller ID. Use the `name<phone_number>` format, such as `HR<222134>`. If you do not enter the caller IDs, your organization's main number will be used. If you add both IDs, the emergency ID will only be used when making emergency calls. All other calls will use the external caller ID.
Description	Enter any notes for the extension.
Device Setting	See Editing gateway extensions on page 140.
User Setting	See User Setting on page 161

5. Click *OK*.

Modifying analog extension (200D-T, 1000E-T, and 20E2 models only)

The FortiVoice 200D-T and 1000E-T each has one analog port and a default analog extension. The FortiVoice 20E2 has two analog ports and two default analog extensions.You can edit the extensions' default configuration.

Analog lines, also referred to as POTS (Plain Old Telephone Service), are used for standard phones, fax machines, and modems.

To view the default analog extension, go to *Extension* > *Extension* > *Analog Extensions*.

GUI field	Description
Maintenance	Select an extension and click this button to manage its voicemail box. You can check the size of the box and empty the box. Click *Back* to return to the *Analog* tab.
Enabled	Select to activate the extension.
Number	The analog extension number.
Display Name	The name displaying on the extension.

To edit the default analog extension

1. Go to *Extension* > *Extension* > *Analog Extensions.*
2. Select the default extension and click *Edit*.
3. Configure the following:

GUI field	Description
Number	Enter the extension number following the extension number pattern. See Configuring PBX options on page 103. If required, click *Edit Preference* to modify the user preferences. See Setting extension user preferences on page 173
User ID	This is the system-generated ID for the extension and is read-only.
Analog port	Select the analog port for the extension. You can click Edit to modify the port.
Enable	Select to activate the extension.
Display name	Enter the name displaying on the extension. This is usually the name of the extension user. Click the + sign if you want to add caller IDs: • *External caller ID*: Enter the external caller ID that displays on a called phone when you make a call. Use the `name<phone_number>` format, such as `HR<222134>`. • *Emergency caller ID*: Enter the emergency caller ID. Use the `name<phone_number>` format, such as `HR<222134>`. If you do not enter the caller IDs, your organization's main number will be used. If you add both IDs, the emergency ID will only be used when making emergency calls. All other calls will use the external caller ID.
Description	Add any notes for the extension.
User Setting	See User Setting on page 161.

4. Click *OK*.

Setting up remote extensions

A remote extension reaches an external phone by automatically selecting a line from a trunk and dialing the phone number. For example, a remote extension could reach an employee’s cell phone or home phone, or a phone at a branch office.

A caller can connect to a remote extension through the auto attendant, or can be transferred to a remote extension by a call cascade. A user at a local extension can manually transfer a caller to a remote extension, or can dial a remote extension directly. If the remote extension is busy or unanswered, the system can route the call using the remote extension’s call cascade.

For example, a caller reaches the auto attendant and dials a local extension. The user is not there, so the call is unanswered. The call cascade of the local extension can be configured to transfer unanswered calls to a remote extension. The remote extension can be configured to dial the user’s cellular phone. This way the user is available outside the office.

Remote extensions are designed to operate with local major telephone service providers. The feature may not function correctly with some telephone and mobile operator’s networks, especially for international phone numbers and mobile phones roaming internationally.

To configure a remote extension

1. Go to *Extension* > *Extension* > *Remote Extension.*
2. Click *New*.

3. Configure the following:

GUI field	Description
Number	Enter the local extension number from which calls are transferred to a remote extension.
Remote number	Enter the remote phone number to which a call to the local extension is transferred. You can enter digits 0–9, space, dash, comma, # and *. If you want to enter an auto attendant number followed by an extension, you can use comma (,) or semicolon (;) to pause the automatic dialing. A comma pauses dialing for two seconds, for example, 1-123-222-1234, 5678#. In this case, once auto attendant 1-123-1234 is dialed, and after two seconds, extension 5678 is automatically dialed. A semicolon pauses dialing for one second, for example, 1-123-222-1234; 5678#. In this case, once auto attendant 1-123-1234 is dialed, and after one second, extension 5678 is automatically dialed.
Enable	Select to activate the remote extension.
Display name	The name displaying on the remote extension when a call is transferred. You can choose to display the name differently than the one you entered here. See Modifying caller IDs on page 116. Click the + sign if you want to add caller IDs: • *External caller ID*: Enter the external caller ID that displays on a called phone when a call is transferred through the remote extension. Use the `name<phone_number>` format, such as `HR<222134>`. • *Emergency caller ID*: Enter the emergency caller ID. Use the `name<phone_number>` format, such as `HR<222134>`. If you do not enter the caller IDs, your organization's main number will be used. If you add both IDs, the emergency ID will only be used when making emergency calls. All other calls will use the external caller ID.
Description	Enter any notes you have for the extension.
User Setting	See User Setting on page 161.

4. Click *Create*.

Configuring fax extensions

If you want to continue using your fax machine with the VoIP phone system, connect the fax machine to an adapter (such as OBIHAI OBi 200, Cisco SPA 112, or Grandstream HT 702) that supports T38 first before connecting it to the FortiVoice unit. T38 is a protocol designed to allow fax to travel over a VoIP network.

In this case, the fax machine is treated like an extension. The FortiVoice unit receives faxes and relays them to the fax machine. Faxes sent from the fax machine will follow the fax sending dial plans.

To use this option, you need to create and enable the fax extensions first. You then need to configure the FortiVoice unit to receive and relay the faxes to the fax machine.

For information on fax configuration, see Configuring fax on page 263.

To create or edit a fax extension

1. Go to *Extension* > *Extension* > *Fax Extension.*
2. Click *New* or double-click an existing extension.
3. Configure the following:

GUI field	Description
Number	Enter the extension number following the extension number pattern. See Configuring PBX options on page 103.
User ID	This is the system-generated ID based on the user ID prefix you set (see User ID prefix on page 106) and the extension number. This option is view only and only appears when you edit an extension. You can add a new user ID through the CLI.
Enable	Select to enable this extension to receive and send faxes that support T38 protocol. This applies to using a fax machine connected to the FortiVoice unit via an adapter that supports T38 protocol. For more information, see Configuring fax on page 263.
Display Name	Enter the name displaying on the extension.
Description	Enter any notes about the extension.
Device Setting	• *SIP Setting*: Select the SIP profile for the phone. Click the *New* icon to add a new profile. See Configuring SIP profiles on page 115. Click the *Edit* icon to modify a selected profile. See Configuring desktop FortiFones on page 132. • *Emergency zone*: Select the emergency zone profile for the phone. Click the *New* icon to add a new profile. See Configuring emergency zone profiles on page 131. Click the *Edit* icon to modify a selected profile. See Configuring emergency zone profiles on page 131. • *Advanced*: • *SIP password*: Enter the password used for configuring your SIP phone from the phone or the Web. You need the phone's IP to access it from the Web. You can check the password strength. See Reviewing system configuration on page 135. Click *Generate* to generate a strong password automatically. Select *View password* to display the password. If you have configured the default SIP user password (see Default SIP user password on page 105), the password appears here. However, you can change it. • *Location*: Select *Internal* if the phone does not traverse through Network Address Translation (NAT) to connect to the FortiVoice unit, and *External* if the phone does. These are system defined locations.
User Setting	
Management	Configure the extension’s role in other Setting.

GUI field	Description
User privilege	Select the services for the extension. Click *Edit* to modify the current user privilege or click *New* to configure a new one. For more information on user privilege, see Configuring user privileges on page 126.
Department	Select the department that the extension belongs to. Click *Edit* to modify the current department or click *New* to configure a new one. For more information on extension department, see Configuring agents on page 225.
Survival branch	Select the local survival branch FortiVoice unit for the extension if the extension is in a local survivability network. Click *Edit* to modify the current branch unit. For more information, see Configuring local survivability on page 145.
Web Access	Configure web user portal and soft client access from mobile or desktop devices.
Authentication type	Select the extension's authentication type: *Local* or *LDAP*.
User password	Enter the password for user web portal access which can be much longer and stronger to mitigate the risk of password guess attack and preserve the User PIN for phone access only. Control of using personal password or voicemail PIN to access user web portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 107. You can check the password strength. See Reviewing system configuration on page 135. Click *Generate* to generate a strong password automatically. Select *View password* to display the password. This option is only available when you select *Local* for *Authentication Type*.
LDAP profile	If you select *LDAP* for *Authentication type*, select an LDAP profile to apply to this extension. For information on LDAP profile, see Configuring LDAP profiles on page 121. You can click *New* to create a new profile or *Edit* to modify the selected one.
Authentication ID	If you select *Try common name with base DN as bind DN* as the user authentication option in the authentication profile you select, enter the authentication ID based on the user objects' common name attribute you entered in the *Common name ID* field of the profile, such as `jdoe`. If you select *Search user and try bind DN* as the user authentication option in the authentication profile you select, leave this field blank. This option is only available if you select *LDAP* for *Authentication type*.
Phone Access	Configure voicemail access by phone or access to restricted phone calls.
Voicemail PIN	Enter the password for the extension user to access voicemail and the user web portal. Selection of using personal password or voicemail PIN to access user web portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 107.

GUI field		Description
		You can check the PIN strength. See Reviewing system configuration on page 135. Click *Generate* to generate a strong password automatically. Select the view PIN icon to display the password. If you have configured the default user PIN (see Default Voicemail PIN on page 105), the password appears here. However, you can change it.
	Personal code	Enter the extension specific account code that can be used to restrict calls. This code is needed to make some restricted calls. You can click *Generate* to get a code.

4. Click *Create* (for new extension) or *OK* (for editing extension).

Setting extension user preferences

Each SIP and analog extension comes with its default user preferences, including voicemail Setting and phone display preference. You can modify these Setting.

Phone users can modify the preferences on the web user portal.

To view the list of extensions, go to *Extension* > *Extension* > *Preference*.

GUI field	Description
Maintenance	Select an extension and click this option to reset the user preferences to the default values.
Number	The extension number.
Display name	The name displaying on the extension. This is usually the name of the extension user.
Voice Message Count	The number of voice mails left on an extension.

To edit extension user preferences

1. Go to *Extension* > *Extension* > *Preference.*
2. Select an extension and click *Edit*.
3. Configure the following:

GUI field		Description
Voicemail Setting		
	Number	The extension number. This is read-only.
	User ID	This is the system-generated ID based on the extension number. You can add a new user ID through the CLI. This is read-only.
	Display name	The name displaying on the extension. This is usually the name of the extension user.

GUI field		Description
		This is read-only.
	Emergency caller ID	The caller ID to display on the destination phone when you dial the emergency number, such as 911. This ID is set when you configure the extension. This is read-only.
	External caller ID	The caller ID you want to display on a called phone instead of the FortiVoice main number (see Main number on page 103) or the trunk phone number (see Phone Number on page 194). This ID is set when you configure the extension. This is read-only.
	Ring duration	Enter the phone ringing duration in seconds before an incoming call goes to voicemail.
	Programmable keys	Select the keypad profile for the phone. Click the *Edit* icon to modify a selected profile. See Configuring programmable keys profiles on page 120.
	Call forward	Select to forward phone calls and enter the phone number to forward the calls. This function only works if call forwarding is enabled in the extension’s user privilege. See Configuring user privileges on page 126.
	Call waiting	Select to enable call waiting. This function only works if call waiting is enabled in the extension’s user privilege. See Configuring user privileges on page 126.
	Do not disturb	Select to enable DND. This function only works if DND is enabled in the extension’s user privilege. See Configuring user privileges on page 126.
	Voicemail handling (Caller press 0 during announcement)	Select to enable reaching the operator by pressing 0 when you hear the announcement of a callee’s voicemail.
	Include caller ID number when playing voicemail message	Select to announce caller’s ID when playing the voicemail.
	Include date and time when playing voicemail message	Select to announce date and time when playing the voicemail.
Notification Options		
	Voicemail	Select the type of email notification when this extension has a voicemail: • *None*: Do not send any notification. • *Simple*: Send an email notification. • *With attachment*: Send an email notification with the

GUI field		Description
		voicemail attached.
	Fax	Select the type of email notification when this extension has a fax: • *None*: Do not send any notification. • *Simple*: Send an email notification. • *With attachment*: Send an email notification with the fax attached.
	Missed call	Select *On* if you want to receive an email notification when an incoming call is missed.
	Email address	Enter the email address to which an email notification is sent.

Voicemail Options		Configure greeting, unavailable, and busy messages.
		Name: Your name of the voicemail. For example, John Doe.
		• *Standard*: Use the system default name for the voicemail. This will be the extension number.
		• *Personal*: Use your own name for the voicemail.
		    • Click *Call me* to ring your extension and record a name using the phone, such as your name or extension number.
		    • Click *Upload* to import a name, such as your name or extension number.
		    • Click *Play* to listen to a recorded name.
		    • Click *Erase* to delete a recorded name.
		    • Click *Download* to save a recorded name.
		Greeting: Select the voicemail greeting mode and greeting content.
		• *Standard*: The system defined greeting.
		• *Simple*: The customer-recorded greeting that applies to any time except when the line is busy and extension is unavailable.
		• *Scheduled*: The customer-recorded greeting that comes with a schedule.
		• *Conditional*: The customer-recorded greeting that only applies to occasions when the line is busy or extension is unavailable.
		• *Audio file:* Click to configure the greeting. This option is only available when you select *Simple*, *Scheduled* or *Conditional.*
		    • Click *Call me* to ring your extension and record a message such as a greeting, unavailable, or busy

GUI field		Description
		message using the phone. This applies to the *Simple* and *Scheduled* modes. • Click *Upload* to import a message such as a greeting, unavailable, or busy message. • Click *Play* to listen to a message such as a greeting, unavailable, or busy message. • Click *Erase* to delete a message such as a greeting, unavailable, or busy message. • Click *Download* to save a message such as a greeting, unavailable, or busy message. If you select *Scheduled* for *Greeting*, click *New* to add a system schedule or create a new one. You can also add a greeting file which is the audio file you configured when clicking *Audio file*. The purpose of having a separate voicemail name file is for occasions that you just want to change the name without touching the greeting file.
Display Preference		Configure the preference for screen display on the user web portal.
	Phone language	Select the prompt language for the extension. The default is English. For information on adding prompt languages, see Managing phone audio settings on page 110.
	Web language	Select the language for the FortiVoice user web portal.
	Theme	Select the display theme for the FortiVoice user web portal.
	Time zone	Select the time zone for the FortiVoice user web portal.
	Idle timeout	Set the timeout for the FortiVoice user web portal.
Account Management		
	Change PIN number	Click to change the password for accessing the voice mailbox and the FortiVoice user web portal.
	Change User Password	Click to change the password for accessing the FortiVoice user web portal.
	SIP User ID and Password	Click to display the extension number and the SIP user password which is used for configuring your SIP phone from the phone or the Web.
Agent		This option appears if you have a call center license.
	PIN required to login/logout from phone	Select to enable an agent to log into/log out of a queue from the extension using the user PIN. For information on feature access codes, see Configuring account codes on page 154.

GUI field		Description
	PIN required to pause/unpause from phone	Select to enable an agent to pause/unpause a queue from the extension using the user PIN. To pause means the agent is not answering calls. For information on feature access codes, see Configuring account codes on page 154.
	Auto-Pause after agent login queue	Select to automatically put the agent in pause (not ready) status after the agent logs into a queue. The agent can unpause a queue to answer calls. For information on feature access codes, see Configuring account codes on page 154.
Follow Me		See Configuring follow me settings on page 177.
Call Handling		*Retain original caller ID*: Select to maintain the original caller's identity when forwarding an inbound call. *Call screening*: Select if you want the FortiVoice unit to prompt callers for their names so that callees can identify the callers before the connect to you. *Record caller name*: By default, this option is selected when you select *Call screening.* If you deselect this option, the FortiVoice unit will not prompt callers for their names. Instead, the FortiVoice unit will ring a called phone but will not connect to the caller. The callee is able to pick up the phone and see the caller's ID and decide whether to pick up the call. For more information on normal or quick call handling, see Handling calls on page 178.
Twinning Setting		This option is only available if *Twinning* is selected in the user privileges of the extension. For more information, see Twinning on page 127. • *Setting*: Select the twinning method. • *Disabled*: Select to disable twinning. • *Simple*: Select to configure a basic twinning by adding a phone number. • *Scheduled*: Select to configure a twinning by adding phone numbers based on a schedule.

4. Click *OK*.

Configuring follow me settings

Follow me allows a call to an extension to be transferred to another destination when you are not available.

This configuration serves as a profile for use in managing calls. See Handling calls on page 178.

To configure follow me Setting

1. Go to *Extension* > *Extension* > *Preference* > *Follow Me.*
2. Click *New*.
3. Enter a *Name* for this setting.
4. Under *Follow Me Numbers*, click *New.*
5. Enter a phone number to which the call to your extension can be transferred.
6. Enter the phone ringing duration, in seconds, before the call goes to voicemail or next number in the sequence.
7. Click *Create*.
8. Repeat steps Under Follow Me Numbers, click New. on page 178 to Click Create. on page 178 of this procedure to add more numbers if you want to transfer a follow me call to multiple numbers in a sequence. The numbers will be dialed according to the sequence in the follow me setting.

Handling calls

Extension > *Extension* > *Preference* > *Call Handling* allows you to manage the call process. For example, you can configure the process to forward a call to another number on a specific schedule.

You can manage a normal call handling by configuring the call process for different situations. You can also manage quick call handling by dialing a code to enter into a default mode and configure the call process for that particular mode if required.

If the extension with configured call handling action is part of another FortiVoice function that also has configured call handling action (for example, a member of a ring group or used for a virtual number), then the call handling action of the other FortiVoice function overrides the extension call handling action.

To handle a normal call

1. Go to *Extension* > *Extension* > *Preference* > *Call Handling.*
2. Click *Normal Call Handling*.
3. Select a call status.
   Each status can only be used for one call management configuration.
4. Select *System default action* or *User defined* action.
   The *System default action* (action shows in brackets) changes depending on the status selection.
5. If you select *User defined*, click *New* to define a call process according to a schedule.
   - Select a pre-configured *Schedule* for the call action. You can click *View* to display the schedule details. For information on configuring schedules, see Scheduling the FortiVoice unit on page 131.
   - For *Call from*, select the call type on which you want to take an action.
   - Add an *Action* for the call process.
     For some call handling processes that may require further actions, you need to add one or more call processes to complete the call handling. For example, after adding a process that contains a *Forward* action, you can add another process with a *Go voicemail* action to complete the call handling. In this case, the call will be forwarded to the phone specified and if the phone is not picked up, a voicemail will be left on this extension.

     Default action is equal to the action when you select *System default action* under *Call Process*.
     - If you select *Follow me*, select a follow me profile. For information on configuring follow me, see Follow Me on page 177.
       This option is available only if call forwarding is enabled in the extension’s user privilege. See Configuring user privileges on page 126.
     - If you select *Play announcement*, select a sound file. For information on configuring sound files, see Managing phone audio settings on page 110

    - If you select *Auto attendant*, select an auto attendant profile. For information on configuring auto attendant, see Configuring auto attendants on page 250.
    - f you select *Forward*, enter the number to which you want to forward the call.
      This option is available only if call forwarding is enabled in the extension's user privilege. See Configuring user privileges on page 126.
  - Click *Create*.
6. Click *OK*.

To handle a quick call

1. Go to *Extension* > *Extension* > *Preference* > *Call Handling* > *Quick call handling.*

GUI field	Description
Effective mode	Displays the call handling status when you dial *720, *721, *722, and *723. For example, if you dial *720, the status will be *Normal* because you have canceled the quick mode.
*720	Dial the code to cancel the quick handling mode.
*721	Dial the code to set to *Out of office* mode. Click the text to modify the quick mode option and time as required.
*722	Dial the code to set to *Away* mode. Click the text to modify the quick mode option and time as required.
*723	Dial the code to set to *Other* mode. Click the text to modify the quick mode option and time as required.

2. If you want to add a new quick call handling process, click *Quick Call Handling*.
3. Select a call status.
   Each status can only be used for one call management configuration.
4. Click *New* to define a call process according to a schedule.
   - Select a pre-configured *Schedule* for the call action. You can click *View* to display the schedule details. For information on configuring schedules, see Scheduling the FortiVoice unit on page 131.
   - Add an *Action* for the call process. You can add multiple actions to process a call in sequence. For example, you can add *Play announcement* and then *Auto attendant*. In this case, an incoming call will be transferred to the auto attendant after an announcement is played.
   - *Default action* is equal to the action when you select *System default action* under *Call Process*.
     - If you select *Follow me*, select a follow me profile. For information on configuring follow me, see Follow Me on page 177.
       This option is available only if call forwarding is enabled in the extension's user privilege. See Configuring user privileges on page 126.
     - If you select *Play announcement*, select a sound file. For information on configuring sound files, see Managing phone audio settings on page 110
     - If you select *Auto attendant*, select an auto attendant profile. For information on configuring auto attendant, see Configuring auto attendants on page 250.
     - If you select *Forward*, enter the number to which you want to forward the call. This option is available only if call forwarding is enabled in the extension's user privilege. See Configuring user privileges on page 126.
   - Click *Create*.
5. Click *OK*.

Creating extension groups

Extension > *Group* lets you configure extension groups including extension departments, ring groups, page groups, and pickup groups.

This section contains the following topics:

Creating user groups

You can create a user group and use it to simplify the configuration of an IP extension voice mailbox, a general voice mailbox, a ring group, a page group, or a pickup group. For example, when creating a ring group, you can select the name of a user group rather than entering each user name individually.

For information on creating IP extension voice mailboxes, see Configuring IP extensions on page 156.

For information on creating general voice mailboxes, see Setting up general voice mailboxes on page 187.

To create a user group

1. Go to *Extension* > *Group* > *User Group.*
2. Click *New*.
3. Enter a name for the group.
4. Optionally, select a department from which you want to configure a user group. For information on extension department, see Creating extension departments on page 180.
5. For *Members,* select the available users or user groups that you want to include in the group and click -> to move them into the *Selected* field.
6. Click *Create*.

Creating extension departments

You can create department profiles for applying to the extensions. For example, you can create a department profile called HR and apply it to extension 1111 to indicate that this extension belongs to the HR department.

For information on applying department profiles, see Setting up local extensions on page 156.

To create an extension department

1. Go to *Extension* > *Group* > *Department.*
2. Click *New*.
3. In the *Name* field, enter the name of the department.
4. In the *Comment* field, enter any notes you have for this department.

5. If you have the call center license, the *Call Center* section appears. For information on call centers, see Setting up a Call Center on page 216.
   a. To set up a call center member group, under *Member,* select the available users or user groups that you want to include in the group and click -> to move them into the *Selected* field.
   b. To set up a call center manager group, under *Manager,* select the available users or user groups that you want to include in the group and click -> to move them into the *Selected* field.
   c. To set up a call center queue group, under *Queue,* select the available users or user groups that you want to include in the group and click -> to move them into the *Selected* field.
6. Click *Create*.

Creating ring groups

A ring group is a group of local extensions and external numbers that can be called using one number. Local extensions and auto attendants can dial a ring group.

A ring group can reach a group of extensions. For example, ring group 301 can ring the sales group at extensions 111, 112, 113, and 114. When a customer calls the sales group, the first available salesperson answers for the group.

To create a ring group

1. Go to *Extension* > *Group* > *Ring Group.*
2. Click *New*.

3. Configure the following:

GUI field	Description
Name	Enter the name for the ring group.
Number	Enter the ring group number following the extension number pattern. See Configuring PBX options on page 103. Clicking in the field displays a list of crossed-out extensions. These numbers are already used and cannot be used as ring group numbers. The ring group number, once dialed, will ring all the extensions in the group.
Display Name	Enter the name displaying on the extensions of the ring group, such as “HR”.
Enable	Select to activate the ring group.
Ring mode	Select how you want the ring group to be called. • *All*: All extensions in the group will ring when the ring group number is dialed. • *Sequential*: Each extension in the group is called one at a time in the order in which they have been added to the group. You can set a timeout period for each ring.
Department	Select the department to which this group belongs.
Members	Select the available extensions or user groups that you want to include in the ring group and click -> to move them into the *Selected* field. For information on creating extensions and user groups, see Setting up local extensions on page 156 and Creating extension groups on page 180.
External numbers	Click *New* to add an external phone number to the ring group. For example, you can add the number of a remote employee to a ring group.
Normal Call Handling	Use this option to configure the call handling for the ring group when you edit a ring group. For more information, see Configuring ring group call handling on page 183.
Advanced setting	• *Ring Pattern*: Select a ring pattern for the group. • *Ring duration*: Set the amount of time in seconds allowing all extensions or each one to ring before going to voicemail. • *Early media*: Select the ring tone for the group. For creating new sound files, see Managing phone audio settings on page 110. • *Caller ID option*: Select how you want the caller ID to display. • *Call waiting*: Select to enable call waiting. • *Emergency call option*: Select *Display emergency caller ID* to show the emergency caller’s ID, or *Disconnect ongoing call* to stop a call that uses the line for emergency call.

4. Click *Create*.

Configuring ring group call handling

Use the *Normal Call Handling* option to configure the call automation. For example, you can configure the process to forward a call to another number on a specific schedule.

You can only configure ring group call handling when editing a ring group.

If the ring group with configured call handling action is part of another FortiVoice function that also has configured call handling action (for example, a member of another ring group or the ring group extension is used for a virtual number), then the call handling action of the other FortiVoice function overrides the ring group call handling action.

For information on the *Normal Call Handling* option, see Normal Call Handling on page 182.

To configure the call process

1. On the *Ring Group* page, click *Normal Call Handling*.
2. Select a call status.
   Each status can only be used for one call management configuration.

   For the *Busy* status, if you set the ring group's ring mode to *All*, the FortiVoice unit will declare the ring group busy only if all extensions in the group are busy; if you set the ring group's ring mode to *Sequential*, the FortiVoice unit will declare the ring group busy only if the last extension in the group is busy after ringing the extensions sequentially and each one is busy at the time of being rung.
3. Select *System default action* or *User defined* action.
   The *System default action* changes depending on the status selection.
4. If you select *User defined*, click *New* to define a call process according to a schedule.
   - Select a pre-configured *Schedule* for the call action. You can click *View* to display the schedule details. For information on configuring schedules, see Scheduling the FortiVoice unit on page 131.
   - Add an *Action* for the call process. You can add multiple actions to process a call in sequence. For example, you can add *Play announcement* and then *Auto attendant*. In this case, an incoming call will be transferred to the auto attendant after an announcement is played.
     Default action is equal to the action when you select *System default action* under *Call Process*.
     - If you select *Voicemail*, enter the extension number of the voice mail.
     - If you select *Play announcement*, select a sound file. For information on configuring sound files, see Managing phone audio settings on page 110
     - If you select *Auto attendant*, select an auto attendant profile. For information on configuring auto attendant, see Configuring auto attendants on page 250.
     - If you select *Forward*, enter the number to which you want to forward the call.
       This option is available only if call forwarding is enabled in the extension's user privilege. See Configuring user privileges on page 126.
   - Click *Create*.
5. Click *OK*.

Creating page groups

A page group is a group of extensions that can be paged using one number. Page groups require telephones that support group paging.

A page group can reach a group of extensions. For example, page group 301 can ring the sales group at extensions 111, 112, 113, and 114. When a call reaches 301, all extensions in the group can pick up and answer the call.

To create a page group

1. Go to *Extension* > *Group* > *Paging Group.*
2. Click *New*.
3. Enter a name for the group.
4. Enter the page group number following the extension number pattern. See Configuring PBX options on page 103. This is the number that, once paged, will ring all the extensions in the group.
5. Enter the name displaying on the extensions of the group, such as "HR".
6. Select *Enable* to activate this group.
7. For *Caller ID option*, select how you want to display the ID of a caller to the group.
   - *No change*: the caller ID will display as is.
   - *Replace*: the caller ID will be replaced by the *Display name* you set.
   - *Prefix*: the caller ID will be prefixed with the *Display name* you set.
   - *Replace by Caller ID from IVR:* the caller ID will be replaced by the IVR caller ID. For information on IVR, see Configuring IVRs on page 225.
   - *Prefix with Caller ID from IVR:* the caller ID will be prefixed by the IVR caller ID. For information on IVR, see Configuring IVRs on page 225.
8. For *Emergency call option*, do the following:
   - Select *Display emergency caller ID* to show the caller ID.
   - Select *Disconnect ongoing call* to interrupt a page in progress when an emergency page comes in.
9. Select the department to which this group belongs.
10. For *Members*, select the available extensions or extension groups that you want to include in the page group and click -> to move them into the *Selected* field.
11. Click *Create*.

Creating multicast paging groups

When being applied in a message group configuration, multicast paging provides a more robust and efficient mechanism to deliver audio and text messages to larger page groups.

For more information on message groups, see Creating message groups on page 185.

To create a multicast paging group

1. Go to *Extension* > *Group* > *Multicast Paging Group.*
2. Click *New* and configure the following:

GUI field	Description
Name	Enter a unique name for the group.
Number	Enter the multicast paging group number following the extension number pattern. See Configuring PBX options on page 103. This is the number that, once paged, will ring all the extensions in the group.
Display name	Enter the name displaying on the extensions of the group, such as "HR".
Status	Select to activate this group.

GUI field	Description
Multicast IP	Enter the multicast address to which the FortiVoice unit can send a single copy of voice or text data, which is then distributed to an entire group of phones.
Multicast Port	Enter the port number on the multicast server through which the FortiVoice unit can send a single copy of voice or text data.
Alert tone	Select to enable notification tone.
Members	Click *Configure Members* and select the available extensions or extension groups that you want to include in the multicast group and click -> to move them into the *Selected* field. Click *OK*.
Description	Select *Click to edit* to enter any notes you have for the group.

3. Click *Create*.

Creating message groups

Message group provides a mass notification service for delivering audio and/or text messages to FortiFones in user groups or a multicast paging group. This solution supports standalone FortiVoice deployments and/or integration with 3rd party Mass Notification Systems to provide emergency notification using FortiFone IP desktop phones.

For more information on multicast paging group, see Creating multicast paging groups on page 184.

To create a message group

1. Go to *Extension > Group > Message Group.*
2. Click *New* and configure the following:

GUI field		Description
Name		Enter a unique name for the group.
Number		Enter the message group number following the extension number pattern. See Configuring PBX options on page 103. This is the number that, once dialed, will send text or audio message to all the extensions in the group.
Display name		Enter the name displaying on the extensions of the group, such as “HR”.
Status		Select *Status* to activate this group.
Message type		Select to send text or audio message.
If you select to send text message, configure the following:		
	Title	Enter the message title.
	Message	Use the variables to compose your message or enter your message directly.
	Delay	Enter the time in seconds that you want to delay sending the text.

GUI field		Description
	Display time	Enter the time in seconds on how long you want the message to display on the extensions.
	Alert tone	Select to activate notification alert on the extensions.
	User group	Click *Configure Members* to select the user groups for this message group and click *OK*. For information on user groups, see Creating user groups on page 180.
If you select to send audio message, configure the following:		
	Sound file	Select an existing sound file or click *New* to create a new one for the audio message. For information on sound files, see Managing phone audio settings on page 110
	Multicast group	Select the multicast paging group for this message group or click *New* to create a new one for the audio message. For information on user groups, see Creating multicast paging groups on page 184.
	Single number	Enter the external phone number to which you want to send this message and click *OK*.

3. Click *Create*.

Creating pickup groups

Some organizations cannot afford to miss phone calls on any extensions. Pickup groups allow some members in a group to answer incoming calls that ring on other extensions while the users are away.

Pickup groups can press the feature codes to pick up incoming calls that ring on other extensions. For more information, see Modifying feature access codes on page 271.

To create a pickup group

1. Go to *Extension > Group > Pickup Group.*
2. Click *New*.
3. Enter a name for the group.
4. Select *Enable* to activate this group.
5. Select the department to which this group belongs.
6. For *Members*, select the *Available* extensions or user groups that you want to include in the pickup group and click -> to move them into the *Selected* field.
   For information on creating extensions and user groups, see Setting up local extensions on page 156 and Creating extension groups on page 180.
7. For *Pickup by members*, select the *Available* extensions or user groups that are allowed to answer incoming calls that ring on other extensions and click -> to move them into the *Selected* field.
8. Click *Create*.

Creating business groups

Business group introduces an abbreviated extension number dialing for phone users in the same logical group. For multi-location enterprise deployments, the abbreviated dialing function allows phone users to dial other extension numbers in the same business group using a shortened number of digits instead of the full extension number.

This option is available for FortiVoice 500F and 1000E and above and only if *Automatic* is selected for *Business Group* under *Phone System* > *Setting* > *Miscellaneous*.

To create a business group

1. Go to *Extension* > *Group* > *Business Group.*
2. Click *New*.
3. Enter a name for the group.
4. Select *Status* to activate this group.
5. Enter the extension *Abbreviated prefix code* for the group, such as 9.
   Any extension with the prefix you enter is included in this business group.
6. For *Abbreviated dialing pattern*, enter the pattern following the extension number pattern. For example, XXXX matches any four-digit number. You can simply dial the last four-digit number of an extension in this group without using the prefix. See Configuring PBX options on page 103.
7. For *Description*, click *Edit* to enter any notes you have for the group.
8. Click *Create*.

Setting up general voice mailboxes

Some organizations, such as the sales team of a company, may have the need to share voice mails within multiple users or a user group for better service and efficiency. With a general voice mailbox, when there is a new voice mail, the entire group is copied or notified. Any member of the group can access the voice mail and once this is done, the notification is gone and others know that the voice mail has been taken care of.

To set up a general voice mailbox

1. Go to *Extension* > *General Voicemail* > *General Voicemail.*
2. Click *New*.

3. Configure the following:

GUI field	Description
Number	Enter the mailbox extension number following the extension number pattern. See Configuring PBX options on page 103.
User ID	This is the system-generated ID based on the mailbox extension number. This option is view only. You can add a new user ID through the CLI.
Enable	Select to activate the mailbox extension.
Display name	Enter the name of the mailbox extension.
Description	Enter any notes for the extension’s mailbox.
User Setting	See User Setting on page 161.

4. Click *Create*.

Working with virtual numbers

A virtual number is an extension that is not assigned to a phone. Unlike auto attendants, when a call goes to a virtual number, the caller does not need to manually select any options by pressing the phone keys. The call process is automated based on time schedules. For example, for after business hour phone calls, you can configure a virtual number to play an announcement, then transfer the call to the voice mailbox. You can also transfer the calls to the auto attendant where the callers can manually select the options based on the auto attendant configuration.

If the virtual number with configured call handling action is part of another FortiVoice function that also has configured call handling action (for example, a member of a ring group), then the call handling action of the other FortiVoice function overrides the virtual number call handling action.

To configure a virtual number

1. Go to *Extension > Virtual Number > Virtual Number* and click *New*.
2. Configure the following:

GUI field	Description
Name	Enter a name for the virtual number.
Number	Enter the virtual number which is not assigned to any phone.
Display name	Enter the name displaying on the extension. This is usually the name of the extension user.
Enable	Select to activate this virtual number.
Bypass sub call handling	Select if you want to bypass the call handling configuration embedded in the call handling of this virtual number.
Comment	Enter any notes you have for the virtual number.
Call Handling	Use this option to configure the call handling for the virtual number. For more information, see Configuring virtual number call handling on page 189.

3. Click *Create*.

Configuring virtual number call handling

Use the *Call Handling* option to configure the call automation. For example, you can configure the process to forward a call to another number on a specific schedule.

For information on the *Call Handling* option, see Call Handling on page 188.

To configure the call process

1. On the *Virtual Number* page, click *New* under *Call Handling*.
2. Select a pre-configured *Schedule* for the call action. You can also click *New* to create a schedule or *Edit* to modify the selected one. For information on configuring schedules, see Scheduling the FortiVoice unit on page 131.
3. Select an *Action* for the call handling.
   Some actions require that you enter further information to complete the call process, such as *Dial extension* and *General mailbox*.

   For some call handling processes that may require further actions, you need to add one or more call processes to complete the call handling. For example, after adding a process that contains a *Set call queue priority* action, you can add another process with a *Call queue* action to complete the call handling. In this case, the call will be processed again with new priority after it is transferred to the queue.
4. Click *Create*.

Configuring Trunks

Setting up trunks enables the FortiVoice unit to connect to the outside world. You can configure trunks that go to your VoIP service provider for long-distance calls, trunks for your PSTN circuits, and trunks that connect your various offices together.

Trunks are applied to user extensions and dial plans. For more information, see Configuring Extensions on page 156 and Configuring Call Routing on page 205.

This topic includes:

Setting up VoIP trunks

You can add one or more VoIP service providers to the FortiVoice unit trunk configuration. The VoIP service providers deliver your telephone services to customers equipped with SIP-based PBX (IP-PBX).

To view the list of VoIP service providers, go to *Trunk > VoIP > SIP.*

GUI field	Description
Test	Select to test if the trunk is created successfully. For more information, see Testing SIP trunks on page 194.
FortiCall	Select to create a SIP trunk with Fortinet's FortiCall service. You can only create one trunk with FortiCall and use it free for 30 days or 300 minutes, whichever comes first. Note that the trial account only allows outbound calling and no international calling is available. If you sign up for the service during a trial, the trial is closed and billing will start. For more information, see Creating a SIP trunk with FortiCall service on page 195.
Enabled	Select to activate this trunk.
Name	The name of the VoIP service provider.
Server	The VoIP provider's domain name or IP address. For example, `172.20.120.11` or `voip.example.com`.
Port	The port for SIP sessions.
SIP Setting	The SIP profile applied to this trunk.
Status	The status of the SIP trunk. • *Not registered*: The trunk is not registered with the VoIP service provider and is not in service.

GUI field	Description
	• *In service*: The trunk is registered with the VoIP service provider and is in service. • *Unavailable*: The trunk is not reachable. • *Alarm detected*: There is a problem with the phone line. • *Admin down*: The trunk is disabled. • *Unmonitored*: The trunk is unknown.

To create a VoIP trunk

1. Go to *Trunk* > *VoIP* > *SIP.*
2. Click *New*.
3. Configure the following:

GUI field		Description
SIP		
	Name	Enter the name of the VoIP service provider.
	Enable	Select to activate the SIP trunk.
	Display name	Enter your caller ID that will appear on the called phone, such as Example Company.
	Main number	Enter the phone number that will appear on the called phone. If you entered the external caller ID in External caller ID on page 174, this trunk phone number will be overridden by the external caller ID.
SIP Setting		
	SIP server	Enter the VoIP provider's IP address or domain name. For example, `172.20.120.11` or `voip.example.com`.
	SIP port	Most SIP configurations use TCP or UDP port 5060 for SIP sessions. If your VoIP service provider uses a different port for SIP sessions, enter the port number. If you select the *Using DNS record* option, this field is greyed out.
	Using SRV record	If you entered the VoIP provider's domain name in the *SIP server* field, select this option to translate the domain name and obtain the SIP port. You can only select this option if your VoIP provider uses the same setting.
	User name	Enter the user name provided by the VoIP service provider for the FortiVoice unit to register with the SIP server.
	Password	Enter the password provided by the VoIP service provider for the FortiVoice unit to register with the SIP server.

GUI field		Description
	Auth. user name	Some VoIP providers may provide you with an authentication user name that is different from your user name for the FortiVoice unit to register with the SIP server. If tat is the case, enter the authentication user name here.
	Realm/Domain	Some VoIP service providers' SIP servers authenticate the PBXes that register with them by requesting the name of the host performing the authentication. If this is the case with your VoIP service provider, enter the name of the host performing the authentication provided by your VoIP service provider.
	SIP Setting	Select the SIP profile to apply the supported phone features and codecs for the trunk. To match the information of the VoIP service provider, you can edit the existing profile or click *New* to add a new one. For more information, see Configuring SIP profiles on page 115.
	Max channel	Each trunk contains multiple channels. The number of channels you can have in a trunk is controlled by your VoIP service provider. This number displays under line appearance option when you configure programmable phone keys for phone profiles. See Configuring phone profiles on page 118. Consult your VoIP service provider for the maximum of channels that you can set to limit the number of concurrent calls. For example, if you want to allow six calls at a time, enter 6. This field accepts value in the range of 1-450 inclusive.
	Overflow check	If selected, the phone calls exceeding the *Max channel* limit will be handled according to the call handling actions set in the dialplan applied to this trunk. For information on dialplans, see Configuring Call Routing on page 205. If unselected, the phone calls exceeding the *Max channel* limit will be disconnected.
	Max outgoing channel	With known max channels, if you need to reserve incoming channels, you may enter the number of outgoing channels allowed and the remaining channels are for incoming calls. For example, the max channel number is 10 and you want to reserve 4 channels for incoming calls, you can enter 6 for *Max outgoing channel*. The maximum channel limit is 2000.
	User=Phone in SIP URI	Select if your service provider requires this option to make the FortiVoice unit to be compatible with the VoIP service provider's configurations.
	Caller ID modification	Select if you want the trunk main number to appear on the called phone. See Main number on page 191. Otherwise, the user name provided by the VoIP service provider for the FortiVoice unit to register with the SIP server will appear on the called phone. See User name on page 191.

GUI field		Description
	Inband ringtone	Select to enable the FortiVoice unit to send ring tone to the caller of an incoming call before the establishment of a call connection. This option is only editable if you enable early media in Advanced Setting on page 90.

	Registration	Enter the SIP registration information from the VoIP service provider by selecting a registration method in *Type* field. You can receive calls after registering with the SIP server of the VoIP service provider.
		• *Disable*: Select to deactivate the registration with the VoIP service provider.
		• *Standard*: Select to use the standard registration method which automatically registers with the SIP server of the VoIP service provider. Enter the registration interval in minutes.
		• *Registration URI*: Enter the registration string provided by the VoIP service provider in the *Registration URI* field.
		The string usually has the following formats:
		`register => user[:secret[:authuser]]@host [:port][/extension]`
		or
		`register => fromuser@fromdomain:secret@host`
		or
		`register => fromuser@fromdomain:secret: authuser@host:port/extension`
		For example, a string could be: `register => 2345:password@mysipprovider.com/1234`
		• *Registrar*: Select to enter the registration information from the VoIP service provider:
		  • *Registrar host/IP*: Enter the VoIP service provider's SIP registration server domain name or IP address. For example, `172.20.120.11` or `voip.example.com.`
		  • *Registrar port:* Most SIP configurations use TCP or UDP port 5060 for SIP sessions. If your VoIP service provider uses a different port for SIP sessions, enter the port number.
		  • *Transport protocol*: Select the transport protocol used for the registration.
		  • *Registration interval*: Enter the registration interval with the SIP server in minutes.

	Outbound Proxy	Some VoIP service providers use proxy servers to direct its traffic. If this is the case, your registration request will go to the proxy server first before reaching the registration server. Configure the following:

GUI field		Description
		• Select to activate the proxy server Setting. • *Proxy (Host/IP)*: Enter the proxy server's domain name or IP address. For example, `172.20.120.11` or `voip.example.com`. • *Proxy port*: Enter the port number of the proxy server. • *Transport protocol*: Select the transport protocol used for the registration.
Fax		Configure fax signal automatic detection and fax handling.
	Automatic fax detection	Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically. Selecting this option may delay the call response time on this trunk.
	Forward fax to eFax account	Some incoming faxes' numbers do not match those of your eFax accounts. Selecting this option and a fax receiving account will send the faxes to the fax account. See Forward tax to eFax account on page 197. This option is only selectable if *Automatic fax detection* is selected.
Phone Number		Click *New* to add the phone number provided by your VoIP service provider. The VoIP service provider SIP server will direct calls from external callers directly to this number. You can add multiple numbers.

4. Click *Create*.

Testing SIP trunks

After you create a SIP trunk, you can select the trunk and click *Test* to see if the trunk works.

For more information, see Test on page 190.

To test a SIP trunk

1. Go to *Trunk > VoIP > SIP.*
2. Select the trunk that you want to test and click *Test*.
3. Select *Test Call-Dry Run* or *Test Call*.
   The *System Configuration Test* page appears.
4. Configure the following:

GUI field		Description
Test Call - Dry Run		Run a system SIP trunk test without making a real phone call.
	Destination number	Enter a destination number to call.

GUI field		Description
	From number	Enter the number from which you want to call the destination number. The FortiVoice unit will connect this number with the destination number for the test.
	Test	Click to start the dry run test and check the *Test result*.
	Reset	Click to remove the test result in order to start a new test.
Test Call		Test the SIP trunk by making a real phone call.
	Destination number	Enter a destination number to call.
	After call is established	Select the FortiVoice action once it calls the destination number: • *Play welcome message*: The FortiVoice unit will play a message to the destination number. • *Connect test call to number*: In the *Number* field, enter the number from which you want to call the destination number. The FortiVoice unit will connect this number with the destination number to test the trunk.
	Test	Click to start the test and check the *Test result*.
	Reset	Click to remove the test result in order to start a new test.

Creating a SIP trunk with FortiCall service

You can create one trunk with FortiCall and use it free for 30 days or 300 minutes, whichever comes first. Note that the trial account only allows outbound calling and no international calling is available.

If you sign up for the service during a trial use, the trial is closed and billing will start.

To create a SIP trunk with FortiCall service

1. Go to *Trunk > VoIP > SIP.*
2. Click *FortiCall*.
   The *Create SIP Trunk* dialog box displays.
3. Note down the *MAC Address* and *System ID* for use if you decide to sign up for the service later.
4. Keep *Create dialplans for this trunk* selected unless you want to create the dialplans by yourself.
   The auto-generated dialplans will replace the default inbound, outbound, and emergency call dialplans. You can delete them if you do not choose to use the FortiCall service.
5. Click *OK*.
6. For *Fax*, see Fax on page 194.
7. For *Register Trial Account*, enter your name, email address, and reseller or partner code.
8. Click *Create*.
9. Click *OK*.
   The FortiCall trunk is created. You will receive an email with sign up and login instructions.

Modifying PSTN/PRI trunks

This section applies to the following models only:

- FVE 200D-T
- FVE 300E-T
- FVE 500E-T2
- FVE 1000E-T
- FVE 2000E-T2

PSTN (Public Switched Telephone Network)/PRI (Primary Rate Interface) trunks connect your PBX or VoIP network to your PSTN service providers and through them to the outside world. These trunks can be analog or digital phone lines.

You can modify the default trunks or create new ones.

To view the PSTN trunks, go to *Trunk > PRI > PRI.*

GUI field	Description
Enabled	Select to activate the trunk.
Name	The name of the trunk.
Status	The trunk statuses, including: • *In service:* The trunk is currently in use. • *Not activated:* The trunk is not enabled. • *Idle*: The trunk is not in use. • *Unavailable*: The trunk is not reachable. • *Conflict*: The trunk conflicts with another one. • *Alarm detected*: There is a problem with the trunk. • *Admin down*: The trunk is disabled.
Type	The trunk type: digital or analog.

To add a T1/E1 voice circuit trunk

1. Go to *Trunks > PRI > PRI.*
2. Click *New*.

3. Configure the following:

GUI field		Description
Trunk Setting		
	Name	The name of this trunk. This is view only.
	Enable	Select to activate the trunk.
	Display name	Enter your caller ID that will appear on the called phone, such as Example Company.
	Number	Enter the phone number that will appear on the called phone. If you entered the external caller ID in External caller ID on page 174, this trunk phone number will be overridden by the external caller ID.
	Relay fax	Select to allow T.38 fax relay on the trunk. Enter the fax number.
Hardware Property		Use this option to configure the T1/E1 span. Spans represent trunks (spans) of T1/E1 PSTN lines. The FortiVoice unit supports T1/E1 lines according to the installed voice card. You can add a span name using the CLI. In *Edit span*, click Edit after selecting a span to configure the Setting of the T1/E1 span to match the same Setting of your PSTN service provider. Click *OK* after finishing the configuration. For more information, see Configuring the T1/E1 span on page 198. In *Span*, select the span for the trunk and move it to the *Selected* field.
	Max channel	Indicates the total number of B channels on all spans.
	Max outgoing channel	Enter the number of outgoing channels out of the maximum number of B channels.
Fax		Configure fax and phone signal automatic detection and fax handling.
	Automatic fax detection	Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically.
	Forward tax to eFax account	Select the fax receiving account for the detected faxes.
Phone Number		Click *New* to add the phone number provided by your PSTN service provider. This is your DID number. Your PSTN service provider will direct calls from external callers directly to this number. You can add multiple numbers, including numbers from full or fractional PRI (T1/E1).

4. Click *OK*.

To add an analog CO trunk for 200D-T

1. Go to *Trunks > Analog > Analog.*

2. Click *New*.

3. Configure the following:

GUI field		Description
Analog Setting		
	Name	Enter a name for this trunk.
	Enabled	Select to activate the trunk.
	Display name	Enter your caller ID that will appear on the called phone, such as Example Company.
	Number	Enter the phone number that will appear on the called phone. If you entered the external caller ID in External caller ID on page 174, this trunk phone number will be overridden by the external caller ID.
Hardware Property		
	analog1	Use this option to configure the analog trunk. Click *Edit* to configure the PSTN analog Setting to match the same Setting of your PSTN service provider. Click *OK* after finishing the configuration. For more information, see Configuring the analog voice trunk on page 201.
	Port	Select the FXO ports you want for this trunk and click -> to move them into the *Selected ports* field. Each FXO port provides an analog phone line for a FXO device, such as a phone or fax.
	Max channel	Indicates the total number of channels on the trunk.
	Max outgoing channel	Enter the number of outgoing channels out of the maximum number of channels on the trunk.
Fax		Configure fax and phone signal automatic detection and fax handling.
	Automatic fax detection	Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically.
	eFax account	Select the fax receiving account for the detected faxes.
Phone Number		Click *New* to add the phone number provided by your PSTN service provider. Your PSTN service provider will direct calls from external callers directly to this number. You can add multiple numbers.

4. Click *Create*.

Configuring the T1/E1 span

You can configure the Setting of the T1/E1 span, including full or fractional PRI (T1/E1), to match the same Setting of your PSTN service provider.

For 2000E-T2, if a PRI trunk includes two spans, the configuration of the second span is much simpler as the spans share many configurations.

For more information, see Hardware Property on page 197.

To configure the T1/E1 span

1. On the *PRI* page, click Edit after selecting a span name under *Hardware Property*.
2. Configure the following:

GUI field		Description
Standard Options		
	Name	The name of this span. This is view-only.
	Type	Select the span type: *PRI T1* or *PRI E1*. A T1 span usually supports 23+1 channels, while an E1 span supports 30 channels in CAS (Channel Associate Signaling) mode and 30 B channels and one D channel in ISDN mode.
	Signalling	Select the signaling type of the ISDN PRI: • *PRI signalling, CPE* (Customer Premises Equipment) *side* • *PRI signalling, Network Side* • *PRI R2 signalling*
Advanced Options		
	Framing and coding option	Specify the type of framing and coding to provision the PRI with your PSTN service provider.
	Clocking options	Select the FortiVoice unit's clock synchronization: • Clock sourcing from PSTN network • Internal clocking source This option does not need to match that of your PSTN service provider.
	Receive sensitivity	Select the level of receiver sensitivity which is the ability of the phone receiver to pick up the required level of phone signals to make it operate more effectively within its application. This option does not need to match that of your PSTN service provider.
	D-channel signalling format	Select a signalling method for the D channel which is a signalling channel and carries the information needed to connect or disconnect calls and to negotiate special calling parameters (for example, automatic number ID, call waiting, data protocol). The D channel can also carry packet-switched data using the X.25 protocol. If you choose *Lucent 5ESS,* the facility service for sending the display name is enabled automatically.

GUI field		Description
	Line build out	Select the line build out (LBO). LBO Setting are an inherent part of T1 and T3 network element transmission circuitry. Since cable lengths between network elements and digital signal cross-connect (DSX) vary in the central office, LBO Setting are used to adjust the output power of the transmission signal to achieve equal level point (ELP) at the DSX.
	D-channel	By default, depending on your selection of Type on page 199, the typical channel numbers are: • Full T1: 24 • Full E1: 16 You can also set the channel numbers to others such as 1. The Setting you configure must match the same Setting of your PSTN service provider.
	B-channel	By default, depending on your selection of Type on page 199, the typical channel Setting are: • Full T1: 1-23 • Full E1: 1-15, 17-31 You can also configure the fractional channel numbers. For example, for T1/E1, the channels can be: • 1-12 • 2, 3, 4, 9-15 • 2-4, 9-15 The Setting you configure must match the same Setting of your PSTN service provider.
PRI R2 Setting		Since there is no single signaling standard for R2, the FortiVoice unit addresses this challenge by supporting many localized implementations of R2 signaling. This option is active only if you select PRI R2 signalling for Signalling on page 199.
	Country	Select the country for PRI R2 Setting.
	Max ANI digits	ANI (Automatic Number Identification) is a system used by telephone companies to identify the DN (Directory Number) of a calling subscriber. It allows subscribers to capture or display caller’s telephone number. Enter the number of digits of a caller‘s phone number to be captured.
	Max DNIS digits	Dialed Number Identification Service (DNIS) is a service provided by telephone companies that lets the subscribers determine which telephone number was dialed by a caller.

GUI field		Description
		Enter the number of digits of a dialed call to be sent by the telephone company.
	Caller category	Select the caller type.
	Incoming digits mode	Select the incoming digits mode by consulting your telephone company.
	DTMF option	• *DTMF dialing*: Select to enable dual-tone multi-frequency signaling (DTMF) dialing. • *DTMF answering*: Select to enable dual-tone multi-frequency signaling (DTMF) answering.
	Allow collect calls	Select to allow collect calls.

3. Click *OK*.

Configuring the analog voice trunk

You can configure the Setting of the analog CO trunk to match the same Setting of your PSTN service provider except the TX/RX gain Setting.

For more information, see Hardware Property on page 197.

To configure the analog CO trunk

1. On the *Analog* page, click *Edit* under *Hardware Property*.
2. Configure the following:

GUI field		Description
PSTN Analog Setting		
	Name	The name of this configuration. This is view-only.
	Codec	Select the Codec for the trunk.
	Caller ID signalling	Select the caller ID signalling standard per your phone company's request.

3. Click *OK*.

Configuring office peers

If you have remote offices equipped with VoIP network, you can set up office peer trunks so that offices can call each other as if they are local extensions.

For the office peers to call each other, make sure that your FortiVoice unit and the peer office PBX are mutually registered with each other's IP address and SIP port number.

To view the list of office peer trunks, go to *Trunk > Office Peer > Office Peer.*

GUI field	Description
Fetch Office Directory	Select a trunk and click this button to obtain the phone directory from this office peer. This option only works if the PBX of the remote office is a FortiVoice unit and *Fetch directory* (see Directory on page 203) is selected on the remote unit. You can view the directory by going to *Monitor > Directory* and selecting this office in the *Locations* field. For more information, see Viewing call directory on page 35.
Enabled	Select to activate this trunk.
Name	The name of the office peer.
Display name	Enter the name displaying on the extension.
Type	The type of the trunk.
Server	The domain name or IP address of the remote office's PBX. For example, `172.20.120.11 or peer.example.com`.
Port	The port number for VoIP network on the remote office's PBX.
SIP Setting	The SIP profile applied to this trunk.
Status	The status of the SIP trunk. • *Not registered*: The trunk is not registered with the VoIP service provider and is not in service. • *In service*: The trunk is registered with the VoIP service provider and is in service. • *Unavailable*: The trunk is not reachable. • *Alarm detected*: There is a problem with the phone line. • *Admin down*: The trunk is disabled. • *Unmonitored*: The trunk is unknown.

To set up a site to site office peer

1. Go to *Trunk > Office Peer > Office Peer.*
2. Click *New*.
3. Under *Office peer type*, click *Site to Site*.
4. If you want to change your local number pattern, click the *Edit* icon beside*Local/incoming digit pattern*to modify it.
5. Review the basic *New office peer information*, click *Next*.
6. Configure the following:

GUI field	Description
Name	Enter a name for the trunk.

GUI field			Description
	Display name		Enter the name displaying on the extension.
	Enable		Select to activate the trunk.
Peer Configuration			
	Remote Host/IP		Enter the domain name or IP address of the remote office's PBX.
	Port		Enter the port number for VoIP network on the remote office's PBX.
	Authentication		Optionally, you may configure to authenticate the peers.
		Disable	If you do not need authentication for the office peer, select this option to disable it.
		Symmetric	If you want to authenticate the PBXes forming the office peer trunk., enter the *User name* and *Password*. These Setting must be the same on both PBXes. The PBX on each end will use the Setting to authenticate each other.
		Asymmetric	If you want to authenticate incoming and outgoing calls, enter the *Inbound user name, Outbound user name*, and *Password*. These Setting must be the same on both PBXes forming the office peer trunk. The PBX on each end will use the Setting to authenticate incoming and outgoing calls.
	Outgoing digit pattern		Click the *Edit* icon if you want to modify the digit pattern of the outgoing dial plan for the local and peer offices.
	Advanced		
		Local/incoming digit pattern	Click the *Edit* icon if you want to modify digit pattern of the local/incoming dial plan for the local and peer offices.
		Call routing	Select the call routing plan as required.
		Directory	Select this option and click *Fetch now* to obtain the phone directory from this office peer. This option only works if the PBX of the remote office is a FortiVoice unit and the same option is selected on the remote unit. You can view the directory by going to *Monitor > Directory* and selecting this office in the *Office* field. For more information, see Viewing call directory on page 35.
		Share metric	Enter the hop count value for this FortiVoice unit to share phone directory with a peer office. For example, if you enter 1, the directory can only be shared with the first peer office site designated on the routing table of this FortiVoice unit.

GUI field	Description
SIP Setting	Select the SIP profile for the trunk. You can edit the existing profile or click *New* to add a new one. For more information, see Configuring SIP profiles on page 115.
Max channel	Enter the maximum voice channels for the trunk. This field accepts value in the range of 1-450 inclusive.

7. Click *Create*.
After setting up the peer office, create outgoing and incoming dial plans for the local and peer offices. For more information, see Configuring Call Routing on page 205.

Setting up routing rules for FXO and PRI gateways

Once you create FXO or PRI gateways under *Managed System*, go to *Trunks* and refresh your browser, *Gateways* appears listing all of the FXO or PRI gateways that have been added to the system. You can enable or disable the gateway profiles as well as edit and delete profiles from the system. Any gateway added will have a profile automatically created.

For information on adding gateways, see Managing FXO gateways on page 137 and Managing PRI gateways on page 143.

For information on adding FXO or PRI gateway trunks, see Creating multiple trunk gateways on page 138 and Creating multiple trunk gateways on page 144.

Configuring Call Routing

Dial plans define how calls flow into and out of the FortiVoice unit. Without dial plans, telephone communications among PBXs are impossible.

This topic includes:

- Configuring inbound dial plans on page 205
- Configuring direct inward dialing on page 208
- Viewing office peers for inbound calls on page 210
- Configuring outbound dial plans on page 211
- Viewing office peers for outbound calls on page 215

Configuring inbound dial plans

The *Call Routing* > *Inbound* > *Inbound* submenu lets you configure dial plans for incoming calls to the FortiVoice unit.

When the FortiVoice unit receives a call, the call is processed according to the inbound dial plan. To process the call, the FortiVoice unit selects the dial plan rule that best matches the dialed number and processes the call using the Setting in the dial plan rule. For example, if your main line is 123-4567, you can set a dial plan rule that sends all incoming calls dialing 123-4567 to the auto attendant. Once the auto attendant is reached, the callers can follow the instructions, for instance, to dial an extension.

To view the inbound dial plans, go to *Call Routing* > *Inbound* > *Inbound.*

GUI field	Description
Enabled	Select to activate this dial plan.
Name	The name of the dial plan.
Call handling	The actions to process the incoming calls with matched dialed numbers and/or caller IDs. For details, see Call Handling on page 206.
Handling Description	The specific call handling actions. For details, see New on page 207.
From Trunk	The trunks of the incoming calls that are subject to this dial plan.
Match DID	The phone number pattern in your dial plan that matches many different numbers. For details, see Dialed Number Match on page 206.
Match CID	The caller ID pattern for this dial plan. For details, see Caller ID Match on page 206.

To set up an inbound dial plan

1. Go to *Call Routing* > *Inbound* > *Inbound.*
2. Click *New*.

3. Configure the following:

GUI field		Description
Name		Enter a name for this plan.
Enable		Select to activate this dial plan.
From Trunk		Select the trunks of the incoming calls that are subject to this dial plan. Select the trunks in the *Available* field and click -> to move them into the *Selected* field.
Dialed Number Match		With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers. The called numbers matching this pattern will follow this dial plan rule. Create the number match following Pattern-matching syntax on page 213 and Pattern-matching examples on page 213.
Caller ID Match		Click *New* to set the caller ID pattern following Pattern-matching syntax on page 213 and Pattern-matching examples on page 213 for this dial plan, and click *Create*. You can enter an incoming call's display name string or the caller's phone number string as the pattern. Click *Export* to open or save the caller ID match file and *Import* to browse for a caller ID match file. Caller IDs under this pattern are subject to this plan.
Caller ID Modification		Select one or more caller ID modification configurations. You can associate multiple caller ID modification configurations with a dial plan. For more information on caller ID modification, see Modifying caller IDs on page 116.
Call Handling		Select the actions to process the incoming calls with matched dialed numbers and/or caller IDs.
	Action type	Select the type of action for the plan and configure the actions accordingly. See New on page 207. • *Endpoint Action*: Select if you want to send incoming calls to the local destinations according to operation schedules. For example, send calls to the voicemail after business hours. • *Dial Local Number*: Select if you want to send incoming calls to the local destinations at any time. For example, you can enter 222xxxx as a pattern and strip 222. The FortiVoice unit will only dial the last four digits for all called numbers matching the pattern. • *Call Routing*: Select if you want to route incoming calls (to the FortiVoice unit) to an external phone system using an outbound dial plan.

GUI field	Description
New	Depending on the selected *Action type*, click *New* to configure the actions: • If you select the *Endpoint action* type: **a.** Select the FortiVoice operation schedule for the action. Click *Edit* to modify the selected schedule or click *New* to configure a new one. For more information on FortiVoice schedule, see Scheduling the FortiVoice unit on page 131. **b.** Select an action for the incoming calls under this plan. For some actions, you need to enter the extension (such as *Go voicemail*) or select a profile (such as *Play announcement*). **c.** Click *Create*. **d.** Repeat this procedure if you need more actions for this action type. Do not use the same schedule for more than one action to avoid schedule conflict. • If you select the *Dial local number* type: **a.** Click *New* to add the number pattern in the *Match Pattern*field following Pattern-matching syntax on page 213 and Pattern-matching examples on page 213 for this dial plan. Repeat to add more patterns. **b.** For *Strip*, enter a number to omit dialing the starting part of a pattern. 0 means no action. For example, if your Match Pattern is 222XXXX and Strip is 3, the FortiVoice unit will only dial the last four digits for all called numbers matching the pattern. **c.** For Prefix, add a number before a pattern. For example, if your *Match Pattern* is 9XXX and the numbers under this pattern have been upgraded to have an additional digit 5 at the beginning, you can enter 5 for the *Prefix*. When an incoming call matches the pattern, the FortiVoice unit will add a 5 before the number. **d.** For *Postfix*, add a number after a pattern. For example, if your *Match Pattern* is 9XXX and the numbers under this pattern have been upgraded to have an additional digit 5 at the end, you can enter 5 for the *Postfix*. When an incoming call matches the pattern, the FortiVoice unit will add a 5 after the numb **e.** Click *Create*. • If you select the *Call routing* type, select the available outbound dial plans and click -> to move them into the Selected field. This means that the FortiVoice unit will route incoming calls to an external phone system using the selected outbound dial plans. You may also choose to keep the original caller ID.

4. Click *Create*.

Configuring direct inward dialing

The *Call Routing* > *Inbound* > *DID Mapping* submenu lets you configure how to map Direct Inward Dialing (DID) numbers.

Local phone companies offer DID service to provide a block of telephone numbers for calling into a company's PBX system over limited rented physical lines (also called "trunk lines"). The phone numbers you rent may not be enough to provide a DID number for each workstation, because each DID can only be mapped to one extension. With the FortiVoice unit, you have 2 options to address this issue:

- Only map the DID numbers to the extensions you want.
- Map a DID number to one or more extensions based on the callers' phone numbers.

For more information, see Mapping DIDs on page 209.

To configure a DID

1. Go to *Call Routing* > *Inbound* > *DID Mapping.*
2. Click *New*.
3. Configure the following:

GUI field		Description
Rule name		Enter a name for this DID setting.
Enable		Select to activate this DID setting.
Trunk		Select the trunk used for dialing the DIDs.
Schedule		Select a schedule to apply the rule. For information on creating schedules, see Scheduling the FortiVoice unit on page 131.
Caller ID Match		Click *New* to set the caller ID pattern following Pattern-matching syntax on page 213 and Pattern-matching examples on page 213 for this dial plan, and click *Create*. You can enter an incoming call's display name string or the caller's phone number string as the pattern. Click *Export* to open or save the caller ID match file and *Import* to browse for a caller ID match file. Caller IDs under this pattern are subject to this plan.
Inbound Handling		
	Inbound caller ID modification	Select the caller ID modification configuration. For more information on caller ID modification, see Modifying caller IDs on page 116.
	Inbound fallback action	Select the action to take if a caller not in the caller list dialed the DID number mapped to an extension. For some actions, you need to enter the extension, such as *Dial voicemail*.

GUI field	Description
	For information on filtering callers, see Mapping DIDs on page 209.
Number Mapping	For adding a number mapping, see Mapping DIDs on page 209. Click *Export* to open or save the number mapping file and *Import* to browse for a number mapping file.

Mapping DIDs

You can map a DID number to one extension. You can also map a DID to multiple extensions based on the callers' phone numbers. For example, calling numbers 123-4567, 123-4568, and 123-4569 can call the DID number 222-1000 to reach extension 1234. Calling numbers 234-4567, 234-4568, and 234-4569 can call the same DID number 222-1000 to reach extension 1265. In both cases, the calling numbers will display on the extension.

If a caller outside the configured caller list dialed the mapped DID number, the FortiVoice unit will react according to the selected fall back action. For details, see Inbound fallback action on page 208.

To map DIDs

1. Go to *Call Routing* > *Inbound* > *DID Mapping.*
2. Click *New*.
3. In *Number Mapping*, click *New*.

4. Configure the following:

GUI field	Description
DID number	Enter the DID number that you want to map to an extension. The DID number cannot be mapped to more than one extension unless the DID is bundled with a caller number. Otherwise, an error message about duplicate entry appears and the DID mapping configuration cannot be saved.
Extension	Enter the extension that you want to map to the DID number.
Description	Enter any notes you have for the mapping.
Option	Select *Inbound* to direct incoming calls to the extension through the mapped DID. If this option is not selected, incoming calls to this extension through the mapped DID will follow the inbound fallback action configured in Inbound fallback action on page 208. By default, this option is selected. Select *Outbound* to send the DID numbers of the extensions mapped to the DID with outgoing calls so that the DID numbers can display on the called phones. If this option is not selected, the extension's DID number is not sent with outgoing calls and the phone number displayed on the called phone could be the FortiVoice main number (see Main number on page 103) or the trunk phone number (see Phone Number on page 194) associated with the extension. Alternatively, you can choose the caller ID to display on the called phone when configuring an extension. By default, both *Inbound* and *Outbound* are selected.
Caller Number Patterns	This option allows you to bundle caller number patterns to a DID number which can be mapped to any extension. Enter the caller's phone pattern field and click *Create*. Click the + icon to add more calling numbers patterns. Only the caller numbers matching the patterns you set will reach the mapped extension when they dial the DID number. For information on phone number patterns, see Pattern-matching syntax on page 213 and Pattern-matching examples on page 213.

5. Click *Create*.

Viewing office peers for inbound calls

The *Call Routing* > *Inbound* > *Office Peers* submenu lets you view the office peers involved in the inbound call routing. You may click an office peer link to configure it. For details, see Configuring office peers on page 201.

Configuring outbound dial plans

The *Call Routing* > *Outbound* > *Outbound* submenu lets you configure dial plans for outgoing calls from the FortiVoice unit.

You can configure dial plans on the FortiVoice unit to route calls made from a FortiVoice extension to an external phone system. The external phone system can be one or more PSTN lines or a VoIP service provider. To route calls to an external phone system, you add dial plan rules that define the extra digits that extension users must dial to call out of the FortiVoice unit. The rules also control how the FortiVoice unit handles these calls including whether to block or allow the call, the destinations the calls are routed to and whether to add digits to the beginning of the dialed number.

For example, if users should be able to dial 911 for emergencies, you should include a dial plan rule that sends all calls that begin with 911 to an external phone system. This rule should also override the default outgoing prefix so that users can dial 911 without having to dial 9 first.

To view the outbound dial plans, go to *Call Routing* > *Outbound* > *Outbound.*

GUI field	Description
Test	Select to test if the dial plan is created successfully. For more information, see Testing outbound dial plans on page 212.
Enabled	Select to activate this dial plan.
Name	The name of the dial plan.
Pattern	The phone number pattern in the dial plan that matches other numbers. For details, see Dialed Number Match on page 212.
Match CID	The caller ID pattern for this dial plan. For details, see Caller ID Match on page 212.
Call handling	The call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern. For details, see Call Handling on page 212.

To set up an outbound dial plan

1. Go to *Call Routing* > *Outbound* > *Outbound.*
2. Click *New*.

3. Configure the following:

GUI field	Description
Name	Enter a name for this plan.
Enable	Select to activate this dial plan.
Emergency call	Select to allow emergency call with this plan. By default, this is selected. For information on setting emergency number, see Setting PBX location and contact information on page 102.
Caller ID Match	Click *New* to set the caller ID pattern following Pattern-matching syntax on page 213 and Pattern-matching examples on page 213 for this dial plan, and click *Create*. You can enter a caller's display name string or the caller's phone number string as the pattern. Callers with IDs under this pattern are subject to this plan.
Dialed Number Match	With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers. The dialed numbers matching this pattern will follow this dial plan rule. For information on adding a dialed number match, see Creating dialed number match on page 213.
Call Handling	Click *New* to configure the call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern. For details, see Configuring call handling actions on page 214.

4. Click *Create*.

Testing outbound dial plans

After you create a dial plan, you can select the dial plan and click *Test* to see if the dial plan works.

For more information, see Test on page 211.

To test an outbound dial plan

1. Go to *Call Routing* > *Outbound* > *Outbound.*
2. Select the dial plan that you want to test and click *Test*.
3. Select *Test Call-Dry Run* or *Test Call*.
4. The call test page appears.
5. Configure the following:

GUI field		Description
Test Call - Dry Run		Run a system outbound dial plan test without making a real phone call.
	Destination number	Enter a destination number to call.

GUI field		Description
	From number	Enter the number from which you want to call the destination number. The FortiVoice unit will connect this number with the destination number for the test.
	Test	Click to start the dry run test and view the *Test result*.
	Reset	Click to remove the test result in order to start a new test.
Test Call		Test the outbound dial plan by making a real phone call.
	Destination number	Enter a destination number to call.
	After call is established	Select the FortiVoice action once it calls the destination number: • *Play welcome message*: The FortiVoice unit will play a message to the destination number. • *Connect test call to number*: In the *Number* field, enter the number from which you want to call the destination number. The FortiVoice unit will connect this number with the destination number to test the trunk.
	Test	Click to start the test and view the *Test result*.
	Reset	Click to remove the test result in order to start a new test.

Creating dialed number match

You can create one extension number pattern in your dial plan that matches many different numbers for outbound calls.

The numbers matching this pattern will follow this dial plan rule.

The FortiVoice unit supports the following pattern-matching syntax:

Pattern-matching syntax

Syntax	Description
X	Matches any single digit from 0 to 9.
Z	Matches any single digit from 1 to 9.
N	Matches any single digit from 2 to 9.
[15-7]	Matches a single character from the range of digits specified. In this case, the pattern matches a single 1, as well as any number in the range 5, 6, 7.
.	Wildcard match; matches one or more characters, no matter what they are.
!	Wildcard match; matches zero or more characters, no matter what they are.

Pattern-matching examples

Pattern	Description
NXXXXXX	Matches any seven-digit number, as long as the first digit is 2 or higher.

Pattern	Description
NXXNXXXXXX	This pattern matches with areas with 10-digit dialing.
1NXXNXXXXXX	Matches the number 1, followed by an area code between 200 and 999, then any seven-digit number. In the North American Numbering Plan calling area, you can use this pattern to match any long-distance number.
011.	Matches any number that starts with 011 and has at least one more digit.

To create a dialed number match

1. Go to *Call Routing* > *Outbound* > *Outbound.*
2. Click *New*.
3. In *Dialed Number Match*, click *New*.
4. Configure the following:

GUI field		Description
Match Pattern		Enter the number pattern following Pattern-matching syntax on page 213 and Pattern-matching examples on page 213 for this dial plan. Click the + icon to add more patterns.
Modification		You can manipulate the number patterns you entered.
	Strip	Enter a number to omit dialing the starting part of a pattern. 0 means no action. For example, if your *Match Pattern* is 9XXX and *Strip* is 1, you need to dial the full digit 9XXX, but the first digit, in this case 9, will be stripped by the system.
	Prefix	Add a number before a pattern, such as area code. For example, if your *Match Pattern* is 123XXXX and its area code is 555, you can enter 555 for the *Prefix*. When you dial a number under this pattern, you do not need to dial the area code 555.
	Postfix	Add a number after a pattern. The following characters are also acceptable: • comma (,) • semicolon (;) • number sign (#) For example, if your *Match Pattern* is 9XXX and the numbers under this pattern have been upgraded to have an additional digit 5 at the end, you can enter 5 for the *Postfix*. When you dial a number under this pattern, you do not need to dial the last digit 5.

5. Click *Create*.

Configuring call handling actions

Configure the call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern.

To configure the call handling action

1. Go to *Call Routing* > *Outbound* > *Outbound.*
2. Click *New*.
3. In *Call Handling*, click *New*.
4. Configure the following:

GUI field		Description
Call Handling		
	Schedule	Select the FortiVoice operation schedule to implement this plan. Click *Edit* to modify the selected schedule or click *New* to configure a new one. For more information on PBX schedule, see Scheduling the FortiVoice unit on page 131.
	Action	Select the call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern.
	Outgoing trunk	Select the trunk for the outbound calls. Click *Edit* to modify the selected trunk or click *New* to configure a new one. For more information on trunks, see Configuring Trunks on page 190.
	Caller ID modification	Select the caller ID modification configuration. Click *Edit* to modify the selected configuration or click *New* to configure a new one. For more information on caller ID modification, see Modifying caller IDs on page 116.
	Warning message	If you select *Allow with warning* or *Deny with warning* in the *Action* field, select the sound file for the warning. Click *Edit* to modify the selected file or click *New* to configure a new one. For more information on sound files, see Managing phone audio settings on page 110.
	Delay	Optionally, if you want to discourage certain users for making outbound calls, enter the call delay time in seconds.

5. Click *Create*.

Viewing office peers for outbound calls

The *Call Routing* > *Outbound* > *Office Peers* submenu lets you view the office peer involved in the outbound call routing. You may click an office peer link to configure it. For details, see Configuring office peers on page 201.

Setting up a Call Center

A call center allows an organization to receive or transmit a large volume of requests by telephone in a centralized office.

You can configure a call center and operate the center on the user web portal.

This option is only available if you have purchased a call center license.

This topic includes:

- Creating call queues and queue groups on page 216
- Configuring agents on page 225
- Configuring IVRs on page 225
- Configuring surveys on page 232
- Setting up monitor view on page 233
- Configuring other agent information on page 235
- Configuring agent profiles on page 236
- Working with call queue statistics on page 238
- Configuring report profiles and generating reports on page 283

Creating call queues and queue groups

Call queuing, or Automatic Call Distribution (ACD), enables the FortiVoice unit to queue up multiple incoming calls and aggregate them into a holding pattern. Each call is assigned a rank that determines the order for it to be delivered to an available agent (typically, first in first out). The highest-ranked caller in the queue is delivered to an available agent first, and every remaining caller moves up a rank.

With call queuing, callers do not need to dial back repeatedly trying to reach someone, and organizations are able to temporarily deal with situations when callers outnumber agents.

This topic includes:

- Creating call queues on page 216
- Creating queue groups on page 224

Creating call queues

Configure a call queue and add it in an inbound dial plan as a call handling action to make it effective. For more information, see Configuring inbound dial plans on page 205.

Call queues consist of:

- Incoming calls waiting in the queue
- Agents who answer the calls in the queues
- A plan for how to handle the queue and assign calls to agents

- Music played while waiting in the queue
- Announcements for agents and callers

Depending on their privileges, agents can log into a queue to answer calls or transfer calls to another queue, which can then be answered by another available agent.

Agents can be static or dynamic. Static agents are always connected to the queues, and dynamic agents need to log into the queue in order to process calls.

To create a call queue

1. Go to *Call Center > Call Queue > Call Queue.*
2. Click *New* and configure the following:

GUI field		Description
Queue ID		Enter an ID for the queue.
Number		Enter an extension for callers to dial and enter into a call queue following the extension number pattern. See Configuring PBX options on page 103. This is another way to use a call queue configuration in addition to adding it in an inbound dial plan as a call handling action. In this case, the dial plan ignores this extension and still uses the extension to which it is applied for call queue action.
Status		Select to enable the call queue.
Display name		Enter the queue name displaying on the queue extension, such as Support.
Description		Enter any notes about this queue.
Department		Select the department to which the queue belongs. For information on creating departments, see Creating extension departments on page 180.
Queue Setting		
	Maximum queue capacity	Enter the maximum number of callers for the call queue. When the call queue is full, other callers will be dealt with according to the *Queue Overflow* call handling action you set in Queue Overflow on page 223. The maximum is 100.
	Maximum queuing time	Enter the maximum call queue waiting time in minutes. When the call waiting time is due, the callers in the queue will be dealt with according to the call handling action you set in Queue Timeout on page 223. The maximum is 720 minutes.
	Ring duration	Enter the time in seconds to ring each agent. If a call is not answered when the ring duration is due, the call is transferred to the next agent. The range is between 5 to 120 seconds.

GUI field		Description
	Music on hold	Select a sound file or music on hold file to play when a caller is waiting. For more information, see Managing phone audio settings on page 110.
Call Distribution		
	Skill Based Routing	Select and choose a call routing option. This option is based on agent skill level scores. For more information, see Creating agent skill levels on page 235. • Lowest level first: The call will ring the agent with the lowest skill level score first and move up the rank if the agent is unable to take the call, that is, the agent's extension is in a Not Ready status. • Highest level first: The call will ring the agent with the highest skill level score first and move down the rank if the agent is unable to take the call, that is, the agent's extension is in a Not Ready status.
	Default skill	This option appears if you select a value other than *Disabled* in the *Skill Based Routing* field. Select the group, such as Billing, Sales, or Support, that the call distribution is executed. You can add a new skill or modify an existing one. For more information, see Adding agent skill sets on page 235.

	Distribution policy	Select a call *Distribution policy*.
		This option works as following:
		• If *Skill Based Routing* is not selected, calls are distributed according to the policy you choose.
		• If *Skill Based Routing* is selected, calls are distributed according to the skill based call routing option you choose. This option only applies to the situation when you have agents with the same skill level in a queue. In such cases, calls are distributed to these agents according to the policy you choose.
		  • *Ring all*: rings all available agents (default).
		  • *Round Robin*: rings all agents in a queue equally in some rational order, usually from the top to the bottom of a list and then starting again at the top of the list and so on.
		  • *Sequential*: rings each agent in a sequential manner regardless of whether they have answered calls.
		  • *Random*: rings an agent at random.
		  • *Least Recent*: rings the agent that least recently received a call.
		  • *Fewest Calls*: rings the agent that has completed the fewest calls in this queue.

GUI field		Description
		• *Weight Random*: rings a random agent, but uses the agent’s number of received calls as a weight. • *Priority Based*: rings agents based on call answering priorities for callers entering the call queue. A new call always starts with the lowest priority. However, a queue manager with privileges can change the priority of a call on the agent console of the user web portal. See Setting caller priorities on page 236.
Additional Setting		
	Distinctive Setting for Agent	*Announce queue name*: Select a sound file that announces the queue name. You can add a new one or modify an existing one. For more information, see Managing phone audio settings on page 110. *Caller ID option*: Select how you want the IDs of the calls to this queue to display. If you select *Prefix*, the queue Display name on page 217 is added before the caller ID on the agent’s phone. If you select *Replace*, the queue Display name on page 217 replaces the caller ID on the agent’s phone. *Ring Pattern*: Select a queue extension ring pattern.
	Business Schedule	In *Available* field, select an operation schedule for the queue and click -> to move it to the Selected field. For example, “business_hour” schedule means agents are only available to answer the calls for this queue during business hours. For information on scheduling, see Scheduling the FortiVoice unit on page 131.

	Announcement to Caller	• *Announce holdtime:* Select if you want to announce the queue waiting time to a caller at the set interval. You may also select to announce only once.
		• *Announce position:* Select to announce a caller’s waiting position in the queue, such as “You are caller No. 5 in the call queue”.
		  ◦ *No*: Do not announce a caller’s position.
		  ◦ *Always*: Always announce a caller’s position.
		  ◦ *Abbreviated*: Announce a caller’s position only once if the caller is over the marked position and always announce once before the caller reaches the marked position.
		  ◦ *Minimal*: Announce only when the caller is within the marked position.
		• *Mark position*: Enter the benchmark for selecting *Abbreviated* or *Minimal* setting under *Announce position*.

GUI field			Description
			For example, if you select *Abbreviated* and enter 5, a caller's position is announced when the caller becomes No. 5 in the queue and announced only once before the caller becomes No. 5 in the queue. • *Announcement interval:* Enter the announcement frequency in seconds. • *Custom announcement*: You can also customize the announcement Setting. If you select *Periodic* or *Random*, enter the announcement frequency in seconds in *Announcement interval*. Also, select a greeting sound file for the announcement. For more information, see Managing phone audio settings on page 110. • *Queue Entry Announcement*: Select *Enable* to announce to callers when they enter a call queue. You can also select to disable this function. Also, select a greeting sound file for the announcement. For more information, see Managing phone audio settings on page 110.
	Service Level		• *Interval:* Enter the time period in minutes for calculating the threshold up to a maximum of 10080 (or one week). • *Threshold:* Enter the call answering rate for a certain period of time. The action triggered by the threshold being reached is configured in Call Handling on page 222. • *Service level low threshold is used in call handling*: Click *Service level low call handling* to configure how other callers will be dealt with according to the *Queue Overflow* call handling action you set in Service Level Low on page 223 when the call queue is full.
	Alert		
		Events	Select the event that triggers an action which is configured in Call Handling on page 222.
		Setting	• *Send alert email:* Select if you want to send an email when an alert event is triggered. Click *New* to enter an email address. • *Call extension/number:* Select this option and an extension number if you want a phone call when an alert event is triggered. Click New to add an extension. • *GUI popup:* Select to have a popup notification on the user web portal GUI when an alert event is triggered. This only applies to agents with the particular privilege called *Queue alert*. See *Agent Console Privilege* in Configuring agent profiles on page 236. • *Alert interval:* Enter a value in minutes during which

GUI field			Description
			time no alert is sent. For example, if you enter 60, you will not receive any alerts for an hour even if an alert event is triggered. This will be the case each time when you receive an alert notification. If you enter 0, you will receive notifications each time when an event is triggered.
	Callback Setting		This option allows callers waiting in a queue to request a callback following the recorded instructions and wait for an agent to return their call.
		Status	Select to enable this option.
		Callback mode	• *Agent call back manually (from call center console):* Select to allow an agent to manually call the caller using the agent console on the user web portal. • *Call Back When Agents Available*: Select to allow the FortiVoice unit to call the caller automatically based on the callback number collected when an agent is available. • *Virtual Placeholder*: Select to allow the FortiVoice unit to hold a caller's previous call waiting position. This happens when a caller does not wish to wait and leaves his/her number following the prompt. When the caller calls back later, the FortiVoice unit checks the caller's number against the ones left and put the caller in his/her previous waiting position is a match is found.
		Prompt voice menu	Select the method to collect the callback number. • *System Default*: Select to use system defined voice file. • *User Defined IVR*: Select to use user configured IVR. For more information on IVR, see Configuring IVRs on page 225.
		Prompt to caller after callback call established	Select to ring the caller when a callback call is set up. Select a greeting sound file for the announcement. For more information, see Managing phone audio settings on page 110.
	Survey Setting		Surveys are used to collect customer feedback to ensure that the service delivered by your call center agents consistently meets corporate standards and drives high customer satisfaction.
		Status	Select to enable this option.
		Survey	Choose the survey configuration for the call queue. For more information on surveys, see Configuring surveys on page 232.
Agent			

GUI field		Description
	Agent type	Select the agent login mode. Once enrolled into the queue, static agents are always connected to the queues while dynamic agents need to log into the queue in order to process calls.
	Auto-logout time	If you select *Dynamic* login mode, enter the agent login expiry time in hours. For example, if you enter 5, the agent will be logged out 5 hours after having logged into the queue.
	Logout all agents after scheduled business hour	If you select *Dynamic* login mode, select to log out all agents in the queue when the scheduled business hour is due.
	Wrap up time	Enter the time (in seconds) needed by agents to complete a queue call including taking notes or record-keeping, starting from the moment that call is hang up. The default is 0 second.
	Wrap up outgoing call	Select if the agent needs to make an outgoing customer call and time to take notes or record-keeping, starting from the moment that call is hang up. You can enter the wrap up time in the Wrap up time on page 222field.
	Call waiting	Select this option so that if an agent is on the phone when a queue call comes in, the caller information will display on the agent's phone. The agent can choose to answer the call or not. If the agent does not answer the call, after the ring duration is due, the call is transferred to the next agent. This option is different from the call waiting feature of a regular extension (See Setting extension user preferences on page 173). On a regular extension, the call waiting feature only applies to the calls that directly go to the extension. On a queue extension, the call waiting feature only applies to the calls that go to the extension from the queue.
	Agent Members	• Click to expand *Agent members* for enrolling agents into the queue. • In the *Available* field, select the agents for this queue. • Click -> to move it into the *Selected* field. • Click *OK*. You can type an agent's extension or name in the *Search* field and press Enter to search for the agent. Note that mobile softclient cannot be assigned to a queue as an agent.
Call Handling		

GUI field		Description
	When no logged-in agent	You may select to queue a caller or not if there is no agents available. If you select *Do not queue*, an incoming call will be handled by your general call handling configuration, such as auto attendant.
	Scheduled Business Hour Call Handling	This option is only available when you edit a call queue. For details, see Configuring scheduled business hour queue call handling actions on page 223.
	Non Scheduled Business Hour Call Handling	This option is only available when you edit a call queue. For details, see Configuring scheduled business hour queue call handling actions on page 223.

3. Click *OK*.

Configuring scheduled business hour queue call handling actions

Configure the call handling action for the queue. This action applies to all calls once they enter into the queue.

This option is only available when you edit a queue.

To configure the call handling action

1. Go to *Call Center > Call Queue > Call Queue.*
2. Select a call queue for which you want to configure queue call handling actions and click *Edit*.
3. In *Call Handling*, click *Scheduled Business Hour Call Handling*.
4. Configure the situation upon which corresponding call process can be configured:

GUI field	Description
Queue Overflow	The situation when callers exceed the maximum waiting callers you set. See Maximum queue capacity on page 217. A popup notification appears when this barometer is triggered.
Queue Timeout	Callers waiting time exceeds the maximum waiting time set in Maximum queuing time on page 217. A popup notification appears when this barometer is triggered.
Service Level Low	Service level represents the maximum amount of time a caller should ideally have to wait before being presented to an agent. You need to set the service-level-calculation-option, service-level-interval, and service-level-threshold in the FortiVoice CLI under `config service call-queue`. For example, if service level interval is set to 60 seconds and the service level percentage is 80 percent, that means 80 percent of the calls that came into the queue were presented to an agent in less than 60 seconds. Any service level percentage lower than 80 is considered to be low.

GUI field	Description
All Agents Logout	There are no agents in the queue to answer calls. The action for this option only works if you select *Queue caller* for When no logged-in agent on page 223.
All Agents Paused	There are no agents in the queue to answer calls. The action for this option only works if you select *Queue caller* for When no logged-in agent on page 223.
Unclassified	Any reason that you need to schedule call handlings.

5. For each situation, click *New* to configure its call handling action.
   - Select the FortiVoice operation schedule to implement this call handling action. For more information on schedules, see Scheduling the FortiVoice unit on page 131.
   - Select the call handling action. Depending on the action selected, further configuration may be needed. For example, if you select *Dial extension* for *Action*, enter the extension to which a call is transferred.
6. Click *Create*, then *OK*.

Configuring non scheduled business hour queue call handling actions

Configure the call handling action for the queue. This action applies to all calls once they enter into the queue.

For some processes that may require further actions, you need to add one or more call processes to complete the call handling. For example, after adding a process that contains a *Set call queue priority* action, you can add another process with a *Transfer to queue* action to complete the call handling. In this case, the call will be processed again with new priority after it is transferred to the queue.

This option is only available when you edit a queue.

To configure the call handling action

1. Go to *Call Center > Call Queue > Call Queue.*
2. Select a call queue for which you want to configure queue call handling actions and click *Edit*.
3. In *Call Handling*, click *Non Scheduled Business Hour Call Handling*.
4. On the *Call Processing* page, click *New* to configure call handling action.
5. For *Schedule*, select the FortiVoice operation schedule to implement this call handling action. For more information on schedules, see Scheduling the FortiVoice unit on page 131.
6. For *Action*, select the call handling action. Depending on the action selected, further configuration may be needed. For example, if you select *Dial extension* for *Action*, enter the extension to which a call is transferred.
7. Click *Create*, then *OK*.

Creating queue groups

You can group queues together to facilitate queue management.

To create a call queue

1. Go to *Call Center > Call Queue > Queue Group.*
2. Click *New*.
3. Enter a name for the group.

4. Select the available call queues that you want to include in the group and click -> to move them into the *Selected* field.
5. Click *Create*.

Configuring agents

Extensions with call center agent function enabled can be further configured with other call center information, such as agent profile, managed departments, and skill sets. Call center user groups can also be set up to form the basis for department and group management.

To configure an agent

1. Go to *Call Center > Agent > Agent.*
   All extensions with call center agent function enabled display. Clicking *Extensions* opens the IP extensions configuration page. For information, see Configuring IP extensions on page 156.
2. Select the extension you want to configure and click *Edit*.
3. Select an agent profile. For more information, see Configuring agent profiles on page 236.
4. For *Managed departments*, select the departments to be managed by this agent if required, and click -> to move it to the *Selected* filed.
5. Click *Member of Queues* to select the call queues to join.
   - *Main/Outgoing queue*: This option is for collecting the outgoing calls from all queues by this agent and displaying them in Working with call queue statistics on page 238. You can select any queue of which this agent is a member for that purpose except *None* which will not collect agent's outgoing call information.
   - *Queues*: Select the queues of which you want the extension/agent to be a member, and click *Apply*.
6. Add skill sets for the agent by clicking *New* under *Skill Sets*.
7. Select the skill set for the agent, including skills and level, and click *Create*. For more information about agent skills and levels, see Adding agent skill sets on page 235 and Creating agent skill levels on page 235.
8. Click *OK*.

To set up a user group

1. Go to *Call Center > Agent > Group.*
2. Click *New*.
3. See Creating user groups on page 180.

Configuring IVRs

FortiVoice Interactive Voice Response (IVR) function allows it to interact with callers through the use of voice and DTMF tones input via keypad. Callers proceed according to the IVR audio instructions to reach the callees or get the information they need.

Based on the information collected from callers and by interacting with the backend database, FortiVoice IVR can prioritize the calls using call queues and present callers' information to the agents.

FortiVoice IVR interfaces with RESTful Web service for querying caller information from the database.

For more information, see *IVR Technical Note*.

This topic includes:

- Setting up an IVR on page 226
- Configuring RESTful service on page 231

Setting up an IVR

Call Center > IVR > IVR allows you to view the existing IVR list and create new IVRs.

Creating new IVRs includes configuring:

- SIP header collector to share IVR information among multiple FortiVoice units based on information gathered by digit and RESTful collectors (see To configure a SIP header collector on page 226)
- the digits collector to collect digit inputs from callers (see To configure a digit collector on page 227)
- the RESTful collector to gather caller information from database (see To configure a RESTful collector on page 228)
- call handling to route the calls based on information gathered by digit and RESTful collectors, and
- error handling to deal with unknown errors and RESTful service errors.

To view the IVR list

1. Go to *Call Center > IVR > IVR.*
2. Click the *Expand all/Collapse all*.
   The IVR tree list displays. Under each IVR name, configuration items are listed. Clicking an item opens its configuration page.

To configure a SIP header collector

1. Go to *Call Center > IVR > IVR* and click the Switch (two opposite arrows) icon.
2. Click *New* and type the name of the IVR and description.
3. Click *Create*.
4. From the IVR name list, select the name you created and click *Edit* to open the IVR configuration page.
5. For *Description*, select *Edit* to enter any notes you have for the IVR.
6. Click *Add SIP Header Collector*.

GUI field	Description
Name	Enter a name for the SIP header collector.
Description	Enter any notes you have for the SIP header collector.
Variable	Click *New* and do the following: **1.** For *Variable*, enter a value for a SIP header field based on your organization’s SIP header definitions, for example, ticket_id. This value must be the same on every FortiVoice unit that shares IVR information. **2.** For *Action on returned data*, do the following: • *None*: Select if you do not want to share the information that the SIP header collector gathers with other interfaces. • *Add to agent console - Display name:* Select if you want agents in the queues where the IVR calls are routed to see the information that the SIP header collector gathers. Enter a name for the information to display on the agent console.

GUI field	Description
	• *Add to SIP header - Field name*: Select if you want to share the information that the SIP header collector gathers with other SIP header collectors. Enter a value that matches the value on the SIP header to enable information sharing. • *Add to remote CDR - Field name*: Select if you want to share the information that the SIP header collector gathers with a remote CDR database. Enter a value that matches the value on the remote CDR to enable information sharing. • test *Add to report - Field name*: Select if you want to share the information that the SIP header collector gathers with survey reports. Enter a value that matches the value on the surveys to enable information sharing. For information on surveys, see Configuring surveys on page 232. **3.** Click *Create.*

7. Click *Create.*
   You can create a maximum of 10 SIP header collectors which are saved as variables.

To configure a digit collector

1. After configuring the SIP header collector, click *Add Digits Collector* to configure digit inputs collection from callers. You can create a maximum of 10 digit collectors.

GUI field	Description
Name	Enter a name for the digit collector.
Prompt	Select the audio file that you want callers to listen to. You can also create a new file or edit the selected one. For more information, see Managing phone audio settings on page 110.
Enable read back	Select if you want the digit inputs to be read out to the caller.
Action on returned data	• *None*: Select if you do not want to share the information that the digit collector gathers with other interfaces. • *Add to agent console - Display name:* Select if you want agents in the queues where the IVR calls are routed to see the information that the digit collector gathers. Enter a name for the information to display on the agent console. • *Add to SIP header - Field name*: Select if you want to share the information that the digit collector gathers with other SIP header collectors. Enter a value that matches the value on the SIP header to enable information sharing. • *Add to remote CDR - Field name*: Select if you want to share the information that the digit collector gathers with a remote CDR database. Enter a value that matches the value on the remote CDR to enable information sharing. • *Add to report - Field name*: Select if you want to share the information that the digit collector gathers with survey reports. Enter a value that matches the value on the surveys to enable information sharing. For information on surveys, see

GUI field		Description
		Configuring surveys on page 232.
Description		Enter any notes you have for the digit collector.
Digits Setting		
	Min digits	Enter the minimum digits the digits collector allows. The range is 1-30.
	Max digits	Enter the maximum digits the digits collector allows. The range is 1-30.
	Max invalid input allowed	Enter the number of times a caller is allowed for inputting wrong digits. The call will be terminated if the limit is reached. The range is 0-10.
	Timeout	Enter the time limit that a caller is allowed for taking NO action after the call is put through. The call will be terminated if the time limit is reached. The range is 0-600 seconds.
	Max timeout allowed	Enter the number of timeouts a caller is allowed for taking no action after the call is put through. The call will be terminated if the number of timeouts limit is reached. The range is 0-10. For example, if *Timeout* is set to 10 seconds and *Max timeout allowed* to 3, a caller would have a total of 30 seconds timeout time after he or she dials in and takes no action afterwards.

2. Click *Create*.
   You can create a maximum of 10 digit collectors which are saved as variables.

To configure a RESTful collector

1. After configuring the digit collector, click *Add RESTful Collector* to configure the database collector for resource querying.

GUI field	Description
Name	Enter a name for the RESTful collector.
Service	Select the RESTful service for the collector. You can also create a new service or edit the selected one. For more information, see Configuring RESTful service on page 231.
Method	Choose the method to submit the information collected by the FortiVoice IVR system to the database server (as HTTP POST or HTTP GET) and use the value as a variable in your SQL statement.
Parameters	Select *Edit* to enter query parameters to customize the results returned from a GET or POST operation on the database, such as sorting or filtering. Optionally, click *Add Variable* to insert self or system defined variables into the parameters.
URL	Once you select Service on page 228, its URL displays here.

GUI field		Description
HTTP Headers		Select *Edit* to enter a HTTP header for information querying on the RESTful web service. Optionally, click *Add Variable* to insert self or system defined variables into the HTTP header. This option is only available if you select *Get* for *Method*.
Posting HTTP Headers		Select *Edit* to enter a HTTP header for information querying on the RESTful web service. Optionally, click *Add Variable* to insert self or system defined variables into the HTTP header. This option is only available if you select *Post* for *Method*.
Posting Message Body		Select *Edit* to enter a HTTP message body for information querying on the RESTful web service. Optionally, click *Add Variable* to insert self or system defined variables into the HTTP body. This option is only available if you select *Post* for *Method*.
Timeout		Enter the time allowed for the query to be processed. If the time elapses before the query response is complete, partial information may be returned. The range is 0-600 seconds.
Max retry allowed		Enter the number of database query tries allowed. The query will be denied if the retry limit is reached. The range is 0-10.
Description		Enter any notes you have for the RESTful collector.
New (under Fields)		Click to name each of the attributes returned from a database query to present it or use it as a variable.
	Field	Enter a name for the attribute you want to define.
	Query	Enter the query parameter for the attribute you want to define. Optionally, click *Add Variable* to insert self or system defined variables into the parameter.
	Action on returned data	• *None*: Select if you do not want to share the information that the RESTful collector gathers with other interfaces. • *Add to agent console - Display name:* Select if you want agents in the queues where the IVR calls are routed to see the information that the RESTful collector gathers. Enter a name for the information to display on the agent console. • *Add to SIP header - Field name*: Select if you want to share the information that the RESTful collector gathers with other SIP header collectors. Enter a value that matches the value on the SIP header to enable information sharing. • *Add to remote CDR - Field name*: Select if you want to share the information that the RESTful collector gathers with a remote CDR database. Enter a value that matches the value on the remote CDR to enable information sharing. • *Add to report - Field name*: Select if you want to share the

GUI field	Description
	information that the RESTful collector gathers with survey reports. Enter a value that matches the value on the surveys to enable information sharing. For information on surveys, see Configuring surveys on page 232.

2. Click *Create* and then *Create*.
   You can create a maximum of 10 RESTful collectors which are saved as variables.

To configure IVR handling

1. After configuring the RESTful collectors, click *Add IVR handling* to configure call processing using the digit and RESTful collector configurations.
   SIP header, digit and RESTful collector configurations only take effect after IVR handling is set up.

GUI field		Description
Condition		Configure the conditions based on which call processing actions are taken.
	Unconditional	Select if you do not need to configure the conditions. In this case, the system default condition applies.
	Variable	Click *Add* to insert self or system defined digit or RESTful variable for the condition. This option appears if you deselect *Unconditional*.
	Operator	Use query operators to assign a value to the variable, or perform mathematical operations. This option appears if you deselect *Unconditional*.
	Value	Enter the value assigned by the operator to the variable. Optionally, click *Add Variable* to insert self or system defined variables into the value. This option appears if you deselect *Unconditional*.
	Description	Enter any notes you have for the IVR handling.
Action		Click *New* to configure the actions to take based on the conditions.
	Action type	Select the IVR action. Depending on the action type selected, further configuration may be needed. For example, if you select *Dial extension*, enter the extension to which a call is transferred. Click *Create*. You can create multiple actions. Some action types have an option for you to add a variable for further configuration, such as *Dial Extension* or *Call Queue*. Instead of manually adding a value, you may choose a predefined variable which contains the further configuration information of the action type you choose.

2. Click *Create.*

To configure error handling

1. After configuring IVR handling, click *Add Error Handling* to deal with unknown errors and RESTful service errors.
2. For *Error type*, select *Unspecified* for unknown errors and *RESTful* for RESTful service errors.
3. Click *New* to select the action. Depending on the action type selected, further configuration may be needed. For example, if you select *Dial extension*, enter the extension to which a call is transferred.
   Some action types have an option for you to add a variable for further configuration, such as *Dial Extension* or *Call Queue*. Instead of manually adding a value, you may choose a predefined variable which contains the further configuration information of the action type you choose.
4. Click *Create*, *Create*.
5. Click *OK* to complete the IVR configuration.

Configuring RESTful service

FortiVoice IVR interfaces with RESTful web service for querying caller information from the database. When RESTful service is set up and a caller dials in, the FortiVoice unit sends caller information inquiry to the RESTful web service which sends back the information to the agent who processes the call.

Call Center > IVR > RESTful service allows you to configure the RESTful web service.

To configure RESTful service

1. Go to *Call Center > IVR > RESTful service,* click *New* and do the following:

GUI field	Description
Name	Enter a name for the configuration.
Protocol	Select the protocol for the service.
Authentication	*Password*: Select to enter the user name and password for logging onto the RESTful server. *OAuth*: Select to use Open Authorization to access the RESTful server without exposing your account credential. • *Service format*: Select Salesforce or other RESTful services configuration format. • *Username*: Enter the login user name registered on the RESTful server. • *Password*: Enter the login password registered on the RESTful server. • *Login server*: Enter the IP address of the RESTful server. • *Client ID*: Enter the consumer key from the RESTful server. • *Client secret*: Enter the consumer secret from the RESTful server. If you choose Salesforce as *Service Format*, enter the consumer key and the token from the server in the format of <consumer key><token>. For information on FortiVoice and Salesforce integration, see *Salesforce Integration with FortiVoice Enterprise Technical Note*. • *Base URL suffix*: Enter the Salesforce object name, for example, /query/, and click *Get Salesforce API URI* to populate the *Base URL* field. Note the leading and trailing "/" must be entered before and after the object name. This option is only available if you choose *Salesforce* for *Service format*.
Base URL	If you choose *None* for *Service format*, enter the URL of the server hosting RESTful service. Click *Test* to validate the URL.
SSL verification	Select if required.
Description	Click *Edit* to enter any notes for the configuration.

2. Click *Create*.

Configuring surveys

You can use surveys to collect customer feedback on the service delivered by your call center agents. You can also set survey rules.

To configure a survey

1. Go to *Call Center > Survey > Survey.*
2. Click *New* and type the name of the survey.
3. For *Description*, enter any comments you have for the survey.

4. Click *New* under *Questionnaire* and configure the following:

GUI field		Description
Name		Enter a name for the digits collector.
Prompt		Select the audio file that you want callers to listen to. You can also create a new file or edit the selected one. For more information, see Managing phone audio settings on page 110.
Enable read back		Select if you want the digit inputs to be read out to the caller.
Question		Enter the survey question.
Digits Setting		
	Max digits	Enter the maximum digits the digits collector allows. The range is 1-30.
	Max invalid input allowed	Enter the number of times a caller is allowed for inputting wrong digits. The call will be terminated if the limit is reached. The range is 0-10.
	Timeout	Enter the time limit that a caller is allowed for taking NO action after the call is put through. The call will be terminated if the time limit is reached. The range is 0-600 seconds.
	Max timeout allowed	Enter the number of timeouts a caller is allowed for taking no action after the call is put through. The call will be terminated if the number of timeouts limit is reached. The range is 0-10. For example, if *Timeout* is set to 10 seconds and *Max timeout allowed* to 3, a caller would have a total of 30 seconds timeout time after he or she dials in and takes no action afterwards.

5. Click *Create*.
   The survey is listed under *Questionnaire*. You may click *New* to add more.
6. If you want callers to comment on the survey, select *Caller Comment*.
7. For *Audio prompt*, select the audio file that explains to callers how to comment on the survey. Click *New* to create a new audio file. For more information, see Managing phone audio settings on page 110.
8. For *Description*, enter any notes for the *Caller Comment*.
9. Click *Create*.

To configure survey settings

1. Go to *Call Center > Survey > Setting.*
2. For *Survey retention month*, enter the number of months that you want to keep the surveys.
3. For *Max survey records*, enter the maximum number of surveys you want to keep.
4. Click *Apply*.

Setting up monitor view

You can create a monitor to let agents with privileges to view the snapshot of the key information of queues on the user web portal, such as number of calls in queue, longest waiting calls, and abandoned calls. You can also create monitor view color themes in addition to the default one.

To apply the queue view configuration, you need to enable it in agent profile and apply the profile to an agent. As a result, the agent will have a *Monitor View* icon once logging into the user web portal.

To set up a monitor view

1. Go to *Call Center > Monitor View > Monitor.*
2. Click *New* and configure the following:

GUI field		Description
Name		Enter a name for the queue view.
Trusted hosts		Enter the IP address and netmask of the device that is permitted to use the monitor view. If you have multiple devices, you may enter up to 10 trusted hosts.
Monitor Items		Click *New* to include the queues or agents that you want to monitor.
	Title	Enter a name for the configuration.
	Type	Choose to monitor queues or agents.
	Refresh interval	Enter the refresh interval time for the monitor view in seconds.
	Color theme	Select the color theme for the monitor view. See To create a monitor view theme on page 234.
	Start time	Enter the time for the monitor view to start.
	Queue	From the *Available* field select the queues to be included and click ->. Click *Create*.
Logo		Select *Customized logo* to add text or logo for agents with privileges to view on the user web portal. In the text editor window, you can type the text or copy and paste a logo here.

3. Click *Create*.

To create a monitor view theme

1. Go to *Call Center > Monitor View > Monitor Theme.*
2. Click *New* and configure the following:

GUI field	Description
Theme name	Enter a name for the theme.
Background color Column header color Row header color Row color Text color	Click each field to select the color for the monitor view background, column header, row header, row, and text.

GUI field		Description
Agent Threshold Setting		Click *New* to set the colors for agent names display in monitor view based on status.
	Status	Choose an agent status for which you want to set a color.
	Threshold value	Enter the refresh interval time for displaying the agent names in seconds.
	Threshold color	Select the color theme for displaying the agent names at the time interval you set.

3. Click *Create*, then *Create*.

Configuring other agent information

Configure call agent skill sets, skill levels, reason codes, data service, and global Setting to be used for configuring agent profiles.

Adding agent skill sets

Depending on the agents skills and the nature of your business, you can classify agents into different groups, such as Billing, Sales, or Support.

To add an agent skill set

1. Go to *Call Center* > *Configuration* > *Skill Set*.
2. Click *New*.
3. Enter a name, such as HR, and description for the skill set.
4. Click *Create*.

Creating agent skill levels

The FortiVoice unit comes with 9 default skill levels, ranging from 10 to 90, with 10 to 30 being junior, 40 to 60 being intermediate, and 70 to 90 being senior. You can modify the default skill level descriptions, or create new skill levels.

To create an agent skill level

1. Go to *Call Center* > *Configuration* > *Skill Level*.
2. Click *New*.
3. Enter the skill level and description.
4. Click *Create*.

Modifying agent reason code descriptions

Agent reason codes explain why agents are not able to take calls, such as due to lunch break, meeting, or vacation. You can add new codes and change code descriptions of the default reason codes.

To add an agent reason code

1. Go to *Call Center > Configuration > Reason Code*.
2. Click *New*.
3. Enter the code name, code number, and code description.
4. Click *Create*.

Configuring data service

If you use a third party software to generate call center reports or statistics, you can configure the FortiVoice unit to back up the data.

To configure data service

1. Go to *Call Center > Configuration > Data Service*.
2. Select *Enabled* to activate the service.
3. Configure the schedule time.
4. Enable *Local* if you want to back up locally.
5. Enable *Remote* and configure the FTP/SFTP server credentials if you want to back up remotely.
6. Enter the email address for sending the call center reports or statistics.
7. Configure the maximum backup number. When the maximum number is reached, the oldest version will be overwritten.
8. Click *Field description* to view the FortiVoice data value description.
9. Click *Apply*.

Setting caller priorities

You can set call answering priorities for callers entering the call queue. A new call always starts with the lowest priority. However, a queue manager with privileges can change the priority of a call on the agent console of the user web portal.

To set caller priorities

1. Go to *Call Center > Configuration > Global Setting.*
2. Enter the caller's highest and lowest priorities.
3. Click *Apply*.

Configuring agent profiles

Create agent profiles to define agent privileges for processing calls. Agent profiles become effective when they are applied to the agent extensions. For more information, see Setting up local extensions on page 156.

To create an agent profile

1. Go to *Call Center > Profile > Profile.*
2. Click *New*.

3. Configure the following:

GUI field		Description
Name		Enter a name for the profile.
Agent		Select the calls an agent can make or process.
	Pickup call from queue	Select to allow the agent to answer queue calls.
	Ring no answer	Select the action to take when nobody answer a call in the queue. • *Do nothing*: No action is taken and the call keeps ringing. • *Auto pause*: The call is paused automatically. • *Auto logout*: The agent to whom this profile applies is automatically logged out of the queue. • *Auto hold off*: The call is automatically put on hold.
	Hold off time	If you select *Auto hold off* for *Ring no answer,* enter the time to put a call on hold.
Queue		Select to allow an agent to prioritize the calls in the queue or transfer calls to another queue on the agent console of the user web portal. If you select *Caller prioritization*, the *Priority* button appears on the agent console of the user web portal. If you select *Transfer call to another queue*, the *Transfer* button appears on the agent console of the user web portal. For *Paused agent ring option*, if you want to ring agents in pause status, select *Ring Targeted*.
Manager Privilege		If the agent is a manager, select the privileges to manage the agents using the agent console of the user web portal. The privileges include coaching, listening, and logging in and logging out agents, or pausing and resuming agents.
Agent Console Privilege		Select *Enable agent console* to choose the widget and GUI popup alert for an agent to view on the agent console of the user web portal.
Monitoring Console Privilege		Select to enable monitoring console on the user web portal.
Monitoring Queue		
	Member of queues	Select to enable the agent to only monitor the queues of which the agent is a member.
	Selected	Select the queues the agent is allowed to monitor by moving the selected queues from the *Available* field to the *Selected* field. The *Available* field lists all queues regardless if the agent is a member of them.
	All	Select to allow the agent to monitor all call queues.

4. Click *Create*.

Working with call queue statistics

Go to *Call Center > Statistics* to view agent and queue daily summaries. You can also download the summaries. The summaries cover a period of 30 days.

To view agent daily summary

1. Go to *Call Center > Statistics > Agent Daily Summary.*

GUI field	Description
Date	The date of the agent call summary.
Agent	The agent ID.
Work Time	The agent’s total work hours for the queue that the agent worked the longest.
Talk Time	The total time the agent talked on the phone in all queues combined.
N/A Time	The total time the agent was away from the phone in all queues combined.
Total Answered	The total calls the agent answered in all queues combined.
Total RNA	The total calls not answered by the agent in all queues combined.
Out. Call	The outgoing calls made by the agent. This option is dependant on your queue management configuration in Call Center on page 163.
Out. Talk Time	The total time of outgoing calls made by the agent. This option is dependant on your queue management configuration in Call Center on page 163.
Voicemail	The number of voicemails left on the agent's extension.

To view queue daily summary

1. Go to *Call Center > Statistics > Queue Daily Summary*.

GUI field	Description
Date	The date of the call queue summary.
Queue	The queue name.
Calls	The number of calls reached this queue.
Abandoned	The number of calls that gave up after reaching the queue.
Overflow	The number of callers exceeding the maximum waiting callers set for the queue and timed-out waiting callers. See Maximum queue capacity on page 217.
Talk Time	The total phone talk time of the queue.
Wait Time	The total time for holding calls in the queue.
Out. Call	The outgoing calls made by the agents in the queue. This option is dependant on your queue management configuration in Call Center on page 163.
Out. Talk Time	The total time of outgoing calls made by the agents in the queue. This option is dependant on your queue management configuration in Call Center on page 163.

Configuring call center report profiles and generating reports

The *Call Center > Report > Report* tab displays a list of report profiles.

A report profile is a group of Setting that contains the report name, its subject matter, its schedule, and other aspects that the FortiVoice unit considers when generating reports from log data. The FortiVoice unit presents the information in tabular and graphical format.

You can create one report profile for each type of report that you will generate on demand or on a schedule.

Generating reports can be resource intensive. To avoid phone processing performance impacts, you may want to generate reports during times with low traffic volume, such as at night. For more information on scheduling the generation of reports, see Configuring report email notifications on page 1.

To view and configure report profiles

1. Go to *Call Center > Report > Report*.

GUI field	Description
Clone	Select a report and click this button to duplicate a report with a new name.
Generate	Select a report and click this button to generate a report immediately. See Generating a report manually on page 1.
View Reports	Click to display the list of reports generated by the FortiVoice unit. You can delete, view, and/or download generated reports. For more information, see Viewing generated reports on page 31.
View Supported Query	Click to display supported query summary.
Name	Displays the name of the report profiles.
Department	The department to which the report belongs.
Schedule	Displays the frequency with which the FortiVoice unit generates a scheduled report. If the report is designed for manual generation, *Not Scheduled* appears in this column.

2. Click *New* to add a profile or double-click a profile to modify it.
   A multisection dialog appears.
3. In *Name*, enter a name for the report profile.
   Report names cannot include spaces.
4. In *Department*, select the department for this report.
   For information on departments, see Creating extension departments on page 180.
5. Click the arrow next to each option, and configure the following as needed:
   - Configuring the report query selection on page 240
   - Configuring the report time period on page 241
   - Configuring report email notifications on page 1
   - Configuring the report schedule on page 1
   - Generating a report manually on page 1
6. Click *Create*.

Configuring the report query selection

When configuring a report profile, you can select the queries that define the subject matter of the report.

Each report profile corresponds to a chart that will appear in the generated report.

To configure the report query selection

1. Go to *Call Center > Report > Report*.
2. Click *New*.
3. Expand *Query List* and click *New*.

4. Configure the following:

GUI field	Description
Name	Enter a name for this query.
Category	Select a category for the report profile. The report chart will correspond to the category selected.
Sub category	Select a sub query type for the report profile. The report chart will correspond to the type selected.
Query	Depending on your selection of Category and Sub category, choose the specific report you want to generate. Depending on the report you choose, select queues or agents for which you want to generate reports.

5. Click *Create.*

Configuring the report time period

When configuring a call center report profile, you can select the time span of log messages from which to generate the report.

To configure the report time period

1. Go to *Call Center > Report > Report*.
2. Click *New*.
3. Expand *Period* to select the time span option you want. This sets the range of log data to include in the report.
4. For *Type*, choose a relative time, such as *Today, Yesterday, Last N hours*, and so on. If you select an option with an unspecified “N” value, enter the number of hours, days or weeks in the *Value* field, as applicable.

Working with Property Management System

Businesses such as hotels use Property Management System (PMS) to manage their services. The PMS can be connected to a PBX such as the FortiVoice unit to configure a customer's room phone by displaying the customer's name on the phone, emptying voicemails when a new customer checks in, logging phone calls, setting wake-up calls, and other services. You can also set the room condition codes for room maids to record the room cleaning status using the room phone.

This option is only available if you have purchased the license.

This topic includes:

- Configuring hotel management settings on page 242
- Configuring hotel room status on page 244

Configuring hotel management settings

Hotel Management > Setting lets you configure the Setting for the FortiVoice unit to interoperate with your PMS, set the room condition codes, such as setting 1 to represent that maid is present and 4 to represent the out-of-service status, and configure guest check in and check out actions.

Configure your PMS Setting accordingly.

To configure hotel management settings

1. Go to *Hotel Management > Setting > PMS.*
2. Configure the following:

GUI field		Description
PMS Setting		
	Enabled	Select to enable the PMS.
	Protocol	Select the protocol used by the FortiVoice unit to communicate with the PMS.
	Serial connection	Select to connect to the PMS using a serial cable. This option is only available for *Micros* protocol.
	LRC	Select to perform longitudinal redundancy check (LRC). This option is only available for *Micros* protocol.
	Mode	Choose to use the FortiVoice unit as server or client when connecting to the PMS. If it is used as client, enter the server IP address in the *Server* field. This option is only available for *Micros* and *Comtrol* protocols.
	Port	Enter the port number that connects to the PMS.

GUI field		Description
		Note that you need to use an adaptor for the FortiVoice-PMS connection. Fortinet recommends using iPocket232 by Precidia. From the ports you configured, connect the PMS serial cable to the adaptor and then connect the RJ45 cable from the FortiVoice unit to the adaptor.
	Call billing	Select to activate call billing. This option is only available for *Micros* and *Comtrol* protocols.
Network Setting		Enter the IP address and netmask of the PMS. If the PMS uses serial connection to an adaptor, enter the IP address and netmask of the adaptor. If you have multiple PMSes, you may enter multiple trusted hosts.
Data sync		This option is only available for *Micros* and *Comtrol* protocols. When the FortiVoice unit is connected to the PMS, it constantly receives all room-based information such as guest name, room privileges, and check in and check out times from the PMS. Normally, you do not need to click the *Data sync* button since the data synchronization is automatic. You only do so when there is a data mismatch between the FortiVoice unit and the PMS. Fortinet recommends performing a manual data sync at off hours because all related operations, such as check in and check out, are suspended during a data sync.

3. Click *Apply*.

To configure check in and check out actions

1. Go to *Hotel Management > Setting > Option.*
2. Configure the following:

GUI field		Description
Check In Action		
	Reset	Set the guest information and room condition to make a room check-in ready. • *Privilege*: Select to enable phone call restriction (internal, local, or long distance) and user privilege (option 1, 2, 3) for the room. If you choose this option, select a *Privilege* for the room user. For information on setting user privileges, see Configuring user privileges on page 126 • *Guest name*: Select to display room number or guest name on the room extension. In the *Name* field, enter `%%NUMBER%%` or `%%NAME%%`. • *Room condition*: Select to clear any condition set for the room.

GUI field		Description
Check Out Action		
	Reset	Set the guest information and room condition to make a room check-out ready. • *Privilege*: Select to enable phone call restriction (internal, local, or long distance) and user privilege (option 1, 2, 3) for the room. If you choose this option, select a *Privilege* for the room user. For information on setting user privileges, see Configuring user privileges on page 126 • *Guest name*: Select to display room number or guest name on the room extension. In the *Name* field, enter `%%NUMBER%%` or `%%NAME%%`. • *Room condition*: Select to clear any condition set for the room. • *Voicemail*: Select to clear all voicemails for the room extension. • *Wake-up call*: Select to clear all wakeup call setups for the room extension.
Advanced		Choose the order for room maids to request for room item by phone. You can choose to dial the item code or number first. For example, if you choose to dial code first and want to request for two beers (code 1) and three waters (code 2), you can dial 1*2*2*3. For information on item code, see To set mini bar code for room maids to order room items on page 244.

3. Click *Apply*.

To set mini bar code for room maids to order room items

1. Go to *Hotel Management* > *Setting* > *Minibar Code.*
2. Click *New*.
3. Enter the item name, for example, Beer.
4. Enter the item code, for example, 5.
5. Click *Create*.
A room maid can dial the code to order things needed for the room using the room phone. For more information, see Advanced on page 244.

Configuring hotel room status

Hotel Management > *Room Status* lets you set hotel room status.

Once the PMS and the FortiVoice unit is properly connected and the PMS is enabled on the FortiVoice unit, all hotel room extensions appear on the FortiVoice unit.

To batch-configure hotel room statuses

1. Go to *Hotel Management* > *Room Status* and click *Server Info.*
   A green dot means the FortiVoice unit is connected with the PMS. Otherwise, a red dot appears.
2. Select more than one room in the list.
   Depending on the situations of the rooms you select, the *Check in, Check out, Privilege, Room condition, Room setting,* and *VIP setting* buttons become active.

   A green dot under *Guest* means this guest room’s extension is bound with the room. Otherwise, a red dot appears. For more information, see Guest phone on page 246.
3. Click a button to batch-configure the room status and apply it to all rooms selected.

To configure a single hotel room status

1. Go to *Hotel Management* > *Room Status.*
2. Select a room extension and click *Edit*.

3. Configure the following:

GUI field		Description
Guest phone		Select to bind the extension with the room and make the room a guest room.
Number		The extension number of the room. You can click the number and modify it if required. For more information, see Configuring IP extensions on page 156.
Room		The hotel room number. You can click the number and modify it if required.
Location		Click to enter the room location.
Guest Setting		This option appears only if you have enabled *Guest phone*.
	Checked-in	Enable the room status to checked-in.
	VIP setting	Select to set the guest as a VIP. Specific VIP treatments are determined by each hotel.
	Room condition	Select the cleaning status of the room. You can add a new code or edit the current one: 1. Click *New* to add a code or select an existing code and click *Edit* to modify it. 2. Select the protocol for connecting to your PMS. 3. Enter a code number. 4. Enter the code description. 5. Click *Create*.
	Guest name	Enter the name of the guest for this room. This option is available only if *Checked-in* is enabled.
	Privilege	Select phone call restriction (internal, local, or long distance) and user privilege (option 1, 2, 3) for the room. For information on setting user privileges, see Configuring user privileges on page 126. This option is available only if the *Checkin status* is *Checked-in.*
	DND	Select if the guest of the room does not want to be disturbed. This option is available only if *Checked-in* is enabled.

4. Click *OK*.

Configuring phone auto dialer

With the auto dialer function, the FortiVoice unit can be configured to automatically dial telephone numbers. Once the call is answered, the FortiVoice unit plays a recorded message.

This topic includes:

- Setting up an auto dialer campaign on page 247
- Creating a recorded broadcast message on page 248
- Adding contacts and contact groups on page 248
- Configuring auto dialer settings on page 249
- Viewing auto dialer reports on page 249

Setting up an auto dialer campaign

Auto Dialer > Campaign > Campaign allows you to set up an auto dialer task to broadcast a recorded message to the dialed phone numbers.

To set up an auto dialer campaign

1. Go to *Auto Dialer > Campaign > Campaign.*
2. Click *New* and configure the following:

GUI field	Description
Name	Enter a name for the campaign.
Caller ID	Enter the caller ID to be displayed on a called phone. You can also select an extension number instead.
Status	The current status of the campaign.
Sound file	Select a recorded message that you want to broadcast. You can also create a new one. For more information, see Creating a recorded broadcast message on page 248.
Retry	Enter the number of times you want to retry calling.
Description	Enter any notes you have for this campaign.
External Numbers	Select the external phone numbers you want to autodial. You can add these numbers by going to *Auto Dialer > Contact > Contact/Contact Group.* See Adding contacts and contact groups on page 248.
Internal Numbers	Select the internal phone numbers you want to autodial. These numbers are the internal extensions on the FortiVoice unit.

3. Click *Create*.
4. If you want to start a campaign, in the campaign list, select one with a status other than *Completed* and click *Start* on top of the screen.

5. Select a campaign start and end time.
6. Click *OK*.

Creating a recorded broadcast message

Auto Dialer > *Campaign* > *Audio* allows you to create a sound file for the auto dialer to broadcast.

To create a sound file

1. Go to *Auto Dialer* > *Campaign* > *Audio.*
2. Click *New*.
3. Enter a name for the sound file.
4. Select an *Action*:
   - *Upload*: Click to upload a sound file. Uploaded sound file should be a WAVE file (*.wav) in 16bit PCM(8000Hz) compression format.
   - *Record*: Click to enter a phone number and click *Send*. When the phone rings, pick it up and record the message.
   - *Play*: Once a file is uploaded or recorded, click to play it.
   - *Download*: Once a file is uploaded or recorded, click to download it.
5. Click *OK*.

Adding contacts and contact groups

Auto Dialer > *Contact* > *Contact/Contact Group* allows you to add contacts and contact groups that can be used in an auto dialer campaign. You may also import or export the contacts.

To add a contact

1. Go to *Auto Dialer* > *Contact* > *Contact*.
2. Click *New* and enter the contact information.
3. Click *Create*.

To add a contact group

1. Go to *Auto Dialer* > *Contact* > *Contact Group.*
2. Click *New*.
3. Enter a name for the group.
4. Select the members for the group.
   Members are created by adding contacts. See To add a contact on page 248.
5. Click *Create*.

Configuring auto dialer settings

Auto Dialer > *Setting* allows you to set the maximum call channels (64 by default) for campaigns. This value represents the number of phones that can be auto dialed at the same time.

Viewing auto dialer reports

Auto Dialer > *Report* allows you to view the status of the auto dialer campaigns, including campaign IDs and names, call status, total number of campaigns, number of uncalled, answered, unanswered calls, and retries, and call duration and time.

Configuring Call Features

The *Call Features* menu lets you configure the Setting for many call features such as conference call, auto attendant, faxing, and much more.

This topic includes:

- Configuring auto attendants on page 250
- Mapping speed dials on page 255
- Configuring conference calls on page 256
- Recording calls on page 258
- Creating call queues and queue groups on page 216
- Configuring call parking on page 262
- Configuring fax on page 263
- Setting calendar reminder on page 270
- Modifying feature access codes on page 271
- Configuring Internet of Things (IoT) on page 276

Configuring auto attendants

An auto attendant can answer a telephone line or VoIP number, and can be included in the call cascade of a local extension, remote extension or ring group.

An auto attendant can answer a call if the receptionist is away or if you do not have a receptionist. Each auto attendant has a message with options. The message tells the caller what the options are. You can load a professionally pre-recorded message, or can record a message using a handset.

Auto attendants limit on FVE models

Model	Number of auto attendants supported
FVE-200F/VM200	20
FVE-300E	30
FVE-500E/500F/VM500	50
FVE-1000E/VM1000	100
FVE-2000E/2000F/VM2000	200
FVE-3000E/VM3000	300
FVE-5000F/VM5000	500
FVE-VM10000	1000
FVE-VM50000	1000

To view the list of auto attendants, go to *Call Feature > Auto Attendant > Auto Attendant*.

GUI field	Description
Delete	Removes a selected auto attendant. You cannot remove an auto attendant that is used in another auto attendant configuration.
Name	The name of the auto attendant.
Direct Actions	The number of key actions configured for the main auto attendant, excluding the key actions for the subsidiary auto attendants.

To create an auto attendant

1. Go to *Call Feature* > *Auto Attendant* > *Auto Attendant* and click *New*.
2. Configure the following:

GUI field	Description
Name	Enter a name for the auto attendant.
Default language	Select the language for the auto attendant greeting message (sound file). If you select *Default*, the greeting message will be the same as what you set for the FortiVoice unit. For more information, see Setting PBX location and contact information on page 102. You can also select other languages. The language files are created in Managing phone audio settings on page 110.
Greeting mode	If you select *Simple*, select a greeting message (sound file) for the auto attendant. See Greeting on page 251. If you select *Scheduled* to add a scheduled greeting, do the following: • In *Scheduled Greeting Setting*, click *New*. • In the *Schedule* field, select a schedule for the greeting. Scheduled are created in Scheduling the FortiVoice unit on page 131. • In the *Greeting* field, select a sound file. You can click *New* to add a new file or *Edit* to modify the selected one. For more information, see Managing phone audio settings on page 110. • Click *Create*.
Greeting	Select a greeting message (sound file) for the auto attendant. You can edit a selected file or create a new one. For more information, see Managing phone audio settings on page 110. This option is only available if you select the *Simple* greeting mode.
Ringing for	Enter the number of seconds for the phone to ring before the auto attendant answers with the greeting message.
Timeout action after	Enter the number of seconds that an auto attendant should be allowed to wait before the caller takes further action according to the voice instructions. Select the action when the auto attendant timeout is reached.

GUI field		Description
		• *Dial Operator*: The call is transferred to an operator. • *Dial Extension*: The call is transferred to the extension you select. You can edit a selected extension or create a new one. For details, see Configuring IP extensions on page 156. • *Go to Voicemail*: The call is transferred to a voicemail box. Select the voicemail extension. • *Ring Group*: The call is transferred to a ring group. Select the ring group. For more information, see Creating ring groups on page 181. • *Call Queue*: The call is transferred to a call queue. Select the queue. For more information, see Creating call queues on page 216. • *Start Over*: The auto attendant will repeat the instructions for the caller. Also enter the maximum times to repeat. • *Hang Up*: The call will be terminated.
Invalid input action after		Enter the number of seconds that an auto attendant should be allowed to wait after the caller enters an invalid input. Select the action when the caller enters an invalid input.
Dial Pad Key Action		Configure the auto attendant keys for callers to use when navigating through the auto attendant hierarchy. For more information, see Configuring key actions on page 253.
	Key	The key that transfers a call to a resource, for example, voicemail, if pressed.
	Action	The resource to which a call is transferred by pressing a key. Some actions require further configuration. For example, if you select *Dial Extension*, you need to enter the extension number.
	Target	The resource target if applicable. For example, an extension number, sound file, or external phone number that leads to a resource.
Advanced		Upon finishing configuring these functions, you need to inform the users on how to use them after they reach the auto attendant. • *Access voicemail*: Enable to allow external callers to reach their voicemail boxes by dialing the default voicemail prompt code *98 or the code you set. For more information about feature code, see Modifying feature access codes on page 271. • *Dial local number*: Select to enable an external caller to dial local extensions. • *Override schedule*: Select to allow a system administrator to dial a code to replace the schedule with a system schedule. For more information, see Configuring system capacity on page 107. • *Allow recording of prompt sound file*: Select to enable an external caller to dial into the FortiVoice unit and record a

GUI field	Description
	sound file. • *Call Bridge (DISA)*: Select an account code for external users to dial into the FortiVoice unit and use the FortiVoice service just like the local extensions. Callers must dial the DISA code followed by the account code before making the calls. You can edit a selected account code or create a new one. For more information on DISA code, see Modifying feature access codes on page 271. For more information on account code, see Configuring account codes on page 154. • *Outbound dialplans allowed for access*: Select the outbound dial plan for users to call the FortiVoice unit and through it to make outbound calls. For details, see Configuring outbound dial plans on page 211. • *Business group*: Select a business group to enable an external caller to dial into an extension within the group using the shortened number. For information about business group, see Creating business groups on page 187.

3. Click *Create*.

Configuring key actions

Configure the auto attendant dial pad keys for callers to use when navigating through the auto attendant hierarchy.

For more information, see Dial Pad Key Action on page 252.

To configure a key action

1. While configuring an auto attendant, click *New* under *Dial Pad Key Action*.
2. Enter the key number that transfers a call to a resource, if pressed.
3. For *Language*, select the language to be used for this key action.
4. Select an *Action*:

GUI field	Description
No Action	The call is not transferred to any resource.

Play Announcement	Play an announcement with directions, business hours, etc.
	• Select the sound file for the announcement. You can click *Edit* to modify an existing one or *New* to add a new one. For information on sound files, see Managing phone audio settings on page 110.
	• Select an action to follow the announcement:
	  • *No action*: The auto attendant takes no action.
	  • *Hang up*: The call will be terminated.
	  • *Start over*: The auto attendant will repeat the announcement.
	  • *Auto attendant*: The call is routed to another auto attendant, which allows actions to be nested into a powerful call routing system.

GUI field	Description
Dial Operator	The call is transferred to the operator.
Dial Extension	The call is transferred to a specified local extension. Select the extension. You can click *Edit* to modify an existing one or *New* to add a new one. For more information, see Configuring Extensions on page 156.
Go to Voicemail	The call is transferred to a voice mailbox, allowing the caller to leave a message. Select the voice mailbox. You can click *Edit* to modify an existing one or *New* to add a new one. For more information, see Configuring IP extensions on page 156.
Ring Group	The call is transferred to the call queue of a ring group. The call is placed on hold. The system will ring the next available extension in the ring group. Select the ring group. You can click *Edit* to modify an existing one or *New* to add a new one. For more information, see Creating extension groups on page 180.
Dial Number	The call is transferred to a specified remote extension number. Enter the remote extension number. For more information, see Setting up remote extensions on page 169.
Call Queue	The call is transferred to a call queue. Enter the call queue configuration. For more information, see Creating call queues and queue groups on page 216.
Lookup Name Directory	Access the dial-by-name directory so the caller can find a user’s extension number by entering the user’s name.
Change Language	Change the auto attendant greeting language. Select the language and a follow-up action. If you choose *Auto attendant* for the follow-up action, select the auto attendant. For *Language*, if you select *Default*, the greeting message will be the same as what you set for the FortiVoice unit. For more information, see Setting PBX location and contact information on page 102. You can also select other languages. The language files are created in Managing phone audio settings on page 110.
Auto Attendant	Route the call to another auto attendant, which allows actions to be nested into a powerful call routing system. For example, the main auto attendant can say “Press one for English. Oprima dos para Español.” Option 1 goes to the English auto attendant and option 2 goes to the Spanish auto attendant. Select an auto attendant. For information on creating auto attendants, see Configuring auto attendants on page 250.
Start Over	The auto attendant will repeat the announcement.
Hang Up	The call is terminated.
IVR	Route the call to the FortiVoice IVR system. For more information, see Configuring IVRs on page 225.

5. For *Music on hold*, select the voice prompt to be used for this key action. See Managing phone audio settings on page 110.
6. Optionally, enter any comments about this key action.
7. Click *Create*.

Mapping speed dials

For fast and efficient dialing, use the speed dial pattern to map the phone numbers, mostly outbound numbers.

You can map a speed dial code directly to a number if you only have a few numbers to map. You can also use speed dial rules to map a group of numbers.

To map a speed dial number

1. Go to *Call Feature* > *Speed Dial* > *Number*.
2. Click *New*.
3. Enter a name for the speed dial mapping.
4. For *Dialed Code*, enter the number based on the speed dial number pattern you set. For example, 333. For more information, see To set speed dial rules for mapping groups of numbers on page 255.
5. Enter the phone *Number* to map to the speed dial code.
   You can enter digits 0–9, space, dash, comma, # and *.

   Speed dial pattern accepts # as the lead digit (Eg. #XX or #613XXX).

   If you want to enter an auto attendant number followed by an extension, you can use comma (,) or semicolon (;) to pause the automatic dialing.
   A comma pauses dialing for two seconds, for example, 1-123-222-1234, 5678#. In this case, once pressing the speed dial code you set, auto attendant 1-123-1234 is reached, and after two seconds, extension 5678 is automatically dialed.
   A semicolon pauses dialing for one second, for example, 1-123-222-1234; 5678#. In this case, once pressing the speed dial code you set, auto attendant 1-123-1234 is reached, and after one second, extension 5678 is automatically dialed.
6. Optionally, enter a note for the mapping, such as “This is for customer A”.
7. Click *Create*.

To set speed dial rules for mapping groups of numbers

1. Go to *Call Feature* > *Speed Dial* > *Rule*.
2. Click *New*.
3. Enter a name for the speed dial mapping.
4. For *Dialed Pattern*, enter a speed dial pattern supported by the FortiVoice unit, for example, *83XXX.
   For information on setting speed dial number pattern, see Configuring PBX options on page 103.
5. For *Mapped Pattern*, enter the phone number pattern to map to the dialed pattern, for example, 6112239XXX.
   The mapped pattern tail’s number of digits must match that of the dialed pattern.
6. Optionally, enter a note for the mapping.
7. Click *Create*.
   In our example, when you dial *83111, phone number 6112239111 will be reached.

Configuring conference calls

The *Call Feature* > *Conferencing* tab lets you configure and enable conference call Setting.

You can configure and enable a user conference call privilege for extension users to hold their own conference calls on the user web portal. You can also set up a static or dynamic (calendar-based) conference call for the users.

To configure a user conference call

1. Go to *Call Feature* > *Conferencing* > *User Conferencing.*
2. Configure the following:

GUI field	Description
Enabled	Select to activate this conference call.
Number	Enter an extension number that is mapped to the external number callers can dial to join a conference call.
External numbers info	Enter the external phone number that callers can dial to join a conference call. Conference organizers can share it with the participants.
Music on hold	Select to play background music that callers hear after the joining message and leaving message are played. For information on creating music on hold file, see Managing phone audio settings on page 110.
Quiet mode	Select to not record and announce participant's name.
Users	Click *New* to add the extension users who have the privilege to organize conference calls. *User*: Select the extension for the user. Conferencing ID: Enter the ID that users need to organize conference calls. You can also click *Generate* to get a system generated ID. Click *Create*. Click *View Scheduled Conferences* to display the conferences that have been scheduled and pick a free time slot for your conference schedule.

3. Click *Apply*.

To set up a static conference call

1. Go to *Call Feature* > *Conferencing* > *Admin Conferencing* and click *New.*
2. Configure the following:

GUI field	Description
Mode	Select *Static*.
Name	Enter a conference call name.
Enabled	Select to activate this conference call.
Number	Enter a number that callers can dial and enter the user PIN to join a conference call.
Setting	

GUI field		Description
	Display name	Enter the name displaying on the conference call extension, such as “HR”.
	Attendee PIN	Enter a password for joining the conference call. A caller needs to dial the conference call number and enter this password to join the conference call. The default is 123456. This password is always valid and should only be sent to the people who need it.
	Organizer PIN	Enter the PIN number to be used by the conference organizer to host a conference call. The default is 123123. This password is always valid and should only be sent to the people who need it.
	Description	Enter any notes you have for this conference call.
	Music on hold	Select to play background music that callers hear after the joining message and leaving message are played. For information on creating music on hold file, see Managing phone audio settings on page 110.
	Quiet mode	Select to not record and announce participant's name.
Recursive Schedules		If you want conference calls on repeating schedules, select this option and click *New* to select a schedule. Enter a password for joining the conference call and click *Create*. This option is useful if you want to limit the participants to a particular recursive conference call. They can only join the conference call during the scheduled time period and by entering the password you set. For information on setting up a schedule, see Scheduling the FortiVoice unit on page 131.
One Time Schedules		If you want to set up a one time conference call, select this option and click *New* to enter the start and end time. Enter a password for joining the conference call and click *Create*. This option is useful if you want to limit the participants to a particular one time conference call. They can only join the conference call during the scheduled time period and by entering the password you set. If the one time schedule conflicts with the recursive schedule, the one time schedule has priority.

3. Click *Create*.

To configure a dynamic conference call

1. Go to *Call Feature* > *Conferencing* > *Admin Conferencing* and click *New.*
2. Configure the following:

GUI field		Description
Mode		Select *Dynamic*.
Name		Enter a conference call name.
Enabled		Select to activate this conference call.
Number		Enter the number that callers can dial and enter the user PIN to join a conference call.
Setting		
	Display name	Enter the name displaying on the conference call extension, such as "HR".
	Description	Enter any notes you have for this conference call.
	Music on hold	Select to play background music that callers hear after the joining message and leaving message are played. For information on creating music on hold file, see Managing phone audio settings on page 110.
	Quiet mode	Select to not to record and announce participant's name.

3. Click *Create*.
4. In the conference call list, select the one you created.
5. Double-click a date to schedule a conference.
6. Click *OK*.

Recording calls

For supervising and monitoring purposes, you can record incoming and outgoing calls to and from the extensions matching the caller number patterns or dialed number patterns you set. You can also select the recorded file format and archive the recorded calls.

This topic includes:

- Configuring call recordings on page 258
- Archiving recorded calls on page 260
- Setting the recorded file format on page 262

Configuring call recordings

Call Feature > *Call Recording* > *Policy* allows you to configure call recordings by creating, editing, removing, saving, or viewing a recording.

GUI field	Description
View Recordings	Click to view, listen, search, or save the recordings. You can also do so by going to *Status* > *Storage* > *Recorded Calls.* For details, see Playing recorded calls on page 35.
Enabled	Select to activate this call recording service.
Name	The name of the call recording service.
Description	Information of call recording configuration.

To configure a call recording

1. Go to *Call Feature* > *Call Recording* > *Policy*.
2. Click *New*.

GUI field		Description
Recording Policy		
	Name	Enter a name for this configuration.
	Enable	Select to activate this configuration.
	Description	Select the category of calls you want to record: by phone number, department, user group, trunk, or queue.
	Caller number pattern	This option appears if you select *By Phone Number* for *Description*. Enter the number pattern to match the callers' phone numbers following the pattern: ^[0-9XNZ]*[^\.]*$ where X=(0-9), Z=(1-9), and N=(2-9). For more information, see Configuring PBX options on page 103. The phone calls from the numbers matching the pattern will be recorded.
	Dialed number pattern	This option appears if you select *By Phone Number* for *Description*. Enter the number pattern to match the dialed phone numbers following the pattern: ^[^_][0-9XNZ\.]*$ where X=(0-9), Z=(1-9), and N=(2-9). For more information, see Configuring PBX options on page 103. The phone calls to the numbers matching the pattern will be recorded.
	Department	This option appears if you select *By Department* for *Description*.

GUI field		Description
		Select the extension department of which you want to record the calls. You can add a new department or modify an existing one. For more information, see Creating extension departments on page 180.
	Group	This option appears if you select *By User Group*for *Description*. Select the user group of which you want to record the calls. You can add a new group or modify an existing one. For more information, see Creating user groups on page 180.
	Trunk	This option appears if you select *By Trunk* for *Description*. Select the trunk of which you want to record the calls. You can add a new trunk or modify an existing one. For more information, see Configuring Trunks on page 190.
	Queue	This option appears if you select *By Queue* for *Description*. Select the call queue of which you want to record the calls. For more information, see Creating call queues and queue groups on page 216.
	Direction	This option appears if you select *By Queue* for *Description*. Select the direction of call queue of which you want to record the calls.
	Record ratio	Enter the recording percentage.
	Retention duration	Enter the days for which you want to keep the recordings.
	File name format	Select the format of the downloaded recorded call files generated under this policy. The file format is useful when you filter downloaded recorded call files by going to *Status > Storage.*

3. Click *Create*.

Archiving recorded calls

Configure the Setting to archive the recorded calls.

To configure the recording archive Setting

1. Go to *Call Feature* > *Call Recording* > *Archive.*
2. Configure the following:

GUI field		Description
Rotation Setting		
	Recording rotation size/time	Enter the recorded file rotation size and time. When the file reaches either the rotation size or time specified, whichever comes first, the archiving file is automatically renamed. The FortiVoice unit generates a new file, where it continues saving recording archives. You can access all rotated files through search.
	Archiving options when disk quota is full	Specify what the FortiVoice unit should do if it runs out of disk space. Select *Overwrite* to remove the oldest archived folder in order to make space for the new archive, or select *Do Not Archive* to stop archiving more recorded calls.
Destination Setting		
	Destination	Select an archiving destination: *Local*: the FortiVoice unit's local hard drive or a NAS server. *Remote*: a remote FTP or SFTP storage server.
	Local disk quota	If *Local* is the archiving destination, enter the disk space quota. The total disk quota for archiving calls cannot exceed 50% of the total storage disk size. For example, if the storage disk has a size of 100 GB, a maximum of 50 GB can be used for call archiving. If this quota is met and a new call must be archived, the FortiVoice unit either automatically removes the oldest call archive folder in order to make space for the new archive or stops archiving, depending on the Setting you specify under Rotation Setting on page 261.
If *Remote* is the archiving destination, configure the following:		
	Protocol	Select the protocol that the FortiVoice unit will use to connect to the remote storage server, either SFTP or FTP.
	IP address	Enter the IP address of the remote storage server.
	User name	Enter the user name of an account the FortiVoice unit will use to access the remote storage server, such as FortiVoice.
	Password	Enter the password for the user name of the account on the remote storage server.
	Remote directory	Enter the directory path on the remote storage server where the FortiVoice unit will store archived calls, such as `/home/fortivoice/call-archives`.
	Remote cache quota	Enter the FortiVoice cache quota that is allowed to be used for remote host archiving. The total cache quota for archiving calls cannot exceed 20% of the total storage disk size. For example, if the storage disk has a size of 100 GB, a maximum of 20 GB can be used for call archiving.

GUI field	Description
	If this quota is met and a new call must be archived, the FortiVoice unit either automatically removes the oldest call archive folder in order to make space for the new archive or stops archiving, depending on the Setting you specify under Rotation Setting on page 261.
Schedule	Select a schedule for the archiving.

3. Click *Apply*.

Setting the recorded file format

Select the format for recording calls. Recording bit rate is the number of bits that are conveyed or processed per unit of time.

To set the recorded file format

1. Go to *Call Feature* > *Call Recording* > *Setting.*
2. Select the format- recording bitrate: *Standard* or *Low rate*.
3. Click *Apply*.

Configuring call parking

Call park is a feature for placing a call on hold and then retrieving it from any other local extension. By default, the FortiVoice unit has 20 park orbits, 301–320.

To view the parked calls, see Viewing parked calls on page 24.

To configure call parking

1. Go to *Call Feature* > *Call Parking* > *Call Parking.*
2. For *Park call number*, enter the number to dial to park a call. The default is 300.
   For example, if you enter 300, depending on the phone, when a user receives a call and wants to park it, the user may:
   - Press *1300.
     The FortiVoice unit selects the first available park orbit (301–320). The user hears a confirmation indicating the caller has been parked successfully and into which park orbit.
     By default, dialing *1 and then 300 parks a call.
   - Provide the park orbit to the person with the parked call through paging or other means (e.g. “Mary, there is a call parked for you in 301”. Mary can then pick up any phone and dial 301 to retrieve the parked call.).
3. For *Park line start*, enter the starting park orbit. The default is 301.
4. For *Park line end*, enter the ending park orbit. The default is 320.
5. For *Parking time out*, enter the time, in seconds, to time out the parked call. The default is 60 seconds.
6. For *Music on hold*, select the music on hold file to play while the call is place on hold. Click *Edit* to modify the selected file or click *New* to configure a new one. For more information on music on hold, see Managing phone

audio settings on page 110.

7. Click *Apply*.

Configuring fax

The FortiVoice unit supports fax in the following ways:

- Use the FortiVoice unit to send and receive faxes. The FortiVoice unit contains a full featured fax server that is able to receive faxes and forward them in PDF format to an extension's user web portal or a user's email. End users can log into their web portal to view the faxes and upload PDF or JPEG files to send faxes. For configuration information, see Receiving faxes on page 263 and Sending faxes on page 264.
- If you want to continue using your fax machine with the VoIP phone system, connect the fax machine to an adapter (such as OBIHAI OBi 200, Cisco SPA 112, or Grandstream HT 702) that supports T.38 first before connecting to the FortiVoice unit. T.38 is a protocol designed to allow fax to travel over a VoIP network.

  In this case, the fax machine is treated like an extension. The FortiVoice unit receives faxes and relays them to the fax machine. Faxes sent from the fax machine will follow the fax sending dial plans.

  To use this option, you need to create and enable the fax extensions first. You then need to configure the FortiVoice unit to receive and relay the faxes to the fax machine. See Configuring fax extensions on page 170, Receiving faxes on page 263 and Sending faxes on page 264.
- With FortiVoice 200D-T, if you want to use your existing analog phone line, connect the fax machine directly to the FXS port. Make sure that the fax function is enabled when configuring the analog extension. See Modifying analog extension (200D-T, 1000E-T, and 20E2 models only) on page 167.

This topic includes:

- Receiving faxes on page 263
- Sending faxes on page 264
- Archiving faxes on page 268
- Configuring other fax settings on page 269

Receiving faxes

Configure the FortiVoice unit to receive faxes over the VoIP network and forward the faxes to extensions or emails. You can configure one or more faxes to meet the needs of different departments, for example.

To configure receiving faxes

[NG - Double-check the step numbering.]

1. Go to *Call Feature > Fax > eFax Account* and click *New.*
2. Configure the following:

GUI field		Description
Incoming Fax Setting		
	Name	Enter a name for the receiving fax configuration.
	Number	Enter an extension for this fax. This is where the incoming faxes go to.

GUI field		Description
	Display name	Enter the name displaying on the extension.
	Enable	Select to activate this fax.
	Description	Enter any notes for the incoming fax Setting.
External Numbers		Map the DID numbers to the extension of the fax. Incoming faxes to the DIDs will all reach the extension. For information on DID, see Mapping DIDs on page 209. To map the DID numbers: **1.** Click *New*. **2.** Select *Enable* to activate this DID mapping. **3.** Select the trunk used for dialing the DIDs. **4.** Enter the DID number that you want to map to an extension. **5.** Click *Create*.
Select Fax Monitors		Select the users that can monitor the faxes received on this fax extension in their FortiVoice user web portal and can choose to view, delete, resend, forward, or download the faxes. The selected users will also receive email notifications when a fax is received if their extensions are linked with email addresses. The notification will also have a PDF attachment of the fax if their extensions are configured with email notification attachment option. For more information, see Setting extension user preferences on page 173. This is useful if you have a fax that serves several departments.
Fax to Email		Enter the email addresses to receive the faxes sent to this extension. Users will receive the faxes in PDF format. You may customize the email template. For details, see Customizing call report and notification email templates on page 106.
Relay to Fax Machine		Select the fax machines connected to the FortiVoice unit via T.38 adapters. Faxes will be relayed to the selected machines.
Archive		Select *Fax archive* to activate fax archiving and enter the file name to archive following the formats in the drop-down list. To view faxes sent and received through the FortiVoice unit, see Viewing archived faxes on page 36.

3. Click *Create*.

Sending faxes

Configure the dial plans for sending faxes. The dialed fax numbers matching the configured number pattern will be subject to the call handling actions.

The fax sending dial plans will not interfere with phone call dial plans since the FortiVoice unit deals with the dial plans separately.

For information on dial plans, see Configuring Call Routing on page 205.

You send faxes in the user web portal. Senders will receive email notifications when a fax is sent if their extensions are linked with email addresses. The notification will inform if the fax has been successfully sent and have a PDF attachment of the fax if their extensions are configured with email notification attachment option. For more information, see Setting extension user preferences on page 173.

In addition, senders can always view the status of the fax sent in their FortiVoice user web portal. For more information, see the online help of the web user portal.

To view the outbound dial plans, go to *Call Feature > Fax > Sending Rule.*

GUI field	Description
Test	Select to test if the dial plan is created successfully. For more information, see Testing dial plans for sending faxes on page 265.
Enabled	Select to activate this dial plan.
Name	The name of the dial plan.
Pattern	The phone number pattern in the dial plan that matches other numbers. For details, see Dialed Number Match on page 265.
Call handling	The call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern. For details, see Call Handling on page 265.

To set up a fax sending dial plan

1. Go to *Call Feature > Fax > Sending Rule.*
2. Click *New*.
3. Configure the following:

GUI field	Description
Name	Enter a name for this plan.
Enable	Select to activate this dial plan.
Dialed Number Match	With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers. The dialed numbers matching this pattern will follow this dial plan rule. For information on adding a dialed number match, see Creating dialed number match on page 266.
Call Handling	Click *New* to configure the call handling action for the numbers matching the configured number pattern. For details, see Configuring call handling actions on page 267.

4. Click *Create*.

Testing dial plans for sending faxes

After you create a dial plan, you can select the dial plan and click *Test* to see if the dial plan works.

For more information, see Test on page 265.

To test a dial plan

1. Go to *Call Features > Fax > Sending Rule.*
2. Select the dial plan that you want to test and click *Test*.
3. Select *Test Call - Dry Run* or *Test Call*.
4. Configure the following:

GUI field		Description
Test Call - Dry Run		Run a system outbound dial plan test without making a real phone call.
	Destination number	Enter a destination number to call.
	From number	Enter the number from which you want to call the destination number. The FortiVoice unit will connect this number with the destination number for the test.
	Test	Click to start the dry run test and view the *Test result*.
	Reset	Click to remove the test result in order to start a new test.
Test Call		Test the dial plan by making a real phone call.
	Destination number	Enter a destination number to call.
	After call is established	Select the FortiVoice action once it calls the destination number: • *Play welcome message*: The FortiVoice unit will play a message to the destination number. • *Connect test call to number*: In the *Number* field, enter the number from which you want to call the destination number. The FortiVoice unit will connect this number with the destination number to test the trunk.
	Test	Click to start the test and view the *Test result*.
	Reset	Click to remove the test result in order to start a new test.

Creating dialed number match

You can create one extension number pattern in your dial plan that matches many different numbers for outbound calls.

The numbers matching this pattern will follow this dial plan rule.

The FortiVoice unit supports the following pattern-matching syntax:

Pattern-matching syntax

Syntax	Description
X	Matches any single digit from 0 to 9.
Z	Matches any single digit from 1 to 9.
N	Matches any single digit from 2 to 9.
[15-7]	Matches a single character from the range of digits specified. In this case, the pattern matches a single 1, as well as any number in the range 5, 6, 7.

Syntax	Description
.	Wildcard match; matches one or more characters, no matter what they are.
!	Wildcard match; matches zero or more characters, no matter what they are.

Pattern-matching examples

Pattern	Description
NXXXXXX	Matches any seven-digit number, as long as the first digit is 2 or higher.
NXXNXXXXXX	This pattern matches with areas with 10-digit dialing.
1NXXNXXXXXX	Matches the number 1, followed by an area code between 200 and 999, then any seven-digit number. In the North American Numbering Plan calling area, you can use this pattern to match any long-distance number.
011.	Matches any number that starts with 011 and has at least one more digit.

To create a dialed number match

1. Go to *Call Feature* > *Fax* > *Sending Rule*.
2. Click *New*.
3. In *Dialed Number Match*, click *New*.
4. Configure the following:

GUI field		Description
Match Pattern		Enter the number pattern for this rule (see Pattern-matching syntax on page 266 and Pattern-matching examples on page 267). Click + to add more patterns.
Modification		You can manipulate the number patterns you entered.
	Strip	Enter a number to omit dialing the starting part of a pattern. 0 means no action. For example, if your *Match Pattern* is 9XXX and *Strip* is 1, you only need to dial the last three digits for this pattern.
	Prefix	Add a number before a pattern, such as area code. For example, if your *Match Pattern* is 123XXXX and its area code is 555, you can enter 555 for the *Prefix*. When you dial a number under this pattern, you do not need to dial the area code 555.
	Postfix	Add a number after a pattern. For example, if your *Match Pattern* is 9XXX and the numbers under this pattern have been upgraded to have an additional digit 5 at the end, you can enter 5 for the *Postfix*. When you dial a number under this pattern, you do not need to dial the last digit 5.

5. Click *Create*.

Configuring call handling actions

Configure the call handling action for the numbers matching the configured number pattern.

To configure the call handling action

1. Go to *Call Feature >> Fax > Sending Rule*.
2. Click *New*.
3. In *Call Handling*, click *New*.
4. Configure the following:

GUI field	Description
Schedule	Select the FortiVoice operation schedule to implement this plan. Click *Edit* to modify the selected schedule or click *New* to configure a new one. For more information on PBX schedule, see Scheduling the FortiVoice unit on page 131.
Action	Select the call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern.
Outgoing trunk	Select the trunk for sending faxes. Click *Edit* to modify the selected trunk or click *New* to configure a new one. For more information on trunks, see Configuring Trunks on page 190.
Caller ID modification	Select the caller ID modification configuration. Click *Edit* to modify the selected configuration or click *New* to configure a new one. For more information on caller ID modification, see Modifying caller IDs on page 116.
Warning message	If you select *Allow with warning* or *Deny with warning* in the *Action* field, select the sound file for the warning. Click *Edit* to modify the selected file or click *New* to configure a new one. For more information on sound files, see Managing phone audio settings on page 110.
Delay	Optionally, if you want to discourage certain users for sending faxes, enter the call delay time in seconds.

5. Click *Create*.

Archiving faxes

Configure the Setting to archive the faxes.

To configure archiving faxes

1. Go to *Call Feature > Fax > Archive.*
2. Configure the following:

GUI field		Description
Rotation Setting		
	Fax rotation size/time	Enter the archived fax file rotation size and time. When the file reaches either the rotation size or time specified, whichever comes first, the archiving file is automatically renamed. The FortiVoice unit generates a new file, where it continues saving recording archives. You can access all rotated files through search.

GUI field		Description
	Archiving options when disk quota is full	Specify what the FortiVoice unit should do if it runs out of disk space. Select *Overwrite* to remove the oldest archived folder in order to make space for the new archive, or select *Do not archive* to stop archiving more recorded calls.
	Schedule	Select a schedule for the rotation.
Destination Setting		
	Destination	Select an archiving destination: *Local*: the FortiVoice unit's local hard drive or a NAS server. *Remote*: a remote FTP or SFTP storage server.
	Local disk quota	If *Local* is the archiving destination, enter the disk space quota. The total disk quota for archiving calls cannot exceed 20% of the total data disk size. For example, if the data disk has a size of 100 GB, a maximum of 20 GB can be used for fax archiving. If this quota is met and a new fax must be archived, the FortiVoice unit either automatically removes the oldest fax archive folder in order to make space for the new archive or stops archiving, depending on the Setting you specify under Rotation Setting on page 261.
If *Remote* is the archiving destination, configure the following:		
	Protocol	Select the protocol that the FortiVoice unit will use to connect to the remote storage server, either SFTP or FTP.
	IP address	Enter the IP address of the remote storage server.
	User name	Enter the user name of an account the FortiVoice unit will use to access the remote storage server, such as FortiVoice.
	Password	Enter the password for the user name of the account on the remote storage server.
	Remote directory	Enter the directory path on the remote storage server where the FortiVoice unit will store archived calls, such as `/home/fortivoice/call-archives`.
	Remote cache quota	Enter the FortiVoice cache quota that is allowed to be used for remote host archiving. The above statement regarding the *Local disk quota* also applied to the cache quota.

3. Click *Apply*.

Configuring other fax settings

Configure the station IDs, fax header, T.38 fax options, and fax sending queue for outgoing faxes.

To configure fax settings

1. Go to *Call Feature* > *Fax* > *Setting.*
2. Configure the following:

GUI field		Description
System station ID		Enter a station ID that shows on each fax sent from the FortiVoice unit.
System fax header		Enter a fax subject header that shows on each fax sent from the FortiVoice unit.
T.38 Fax		
	Sending Fax: Initiate a T.38 reinvite if the remote end does not	Select if the fax receiving terminal does not reply to a T.38 invitation.
	Sending/Receiving: Fallback to audio (G.711) mode on T.38 failure	Select to use G.711 mode if T.38 communication fails.
	UDPTL port start	T.38/UDPTL uses UDP as its transport protocol. Enter the UDP Transport Layer start port.
	UDPTL port end	Enter the UDP Transport Layer end port.
Send Queue		
	Max retry times	Enter the maximum number of times to resend a fax. This is useful if a fax cannot be sent due to busy lines or other reasons.
	Retry interval	Enter the time interval between fax sending retries.
	Wait time for an answer	Enter the waiting time for a “go-ahead” signal from the fax receiving terminal. After the waiting time is over, the FortiVoice unit will either retry to send the fax or stop sending it depending on the *Max retry times* configuration.

3. Click *Apply*.

Setting calendar reminder

You can schedule daily events and send event reminders. You first create a reminder record before setting up reminder events. One reminder record can contain multiple reminder events.

To schedule an event

1. Go to *Call Feature* > *Reminder* and click *New*.
2. Enter a name for the reminder.
3. Enable the reminder and add notes if required.
4. Click *Create*.
5. In the reminder list, select the reminder record you just created.

6. Click *Edit in calendar mode*.
7. Double-click a date.
8. Configure the following:

GUI field	Description
Title	Enter a name for the reminder event.
Location	Enter the location for the event.
Start time	Specify when the event starts.
Recurrence	Click *None* to configure recurrence Setting.
Description	Enter any notes as required.
Guest	Select the internal and external phone numbers to which you want to send event reminder calls.
Reminder audio	Configure the reminder audio that are sent to the selected guest phones and click *Create*. • *Default*: The reminder audio will be a beep sound. • *Customized*: Click to customize the reminder audio. For *Action*, click *Call me* to record a message from an extension; *Upload* to look for an existing reminder audio; and *Download* to save the audio file. For *Extension*, if you select *Call me* for *Action,* select the extension on which you want to record a message. • *Play*: Click to play the reminder audio file.

9. Click *Create*, then *Close*.

Modifying feature access codes

By default, the FortiVoice unit defines the following codes for users to access certain features by dialing the codes. You can go to *Call Feature > Feature Code > Vertical Service Code/Mid-Call/DTMF Code* and double-click a feature name to modify its code and description, but that does not change the mapping between the code and the feature. For example, if you change the DISA code from the default ** to 12, dialing 12 still accesses the DISA feature.

There are:

Vertical Service Codes: a sequence of digits and the signals star (*) and number sign (#) dialed on a telephone keypad or rotary dial to enable or disable certain telephony service features.

Mid-Call/DTMF Codes: allow you to hold, transfer, and conference calls by using DTMF digit codes entered on the phone.

Vertical Service Codes

GUI field	Description
Call bridge (DISA)	Direct Inward System Access (DISA) service allows external users to dial into PBX and use PBX service just like the local extensions. To use DISA, dial the PBX main number and then ** or the code you set. The PBX will prompt you to enter the account code (account code set at *PBX > Class of Service > Account code*). Once you pass authorization, you can use PBX service just like a local extension.
Check hot desk login status	Hot-desking refers to the sharing of one phone by multiple users at different time periods. Dial *10 or the code you set to check hot desk login status including login expiry time.
Hot desk user login	Hot-desking refers to the sharing of one phone by multiple users at different time periods. Each user can log into the phone by pressing *11 or the code you set and enter his extension number and voicemail PIN following the prompts.
Hot desk user logout	To log out hot desking, press *12 or the code you set.
Reset the phone to be 'unassigned' by admin	This code is used to remove the extension number of a FortiFone by the administrator. Dial *15 or the code you set on any FortiFone that connects to the FortiVoice unit and enter the phone configuration PIN. For information on setting the phone configuration PIN, see Configuring SIP phone auto-provisioning on page 91.
Reset the phone to be 'unassigned' by user	This code is used to remove the extension number of a FortiFone by the user. Dial *16 or the code you set on your FortiFone that connects to the FortiVoice unit and enter the phone configuration PIN. For information on setting the phone configuration PIN, see Configuring SIP phone auto-provisioning on page 91
Configure phone to an extension by administrator	This code is used to set an extension number for a FortiFone by the administrator. Dial *17 or the code you set on any FortiFone that connects to the FortiVoice unit and enter the phone configuration PIN. You can then enter an existing extension to set it as the extension of this phone. For information on setting the phone configuration PIN, see Configuring SIP phone auto-provisioning on page 91.
Configure phone to an extension by user	This code is used to set an extension number for a FortiFone by a phone user. Dial *18 or the code you set on your FortiFone that connects to the FortiVoice unit and enter the phone configuration PIN provided by the administrator. You can then enter an existing extension to set it as the extension of this phone.
Lookup name directory from extension	Dial *411 or the code you set to access the phone directory where you can look for an extension by entering a person’s name.

GUI field	Description
Listen/Barge on a call	Dial *50 or the code you set to monitor a call by listening to it. You also need to enter your voicemail PIN. For details, see Monitor/Recording on page 129
Agent login to all queues	Dial *61 or the code you set to log into the queues of which your extension is a member.
Agent logout from all queues	Dial *62 or the code you set to log out of the queues of which your extension is a member.
Agent login to a queue	Dial *63 or the code you set and enter your voicemail password and the queue extension to log into this queue. The voicemail password is required only if this option is selected for your extension. For more information, see Call Center on page 163.
Agent login from a queue	Dial *64 or the code you set and enter your voicemail password and the queue extension to log out of this queue. The voicemail password is required only if this option is selected for your extension. For more information, see Call Center on page 163.
Login all queue members	Dial *65 or the code you set to login all members of a queue of which your extension is a member. This is an action by the administrator.
Logout all queue members	Dial *66 or the code you set to logout all members of a queue of which your extension is a member. This is an action by the administrator.
Pause agent all queues	Dial *67 or the code you set and enter your voicemail password and the reason code to pause all queues of which this extension is a member. For information on reason codes, see Modifying agent reason code descriptions on page 235.
Unpause agent all queues	Dial *68 or the code you set and enter your voicemail password and the reason code to unpause all queues of which this extension is a member. For information on reason codes, see Modifying agent reason code descriptions on page 235.
Set call forward	Dial *71 followed by a code to set user’s call forward: 1 to enable, 0 to disable, and 9 to change the forwarding number.
User’s quick mode switch	Dial *72 followed by 1, 2, or 3 and enter your voicemail password to temporarily replace the original personal schedule with one of the three default ones. You may also modify the temporary schedule. Dial *720 to go back to the original schedule.
User’s twinning mode switch	Dial *73 followed by 1 to enable twinning and 0 to disable twinning. For information on twinning, see Twinning Setting on page 177.
Enter floating mode and make outgoing call on floating host device	This code allows you to make international or long distance calls from a floating host device which is a device (usually a phone) that allows other extensions to originate a call. Dial *74 or the code you set and dial the outgoing call number when hearing the dial tone. When you are prompted to input the code, enter the code based on the call restriction in the user privileges associated with your extension. For more information, see Floating code format on page 275.

GUI field	Description
Hotel room condition	Dial *75 or the code you set and enter a maid code to show the room condition. The maid codes include: 1: Maid present 2: Clean 3: Not clean 4: Out of service 5: To be inspected 6: Occupied/clean 7: Occupied/not clean 8: Vacant/clean 9: Vacant/not clean For information on maid codes, see Configuring hotel management settings on page 242.
Minibar notification	Dial *76 or the code you set and enter a minibar code to order room items. For information on minibar codes, see Configuring hotel management settings on page 242.
Wake-up call	Dial *77 or the code you set and enter a time for a wake-up call. The time format should be in the format of `hhmm`. For example, 15:30 is entered as 1530.
DND on	Dial *78 or the code you set to turn on the Do Not Disturb service. Callers will hear the busy sound when they dial your number.
DND off	Dial *79 or the code you set to turn off the Do Not Disturb service. Otherwise, callers will hear the busy sound when they dial your number.
Pickup any ringing extension in pickup group	As a pickup group member, you can dial *80 or the code you set on your phone to pick up a call from any ringing extension. For information on pickup groups, see Creating pickup groups on page 186.
Pickup group extension	As a pickup group member, you can dial *81 or the code you set on your phone followed by a ringing extension number to pick up a call from that extension. For information on pickup groups, see Creating pickup groups on page 186.
System schedule override	An administrator with the privilege can dial *82 followed by 1, 2, or 3 and the administrator PIN to temporarily replace the original system schedule with one of the three default ones. You may also modify the temporary schedule. Dial *820 to go back to the original schedule. See Configuring system capacity on page 107.
Internet of Things	Dial *91 or the code you set and enter the Amazon Alexa account extension to operate your FortiVoice unit through voice commands. For more information, see Configuring Internet of Things (IoT) on page 276.
Intercom	Dial *92 or the code you set and enter an extension to intercom that extension.
Prompt sound file recording	Dial *93 or the code you set and enter the prompt file ID and select the language to record your prompt file.

GUI field	Description
Voicemail direct	Dial *97 or the code you set from your own phone and then enter your voicemail password to directly access your voice mailbox.
Voicemail prompt	Dial *98 or the code you set from any extension and then enter your extension number and voicemail password to access your voice mailbox.
Operator	Dial 0 or the code you set to access the operator.
One key DND	This is for supporting the DND key on the FortiFones. Press the DND key on the FortiFone to turn DND on or off.
Page group	Enter PAGEGROUP or the code you set then the page group number to page the extension group.
Unpark	This is for supporting the Unpark key on the FortiFones. Press this key on the FortiFone to unpark a call.

Mid-Call/DTMF Codes

GUI field	Description
Blind transfer	Blind transfer serves 2 purposes: • During a call, dial *11 or the code you set and then the extension number of a second person to transfer the call to the person without talking to the person. • During a call, dial *11 and then the call parking number (default is 300) to park a call. For details, see Configuring call parking on page 262.
Attended transfer	During a call, dial *12 or the code you set and then the extension number of a second person to transfer the call to the person. Since you want to inform the second person about the call, you can have a private conversation with the person without the first person who made the call hearing it.
Start personal recording	Dial *30 or the code you set to start personal call recording. Personal recordings can be reviewed on the user web portal. Before doing so, have the agreement of the person you talk with or check your local laws regarding phone recording.
Start system recording	Dial *35 or the code you set to start system call recording. System recordings need administrator permission and can be viewed on the system administrator web GUI. Before doing so, have the agreement of the person you talk with or check your local laws regarding phone recording.
Pause system recording	Dial *36 or the code you set to pause system call recording.
Resume system recording	Dial *37 or the code you set to resume system call recording.
Cancel system recording	Dial *38 or the code you set to cancel system call recording.
Park	Dial *40 or the code you set to park a call.

Floating code format

Caller privilege	Code format
Allow	Extension number + * + extension user PIN **or** extension number + * + extension PIN (account code)
Allow with personal code	Extension number + * + extension user PIN
Allow with account code	Extension number + * + user privilege account code
Allow with account and personal code	Extension number + * + user privilege account code **or** extension number + * + extension user PIN

Configuring Internet of Things (IoT)

The FortiVoice unit integrates with Amazon Alexa which allows you to operate your FortiVoice unit through voice commands.

This option is only supported on FVE-100E and above.

This option only appears if you enable it and refresh the browser. For details, see Internet of Things on page 108.

To view the IoT accounts, go to *Call Feature > Internet of Things > IoT Account.*

GUI field	Description
Register	Select an account and click this option to register it on the IoT proxy server to start the service.
Name	The name of the account.
Extension	The extension number associated with the account.
Services	The type of the account.
Description	The comments on the account.
Status	Displays if the account has been registered on the IoT proxy server.

To configure an IoT account

1. Go to *Phone System > Setting > Miscellaneous*.
2. Select *Amazon Alexa* under *Internet of Things*, and click *Apply*.
3. Refresh your browser.
4. Go to *Call Feature > Internet of Things*.
5. Click *New* and configure the following:

GUI field	Description
Account/Email	Enter your email address as the account name.
Authorization code	Enter a password or click *Generate* to have a system generated password.

GUI field	Description
Extension	Select the extension number associated with the account. Make sure that *Internet of Things*setting is enabled in the extension's user privilege. For more information, see Configuring user privileges on page 126.
Description	Enter any notes as required.
Services	Select the *Amazon Alexa* service for the account. If you wish to use the phone to initiate requests to Alexa, select *Allow FortiVoice extension*.

6. Click *Create*.
7. If you want to automatically register this account on the IoT proxy server, click *Yes*. Otherwise, click *No*.
   The FortiVoice unit generates a link for accessing Amazon Alexa on the user web portal.

Configuring Amazon Alexa

After setting up an IoT account on the FortiVoice unit, go to the user web portal with the extension number associated with the IoT account.

To configure Amazon Alexa

1. Log into the user web portal with the extension number associated with the IoT account.
2. Go to *Internet of Things*.
3. Click the *Authorize my extension* link.
4. Accept the terms and conditions.
5. Enter your Amazon username and password or create a new one.
6. Enter your IoT account login credential.
7. Add the FortiVoice skill through Amazon.

With Amazon Alexa now configured, you can now use it in conjunction with the FortiVoice unit. To use Alexa, simply dial *91 on the extension associated with the IoT account before issuing a command.

Configuring Logs and Reports

The *Log & Report* menu lets you configure FortiVoice logging and reporting.

FortiVoice units provide extensive logging capabilities for voice incidents and system events. Detailed log information provides analysis of network activity to help you identify network issues and reduce network misuse and abuse.

Logs are useful when diagnosing problems or when you want to track actions the FortiVoice unit performs as it receives and processes phone calls.

Reports provide a way to analyze log data without manually going through a large amount of logs to get to the information you need.

This topic includes:

About FortiVoice logging

FortiVoice units can log multiple events. See FortiVoice log types on page 278.

You can select which severity level an activity or event must meet in order to be recorded in the logs. For more information, see Log message severity levels on page 279.

A FortiVoice unit can save log messages to its hard disk or a remote location, such as a Syslog server or a FortiAnalyzer™ unit. For more information, see Configuring logging on page 280. It can also use log messages as the basis for reports. For more information, see Configuring call center report profiles and generating reports on page 239.

This topic includes:

FortiVoice log types

FortiVoice units can record the following types of log messages. The Event log also contains several subtypes. You can view and download these logs from the *Logs* submenu of the *Status* tab.

Log types

Log type	Subtype	Description
System	Configuration change Admin activity System activity	Includes system and administration events, such as downloading a backup copy of the configuration. Also includes voicemail, FortiVoice unit monitoring, and DNS events.

Log type	Subtype	Description
	HA DHCP Monitor Voice mail DNS	
Generic	SMTP Activity	Includes SMTP server events.
Voice		Includes phone call events.
Fax		Includes fax events.
DTMF		Includes DTMF (Dual Tone Multi-Frequency) events.
Hotel		Includes hotel management events, such as guest check-in and check-out.
Call center	IVR	Includes call center IVR events.
	AGT	Includes call center agent events.

Avoid recording highly frequent log types such as voice logs to the local hard disk for an extended period of time. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

Log message severity levels

Each log message contains a field that indicates the severity level of the log message, such as `warning`.

Log severity levels

Levels	Description
0 - Emergency	Indicates the system has become unusable.
1 - Alert	Indicates immediate action is required.
2 - Critical	Indicates functionality is affected.
3 - Error	Indicates an error condition exists and functionality could be affected.
4 - Warning	Indicates functionality could be affected.
5 - Notification	Provides information about normal events.
6 - Information	Provides general information about system operations.
6 - Debug	Provides information useful to debug a problem.

For each location where the FortiVoice unit can store log files, you can define the severity threshold of the log messages to be stored there.

Avoid recording log messages using low severity thresholds such as Information or Notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

The FortiVoice unit stores all log messages equal to or exceeding the severity level you select. For example, if you select *Error*, the FortiVoice unit stores log messages whose severity level is *Error*, *Critical*, *Alert*, or *Emergency*.

Configuring logging

The *Log Setting* submenu includes two tabs, *Local* and *Remote*, that let you:

- set the severity level
- configure which types of log messages to record
- specify where to store the logs

You can configure the FortiVoice unit to store log messages locally (that is, in RAM or to the hard disk), remotely (that is, on a Syslog server or FortiAnalyzer unit), or at both locations.

Your choice of storage location may be affected by several factors, including the following:

- Local logging by itself may not satisfy your requirements for off-site log storage.
- Very frequent logging may cause undue wear when stored on the local hard drive. A low severity threshold is one possible cause of frequent logging. For more information on severity levels, see Log message severity levels on page 279.

For information on viewing locally stored log messages, see Viewing log messages on page 32.

This section includes the following topics:

Configuring logging to the hard disk

You can store log messages locally on the hard disk of the FortiVoice unit.

To ensure that the local hard disk has sufficient disk space to store new log messages and that it does not overwrite existing logs, you should regularly download backup copies of the oldest log files to your management computer or other storage, and then delete them from the FortiVoice unit. (Alternatively, you could configure logging to a remote host.)

You can view and download these logs from the *Log* submenu of the *Monitor* tab. For more information, see Viewing log messages on page 32.

For logging accuracy, you should also verify that the FortiVoice unit's system time is accurate. For details, see Configuring the time and date on page 72.

To configure logging to the local hard disk

1. Go to *Log & Report > Log Setting > Local*.
2. Select the *Enabled* option to allow logging to the local hard disk.

3. In *Log file size*, enter the file size limit of the current log file in megabytes (MB). The log file size limit must be between 10 MB and 1000 MB.
4. In *Log time*, enter the time (in days) of file age limit.
5. In *At hour*, enter the hour of the day (24-hour format) when the file rotation should start.
   When a log file reaches either the age or size limit, the FortiVoice unit rotates the current log file: that is, it renames the current log file (elog.log) with a file name indicating its sequential relationship to other log files of that type (elog2.log, and so on), then creates a new current log file. For example, if you set the log time to 10 days at hour 23, the log file will be rotated at 23 o'clock of the 10th day.

   Large log files may decrease display and search performance.

6. From *Log level*, select the severity level that a log message must equal or exceed in order to be recorded to this storage location.
7. From *Log options when disk is full*, select what the FortiVoice unit will do when the local disk is full and a new log message is caused, either:
   - *Do not log*: Discard all new log messages.
   - *Overwrite*: Delete the oldest log file in order to free disk space, and store the new log message.
8. In *Logging Policy Configuration*, click the arrow to review the options and enable the types of logs that you want to record to this storage location. For details, see Choosing which events to log on page 281.
9. Click *Apply*.

Choosing which events to log

Both the local and remote server configuration recognize the following events. Select the check boxes of the events you want to log.

Events logging options

System Log	Select this check box and then select specific system logs. No system types are logged unless you enable this option. • *When configuration has changed*: Log configuration changes. • *Admin login/logout event:* Log all administrative events, such as logins, resets, and configuration updates. • *System activity event*: Log all system-related events, such as rebooting the FortiVoice unit. • *HA*: Log all high availability (HA) activity. • *DHCP event*: Log DHCP server events. • *Monitor*: Log call recording, call barging, and traffic capture events. • *Voice mail event*: Log voicemail events. • *DNS*: Log DNS events.
Generic Log	Select this check box and then select specific events. No event types are logged unless you enable this option. • *SMTP:* Log SMTP relay or proxy events. • *Activity*:

Voice Log	Logs phone call events.
Fax Log	Logs fax events.
DTMF Log	Logs Dual Tone Multi-Frequency events. This option is for local log setting only.
Hotel Log	Logs hotel management events, such as guest check-in and check-out. This option is for local log setting only.
Call Center Log	Logs call center events, such as IVR and agent events. This option is for local log setting only.

Configuring logging to a Syslog server or FortiAnalyzer unit

Instead of or in addition to logging locally, you can store log messages remotely on a Syslog server or a FortiAnalyzer unit.

You can add a maximum of three remote Syslog servers.

Logs stored remotely cannot be viewed from the web-based manager of the FortiVoice unit. If you require the ability to view logs from the web-based manager, also enable local storage. For details, see Configuring logging to the hard disk on page 280.

Before you can log to a remote location, you must first enable logging. For details, see Choosing which events to log on page 281. For logging accuracy, you should also verify that the FortiVoice unit's system time is accurate. For details, see Configuring the time and date on page 72.

To configure logging to a Syslog server or FortiAnalyzer unit

1. Go to *Log & Report > Log Setting > Remote*.
2. Click *New* to create a new entry or double-click an existing entry to modify it.

GUI field		Description
Log to Remote Host		
	Enable	Select to allow logging to a remote host.
	Name	Enter a name for the remote host.
	IP	Enter the IP address of the Syslog server or FortiAnalyzer unit where the FortiVoice unit will store the logs.
	Port	If the remote host is a FortiAnalyzer unit, enter `514`; if the remote host is a Syslog server, enter the UDP port number on which the Syslog server listens for connections (by default, UDP 514).
	Level	Select the severity level that a log message must equal or exceed in order to be recorded to this storage location. For information about severity levels, see Log message severity levels on page 279.
	Facility	Select the facility identifier that the FortiVoice unit will use to identify itself when sending log messages.

GUI field	Description
	To easily identify log messages from the FortiVoice unit when they are stored on a remote logging server, enter a unique facility identifier, and verify that no other network devices use the same facility identifier.
CVS format	Enable this option if you want to send log messages in comma-separated value (CSV) format. Do not enable this option if the remote host is a FortiAnalyzer unit. FortiAnalyzer units do not support CSV-formatted log messages.
Logging Policy Configuration	Click the arrow to review the options and enable the types of logs you want to record to this storage location. For details, see Choosing which events to log on page 281.

3. Click *Create*.
4. If the remote host is a FortiAnalyzer unit, confirm with the FortiAnalyzer administrator that the FortiVoice unit was added to the FortiAnalyzer unit's device list, allocated sufficient disk space quota, and assigned permission to transmit logs to the FortiAnalyzer unit. For details, see the *FortiAnalyzer Administration Guide*.
5. To verify logging connectivity, from the FortiVoice unit, trigger a log message that matches the types and severity levels that you have chosen to store on the remote host. Then, on the remote host, confirm that it has received that log message.
   For example, if you have chosen to record event log messages to the remote host and if they are more severe than *Information*, you could log in to the web-based manager or download a backup copy of the FortiVoice unit's configuration file in order to trigger an event log message.

   If the remote host does not receive the log messages, verify the FortiVoice unit's network interfaces (see Configuring the network interfaces on page 39 and About the management IP on page 38) and static routes (see Configuring static routes on page 42), and the policies on any intermediary firewalls or routers. If ICMP ECHO (ping) is enabled on the remote host, you can use the `execute traceroute` command to determine the point where connectivity fails.

Configuring report profiles and generating reports

The *Log & Report* > *Call Report* > *Call Report*tab displays a list of call center report profiles.

A report profile is a group of Setting that contains the report name, its subject matter, its schedule, and other aspects that the FortiVoice unit considers when generating reports from call center log data. The FortiVoice unit presents the information in tabular and graphical format.

You can create one report profile for each type of report that you will generate on demand or on a schedule.

Generating reports can be resource intensive. To avoid phone processing performance impacts, you may want to generate reports during times with low traffic volume, such as at night. For more information on scheduling the generation of reports, see Configuring report email notifications on page 285.

To view and configure report profiles

1. Go to *Log & Report > Call Report > Call Report*.

GUI field	Description
Generate	Select a report and click this button to generate a report immediately. See Generating a report manually on page 286.
View Reports	Click to display the list of reports generated by the FortiVoice unit. You can delete, view, and/or download generated reports. For more information, see Viewing generated reports on page 31.
Report Name	Displays the name of the report profiles.
Schedule	Displays the frequency with which the FortiVoice unit generates a scheduled report. If the report is designed for manual generation, *Not Scheduled* appears in this column.

2. Click *New* to add a profile or double-click a profile to modify it.
3. In *Name*, enter a name for the report profile.
   Report names cannot include spaces.
4. Enter the *Time period* for the report.
5. Click the arrow next to each option, and configure the following as needed:
   - Configuring the report query selection on page 284
   - Configuring the report query selection on page 284
   - Configuring the report query selection on page 284
   - Configuring report profiles and generating reports on page 283
   - Generating a report manually on page 286
6. Click *Create*.

Configuring the report query selection

When configuring a report profile, you can select the queries that define the subject matter of the report.

Each report profile corresponds to a chart that will appear in the generated report.

To configure the report query selection

1. Go to *Log & Report > Call Report > Call Report*.
2. Click *New*.
3. Expand *Query List* and click *New*.

4. Configure the following:

GUI field	Description
Name	Enter a name for this query.
Category	Select a query type for the report profile. The report chart will correspond to the type selected.
Subcategory	Select a sub query type for the report profile. The report chart will correspond to the type selected.
From	Select to include the source of the incoming calls: *Internal*, *External*, or *Any*.
To	Select to include the source of the outgoing calls: *Internal, External,* or *Any*.
Region	Select the call region, such as international or long-distance.
Report column	Select the source of the call statistics: from caller or receiver.
Sort column	Select the value for filtering the call information. The caller or receiver with the higher value moves to the top of the table. If you select Report column, the sort column value is equal to what you select in the Report column field.

5. Click *Create.*

Configuring report email notifications

When configuring a report profile, you can have the FortiVoice unit email an attached copy of the generated report, in either HTML or PDF file format, to designated recipients.

You can customize the report email notification. For more information, see Customizing call report and notification email templates on page 106.

To configure an email notification

1. Go to *Log & Report* > *Call Report* > *Call Report*.
2. Expand *Email*.
3. In the *Fileformat* field, select the format of the generated attachment, either *HTML*, *PDF* or *CSV*.
4. Enter the email address of the person who will receive the report notification in the *Email address* field and click >> to add it. Enter more email addresses if necessary. Select an email address and click << to remove it.

Configuring the report schedule

When configuring a report profile, you can select when the report will generate. Or, you can leave it unscheduled and generate it on demand. See Generating a report manually on page 286.

To configure the report schedule

1. Go to *Log & Report > Call Report > Call Report*.
2. Expand *Schedule*.
3. Configure the following:

GUI field	Description
Type	• *None*: Select if you do **not** want the FortiVoice unit to generate the report automatically according to a schedule. If you select this option, the report can only be generated on demand. See Generating a report manually on page 286. • *Daily*: Select to generate the report each day. Also configure *Hour*. • *Weekdays*: Select to generate the report on specific days of each week, then select those days in *These weekdays*. Also configure *Hour*. • *Dates*: Select to generate the report on specific date of each month, then enter those date numbers in *These days*. Also configure *Hour*.

You can choose the call rate for calculating the phone bills. For information on setting the call rates, see Configuring report profiles and generating reports on page 283.

To choose the call rate

1. Go to *Log & Report > Call Report > Call Report*.
2. Expand *Rate Setting*.
3. Select an available rate and click ->.

   Only one call rate is allowed per report.

Generating a report manually

You can always generate a report on demand whether the call center report profile includes a schedule or not.

To manually generate a report

1. Go to *Log & Report > Call Report > Call Report*.
2. Click to select the report profile whose Setting you want to use when generating the report.
3. Click *Generate*.
   The FortiVoice unit immediately begins to generate a report. To view the resulting report, see Viewing generated reports on page 31.

The *Log & Report > Call Report > Rate* tab lets you set call rates for calculating phone bills.

To set call rates

1. Go to *Log & Report > Call Report > Rate* and click *New*.
2. Configure the following:

GUI field	Description
Name	Enter a name for the rating profile.

GUI field	Description
Trunk	Select the trunk that will use the rates.
Local	Enter the rate for local phone calls.
Long distance	Enter the rate for long-distance phone calls.
International	Enter the rate for international phone calls.
Other rate	Enter the rate for other types of phone calls.

3. Click *Create*.

Submitting CDRs to a database

If you have a remote third party database, you may submit the Call Detail Records (CDR) to the database. Each CDR contains the full life cycle of a call. Using the database's interface, you can display and review the CDRs.

To enable CDR submission, make sure to select *Remote CDR name*. For more information, see Setting up an IVR on page 226.

This section includes the following topics:

- Configuring CDR submission on page 287
- Modifying CDR templates on page 289
- Creating CDR filters on page 289

Configuring CDR submission

The *Log & Report* > *CDR* > *Submit CDR* submenu lets you configure sending CDR to a database. The configuration values should match those of the database server.

To submit a CDR

1. Go to *Log & Report* > *CDR* > *Submit CDR.*
2. Click *New* and configure the following:

GUI field	
Name	Enter a name for the configuration.
Status	Select to enable the configuration.
Description	Click to enter any notes you have for the configuration.

GUI field		
Remote RESTful Server		Configure the database to which CDRs are submitted. For more information, see Configuring RESTful service on page 231.
	Protocol	Select the protocol used for information transmission between the FortiVoice unit and the database server.
	HTTP headers	Select *Click to edit* to enter a HTTP header for sending information to the database server.
	HTTP timeout	Enter the time allowed for the submission to be processed. The range is 1-60 minutes.
	Authentication	*Password*: Select to enter the user name and password for logging onto the restful server. • *Username*: Enter the login user name registered on the restful server. • *Password*: Enter the login password registered on the restful server. • *URL*: Enter the URL of the server hosting restful service. • *SSL verification*: Select if required. *OAuth*: Select to use Open Authorization to access the restful server without exposing your account credential. • *Service format*: Select Salesforce or other restful services configuration format. • *Username*: Enter the login user name registered on the restful server. • *Password*: Enter the login password registered on the restful server. • *Login server*: Enter the IP address of the restful server. • *Client ID*: Enter the consumer key from the restful server. • *Client secret*: Enter the consumer secret from the restful server. If you choose Salesforce as *Service Format*, enter the consumer key and the token from the server in the format of <consumer key><token>. For information on FortiVoice and Salesforce integration, see *Salesforce Integration with FortiVoice Enterprise Technical Note*. • *URL suffix*: Enter the Salesforce object name, for example, /query/, and click *Get Salesforce API URI* to populate the *Base URL* field. Note the leading and trailing "/" must be entered before and after the object name. This option is only available if you choose *Salesforce* for *Service format*. • *URL*: Enter the URL of the server hosting restful service. • *SSL verification*: Select if required.
Options		
	CDR template	Click *Edit* to customize the default CDR submission template based on the requirements of the database server. Click *OK* when it is done.

GUI field		
		For more information, see Modifying CDR templates on page 289.
	CDR filter	Choose or create a new CDR filter to screen CDRs submitted to the database. For more information, see Creating CDR filters on page 289.
Custom value		Click *New* to add a custom value (a token, for example) that is required by the database server for information exchange.

3. Click *Create*.

Modifying CDR templates

When configuring CDR submission, you need to customize the default CDR submission template based on the requirements of the database server.

To modify a CDR template

1. Go to *Log & Report > CDR > CDR Template.*
2. Select the default CDR template and click *Edit*.
3. Modify the template and click *OK*.

Creating CDR filters

You can use filters to limit the amount of CDRs submitted to the database.

To create a CDR filter

1. Go to *Log & Report > CDR > CDR Filter.*
2. Click *New*.
3. Enter a name for the filter.
4. Using XML, enter the CDR filters based on the values you want, such as call queues or call IDs and so on.
5. For *Description*, enter any notes you have for the filter.
6. Click *OK*.

Configuring Station Messaging Detail Record (SMDR)

FortiVoice SMDR component provides FortiVoice call detail records to third party devices on certain communication and format protocols based on third party's device requirements. For example, Property Management System (PMS) uses the FortiVoice SMDR to manage hotel guest call charges.

Configuring FortiVoice SMDR requires advanced SMDR knowledge and should be performed by advanced administrative users and field engineers.

This section contains the following topics:

- Configuring SMDR settings on page 290
- Setting SMDR formats on page 290

Configuring SMDR settings

Configure SMDR Setting to enable the FortiVoice communications with third party devices.

To configure SMDR settings

1. Go to *Log & Report > SMDR Setting > SMDR*.
2. Select *Enabled* to activate the FortiVoice SMDR function.
3. Select a format protocol for the FortiVoice communications with the third party devices.
   For information on format, see Setting SMDR formats on page 290.
4. For *Port*, enter the port number that connects to the third party devices.
5. For *Max clients*, enter the number of third party devices to which the FortiVoice unit provides SMDR. The range is 1-10.
6. For *Trusted hosts*, enter the IP address and netmask of the third party device.
   If you have multiple third party devices, you may enter up to 10 trusted hosts.
7. Click *Apply*.

Setting SMDR formats

To communicate with third party devices, the FortiVoice SMDR format needs to be defined based on the device requirements so that the devices can recognize the FortiVoice SMDR.

The FortiVoice unit provides example XML SMDR format files. You can modify the files to meet with your needs. The following is an example format file:

Example SMDR format file

```
<smdr_type id="Fortivoice">
      <discard_filter>
            <field name="Disposition" value="NO ANSWER"/>
      </discard_filter>
      <formatting>
            <field name="UniqueID" length="20"/>
            <field name="StartTime" length="20"/>
            <field name="EndTime" length="20"/>
            <field name="SourceForti" length="10"/>
            <field name="DestinationForti" length="10"/>
            <field name="Duration" length="8"/>
            <field type="text" value="@"/>
            <field type="line_break"/>
            <field type="line_break"/>
      </formatting>
</smdr_type>
```

An SMDR format is composed of parts as shown in the above example:

- *smdr_type id*: the name of the SMDR format file.
- *discard_filter*: the data you do not want to send to the third party devices.
- *formatting*: the body of the SMDR format file in the form of field values (for example, *<field name="AnswerTime"/>*), plus the field lengths (for example, *length="13"*) required by the third party devices.

To set a SMDR format

1. Go to *Log & Report > SMDR Setting > SMDR Format*.
2. Click *New*.
3. Click *FortiVoice SMDR field* to display the complete list of FortiVoice SMDR field names.
4. Enter a name and description for the format.
5. For *Content derived from*, select an existing format as a base for configuring the new format.
6. In the *Content* field, follow the SMDR format requirements of the third party device and the example format file above, choose the displayed FortiVoice field names you need to set your SMDR format.
7. Click *Create*.
8. If errors appear, click *SMDR XML Types* to view the Fortinet SMDR format file and correct your format file accordingly.

Configuring alert email

The *Alerts* submenu lets you configure the FortiVoice unit to notify selected users (including administrators) by email when specific types of events occur and are logged. For example, if you require notification about system activity event detections, you can have the FortiVoice unit send an alert email message whenever the FortiVoice unit detects a system activity event.

To set up alerts, you must configure both the alert email recipients (see Configuring alert recipients on page 291) and which event categories will trigger an alert email message (see Configuring alert categories on page 292).

Alert email messages also require that you supply the FortiVoice unit with the IP address of at least one DNS server. The FortiVoice unit uses the domain name of the SMTP server to send alert email messages. To resolve this domain name into an IP address, the FortiVoice unit must be able to query a DNS server. For information on DNS, see Configuring DNS on page 43.

You can customize the alert email. For more information, see Customizing call report and notification email templates on page 106.

This section contains the following topics:

- Configuring alert recipients on page 291
- Configuring alert categories on page 292

Configuring alert recipients

Before the FortiVoice unit can send alert email messages, you must create a recipient list.

To configure recipients of alert email messages

1. Go to *Log & Report > Alert > Configuration*.

GUI field	Description
Test (button)	Clicking on the button will send a test alert email to all configured recipients in the list.
Alert Email Account	Displays the names of email accounts receiving email alerts.

2. Click *New* to add the email address of a recipient.
   A single-field dialog appears.
3. In *Email to*, enter a recipient email address.
4. Click *Create*.
5. To add more users, repeat the previous steps.

Configuring alert categories

Before the FortiVoice unit can send alert email messages, you must specify which events cause the FortiVoice unit to send an alert email message to your list of alert email recipients (see Configuring alert recipients on page 291).

To select events that will trigger an alert email message

1. Go to *Log & Report > Alert > Categories*.
2. Select one or more of the following event categories check boxes:

GUI field	Description
Critical events	Send an alert email message when the FortiVoice unit detects a system error that may affect its operation.
Disk is full	Send an alert email message when the hard disk of the FortiVoice unit is full.
HA events	Send an alert email message when any high availability (HA) event occurs.
Archive quota is exceeded	Send an alert email message when the recorded call archiving account reaches its quota of hard disk space. For information about recorded call archiving account quota, see Archiving recorded calls on page 260.
Deferred emails # over	Send an alert email message if the deferred email queue contains greater than this number of email messages. Enter a number between 1 and 10 000 to define the alert threshold, then enter the interval of time between each alert email message that the FortiVoice unit will send while the number of email messages in the deferred email queue remains over this limit.
RESTful service alert	Send an alert email message if the RESTful server does not respond to FortiVoice inquiries. Enter the interval of time between each alert email message that the FortiVoice unit will send while the RESTful server does not respond to FortiVoice inquiries.
Daily call summary	Send an alert email with a daily call summary including the number of total calls, long distance calls, and international calls.

GUI field	Description
	You need to enter the time for generating the summary which is for the 24 hours period prior to the time you set. For example, if you set 9 for *Schedule at hour*, the summary will be for the period from 9am of the previous day to 9am of the day when you receive the alert email.
PRI alarm	Send an alert email when the PSTN digital line has a problem. This option is not available for every FortiVoice model.
FXO alarm	Send an alert email when the PSTN analog line has a problem. This option is not available for every FortiVoice model.
Trunk lines are saturated	Send an alert email when the SIP/PSTN/PRI trunk lines are fully occupied. SIP trunk alert only works if you select *Overflow check* when configuring SIP trunk. See Setting up VoIP trunks on page 190.
Massive SIP authentication failure	Send an alert email when big scale SIP authentication sessions fail.
SIP trunk/office peer connectivity alert	Select the trunks of which an alert email is sent when a trunk has an issue. Also set the time interval for sending alert email in seconds.

3. Click *Apply*.

Installing firmware

Fortinet periodically releases FortiVoice firmware updates to include enhancements and address issues. After you have registered your FortiVoice unit, FortiVoice firmware is available for download at http://support.fortinet.com.

New firmware can also introduce new features which you must configure for the first time.

For information specific to the firmware release version, see the Release Notes available with that release.

In addition to major releases that contain new features, Fortinet releases patch releases that resolve specific issues without containing new features and/or changes to existing features. It is recommended to download and install patch releases as soon as they are available.

Before you can download firmware updates for your FortiVoice unit, you must first register your FortiVoice unit with Fortinet Technical Support. For details, go to the Fortinet Technical Support website and log in to your existing account or register for an account.

This section includes:

- Testing firmware before installing it on page 294
- Installing firmware on page 295
- Performing a clean firmware installation on page 300

Testing firmware before installing it

You can test a new firmware image by temporarily running it from memory, without saving it to disk. By keeping your existing firmware on disk, if the evaluation fails, you do not have to re-install your previous firmware. Instead, you can quickly revert to your existing firmware by simply rebooting the FortiVoice unit.

To test a new firmware image

1. Connect your management computer to the FortiVoice console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
2. Initiate a connection from your management computer to the CLI of the FortiVoice unit. Requires login as “admin” or an administrator with read and write privileges to the system configuration?
3. Connect port1 of the FortiVoice unit directly or to the same subnet as a TFTP server.
4. Copy the new firmware image file to the root directory of the TFTP server.
5. Verify that the TFTP server is currently running, and that the FortiVoice unit can reach the TFTP server.
   To use the FortiVoice CLI to verify connectivity, enter the following command:
   ```
   execute ping 192.168.2.99
   ```
   where `192.168.2.99` is the IP address of the TFTP server.
6. Enter the following command to restart the FortiVoice unit:
   ```
   execute reboot
   ```

7. As the FortiVoice units starts, a series of system startup messages are displayed.

```
Press any key to display configuration menu........
```

You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiVoice unit reboots and you must log in and repeat the `execute reboot` command.

---

8. Immediately press a key to interrupt the system startup.
   If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[I]: Configuration and information.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter G,F,B,I,Q,or H:
```

9. Type `G` to get the firmware image from the TFTP server.
   The following message appears:

```
Enter TFTP server address [192.168.2.99]:
```

10. Type the IP address of the TFTP server and press Enter.
    The following message appears:

```
Enter Local Address [192.168.2.99]:
```

11. Type a temporary IP address that can be used by the FortiVoice unit to connect to the TFTP server.
    The following message appears:

```
Enter File Name [image.out]:
```

12. Type the firmware image file name and press Enter.
    The FortiVoice unit downloads the firmware image file from the TFTP server and displays a message similar to the following:

```
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]
```

13. Type `R`.
    The FortiVoice image is loaded into memory and uses the current configuration, **without** saving the new firmware image to disk.
14. To verify that the new firmware image has been loaded, log in to the CLI and type:

```
get system status
```

15. Test the new firmware image.
    - If the new firmware image operates successfully, you can install it to disk, overwriting the existing firmware, using the procedure Installing firmware on page 295.
    - If the new firmware image does **not** operate successfully, reboot the FortiVoice unit to discard the temporary firmware and resume operation using the existing firmware.

Installing firmware

You can use either the web-based manager or the CLI to upgrade or downgrade the firmware of the FortiVoice unit.

Administrators whose access profile contains *Read-Write* access in the *Others* category, such as the `admin` administrator, can change the FortiVoice firmware.

Firmware changes are either:

- an upgrade to a newer version
- a reversion to an earlier version

To determine if you are upgrading or reverting your firmware image, examine the firmware version number. For example, if your current firmware version is `FortiVoice-200D 2.00,build0082,120827`, changing to `FortiVoice-200D 2.00,build0081,120801`, an earlier build number and date, indicates that you are reverting.

Reverting to an earlier version may cause the FortiVoice unit to remove parts of the configuration that are not valid for that earlier version. In some cases, you may lose all call data and configurations.

When upgrading, there may also be additional considerations. For details, see Upgrading on page 300.

Therefore, no matter if you are upgrading or downgrading, it is always a good practice to back up the configuration and call data. For details, see Backing up configuration on page 100.

To install firmware using the web-based manager

1. Log in to the Fortinet Technical Support website.
2. Download the firmware image file to your management computer.
3. Log in to the web-based manger as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
4. Install firmware in one of two ways:
   - Go to *Monitor > System Status > Status*, and in the *System Information* area, in the *Firmware version* row, click *Update*. Click *Browse* to locate the firmware and then click *Upload*.
   - Go to *System > Maintenance > Configuration*, under *Restore Firmware*, click *Browse* to locate the firmware. Then click *Restore*.
     Your web browser uploads the firmware file to the FortiVoice unit. The FortiVoice unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.

     If you are downgrading the firmware to a previous version, the FortiVoice unit reverts the configuration to default values for that version of the firmware. You must either reconfigure the FortiVoice unit or restore the configuration file.
5. Clear the cache of your web browser and restart it to ensure that it reloads the web-based manager and correctly displays all changes.
6. To verify that the firmware was successfully installed, log in to the web UI and go to *Monitor > System Status > Status*. Text appearing in the *Firmware version* row indicates the currently installed firmware version.

To install firmware using the CLI

1. Log in to the Fortinet Technical Support website.
2. Download the firmware image file to your management computer.
3. Connect your management computer to the FortiVoice console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
4. Initiate a connection from your management computer to the CLI of the FortiVoice unit, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
5. Connect port1 of the FortiVoice unit directly or to the same subnet as a TFTP server.
6. Copy the new firmware image file to the root directory of the TFTP server.

7. Verify that the TFTP server is currently running, and that the FortiVoice unit can reach the TFTP server.
   To use the FortiVoice CLI to verify connectivity, enter the following command:
   ```
   execute ping 192.168.2.99
   ```
   where `192.168.2.99` is the IP address of the TFTP server.
8. Enter the following command to download the firmware image from the TFTP server to the FortiVoice unit:
   ```
   execute restore image tftp <name_str> <tftp_ipv4>
   ```
   where <name_str> is the name of the firmware image file and <tftp_ipv4> is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.2.99, enter:
   ```
   execute restore image tftp image.out 192.168.2.99
   ```
   One of the following messages appears:
   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```
   or:
   ```
   Get image from tftp server OK.
   Check image OK.
   This operation will downgrade the current firmware version!
   Do you want to continue? (y/n)
   ```
9. Type `y`.
   The FortiVoice unit downloads the firmware image file from the TFTP server. The FortiVoice unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.
   If you are downgrading the firmware to a previous version, the FortiVoice unit reverts the configuration to default values for that version of the firmware. You must either reconfigure the FortiVoice unit or restore the configuration file.
10. If you also use the web-based manager, clear the cache of your web browser and restart it to ensure that it reloads the web-based manager and correctly displays all tab, button, and other changes.
11. To verify that the firmware was successfully installed, log in to the CLI and type:
    ```
    get system status
    ```
12. If you have downgraded the firmware version, reconnect to the FortiVoice unit using its default IP address for port1, 192.168.1.99, and restore the configuration file. For details, see Reconnecting to the FortiVoice unit on page 297 and Restoring the configuration on page 298.
    If you have upgraded the firmware version, to verify the conversion of the configuration file, see Verifying the configuration on page 299. If the upgrade is unsuccessful, you can downgrade the firmware to a previous version.

Reconnecting to the FortiVoice unit

After downgrading to a previous firmware version, the FortiVoice unit reverts to default Setting for the installed firmware version, including the IP addresses of network interfaces through which you connect to the FortiVoice web-based manager and/or CLI.

If your FortiVoice unit has not been reset to its default configuration, but you cannot connect to the web-based manager or CLI, you can restore the firmware, resetting the FortiVoice unit to its default configuration in order to reconnect using the default network interface IP address. For more information, see Performing a clean firmware installation on page 300.

To reconnect using the CLI

1. Connect your management computer to the FortiVoice console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
2. Start HyperTerminal, enter a name for the connection and click *OK*.
3. Configure HyperTerminal to connect directly to the communications (COM) port on your computer and click *OK*.
4. Select the following port Setting and click *OK*:

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

5. Press Enter to connect to the FortiVoice CLI.
   The login prompt appears.
6. Type `admin` and press Enter twice.
   The following prompt appears:
   `Welcome!`
7. Enter the following command:
   `set system interface <interface_str> mode static ip <address_ipv4> <mask_ipv4>`
   where:
   - `<interface_str>` is the name of the network interface, such as `port1`
   - `<address_ipv4>` is the IP address of the network interface, such as 192.168.1.10
   - `<mask_ipv4>` is the netmask of the network interface, such as 255.255.255.0
8. Enter the following command:
   `set system interface <interface_str> config allowaccess <accessmethods_str>`
   where:
   - `<interface_str>` is the name of the network interface configured in the previous step, such as `port1`
   - `<accessmethods_str>` is a space-delimited list of the administrative access protocols that you want to allow on that network interface, such as `ping ssh https`

   The network interface’s IP address and netmask is saved. You can now reconnect to either the web UI or CLI through that network interface. For information on restoring the configuration, see Restoring the configuration on page 298.

Restoring the configuration

You can restore a backup copy of the configuration file from your local PC using either the web-based manager or CLI. For information about configuration backup, see Backing up configuration on page 100.

If you have just downgraded or restored the firmware of the FortiVoice unit, restoring the configuration file can be used to reconfigure the FortiVoice unit from its default Setting.

MISSING OTHER BACKUP FILES SUCH AS DATABASES AND ADDRESS BOOKS

To restore the configuration file using the web UI

1. Clear your browser's cache. If your browser is currently displaying the web-based manager, also refresh the page.
2. Log in to the web-based manager.
3. Go to *System > Maintenance > Configuration*.
4. Under *Restore Configuration*, click *Browse* to locate and select the configuration file that you want to restore, then click *Restore*.
   The FortiVoice unit restores the configuration file and reboots. Time required varies by the size of the file and the speed of your network connection.
5. After restoring the configuration file, verify that the Setting have been successfully loaded. For details on verifying the configuration restoration, see Verifying the configuration on page 299.

To restore the configuration file using the CLI

1. Initiate a connection from your management computer to the CLI of the FortiVoice unit, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
2. Connect a network interface of the FortiVoice unit directly or to the same subnet as a TFTP server.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Verify that the TFTP server is currently running, and that the FortiVoice unit can reach the TFTP server.
   To use the FortiVoice CLI to verify connectivity, enter the following command:
   ```
   execute ping 192.168.2.99
   ```
   where `192.168.2.99` is the IP address of the TFTP server.
5. Enter the following command:
   ```
   execute restore config tftp <file_name> <tftp_ipv4>
   ```
   The following message appears:
   ```
   This operation will overwrite the current Setting!
   (The current admin password will be preserved.)
   Do you want to continue? (y/n)
   ```
6. Enter `y`.
   The FortiVoice unit restores the configuration file and reboots. Time required varies by the size of the file and the speed of your network connection.
7. After restoring the configuration file, verify that the Setting have been successfully loaded. For details on verifying the configuration restoration, see Verifying the configuration on page 299.

Verifying the configuration

After installing a new firmware file, you should verify that the configuration has been successfully converted to the format required by the new firmware and that no configuration data has been lost.

In addition to verifying successful conversion, verifying the configuration also provides familiarity with new and changed features.

To verify the configuration upgrade

1. Clear your browser's cache and refresh the login page of the web-based manager.
2. Log in to the web-based manager using the `admin` administrator account.
   Other administrator accounts may not have sufficient privileges to completely review the configuration.
3. Review the configuration and compare it with your configuration backup to verify that the configuration has been correctly converted.

Upgrading

If you are upgrading, it is especially important to note that the upgrade process may require a specific path. Very old versions of the firmware may not be supported by the configuration upgrade scripts that are used by the newest firmware. As a result, you may need to upgrade to an intermediate version of the firmware first, **before** upgrading to your intended version. Upgrade paths are described in the Release Notes.

Before upgrading the firmware of the FortiVoice unit, for the most current upgrade information, review the Release Notes for the new firmware version. When downloading the firmware image file from the Fortinet Technical Support website, you can access the Release Notes.

Release Notes may contain late-breaking information that was not available at the time this guide was prepared.

Performing a clean firmware installation

Clean installing the firmware can be useful if:

- you are unable to connect to the FortiVoice unit using the web-based manager or the CLI
- you want to install firmware **without** preserving any existing configuration

a firmware version that you want to install requires a different size of system partition (see the Release Notes accompanying the firmware)

- a firmware version that you want to install requires that you format the boot device (see the Release Notes accompanying the firmware)

Unlike upgrading or downgrading firmware, clean installing firmware re-images the boot device. CS: Per Zhenwei Shang. Pending confirmation.Also, a clean install can only be done during a boot interrupt, before network connectivity is available, and therefore requires a local console connection to the CLI. **A clean install cannot be done through a network connection.**

Back up your configuration before beginning this procedure, if possible. A clean install resets the configuration, including the IP addresses of network interfaces. For information on backups, see Backing up configuration on page 100. For information on reconnecting to a FortiVoice unit whose network interface configuration has been reset, see Reconnecting to the FortiVoice unit on page 297.

If you are reverting to a previous FortiVoice version, you might not be able to restore your previous configuration from the backup configuration file.

To clean install the firmware

1. Download the firmware file from the Fortinet Technical Support website.
2. Connect your management computer to the FortiVoice console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
3. Initiate a **local console connection** from your management computer to the CLI of the FortiVoice unit, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.

4. Connect port1 of the FortiVoice unit directly to the same subnet as a TFTP server.
5. Copy the new firmware image file to the root directory of the TFTP server.
6. Verify that the TFTP server is currently running, and that the FortiVoice unit can reach the TFTP server.
   To use the FortiVoice CLI to verify connectivity, if it is responsive, enter the following command:
   `execute ping 192.168.2.99`
   where `192.168.2.99` is the IP address of the TFTP server.
7. Enter the following command to restart the FortiVoice unit:
   `execute reboot`
   or power off and then power on the FortiVoice unit.
8. As the FortiVoice units starts, a series of system startup messages are displayed.
   `Press any key to display configuration menu........`
9. Immediately press a key to interrupt the system startup.

You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiVoice unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appear:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[I]: Configuration and information.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.

Enter G,F,B,I,Q,or H:
```

10. If the firmware version requires that you first format the boot device before installing firmware, type `F`. (Format boot device) before continuing.
11. Type `G` to get the firmware image from the TFTP server.
    The following message appears:
    `Enter TFTP server address [192.168.2.99]:`
12. Type the IP address of the TFTP server and press Enter.
    The following message appears:
    `Enter Local Address [192.168.1.188]:`
13. Type a temporary IP address that can be used by the FortiVoice unit to connect to the TFTP server.
    The following message appears:
    `Enter File Name [image.out]:`
14. Type the firmware image file name and press Enter.
    The FortiVoice unit downloads the firmware image file from the TFTP server and displays a message similar to the following:
    `Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]`
15. Type `D`.
    The FortiVoice unit downloads the firmware image file from the TFTP server. The FortiVoice unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.
    The FortiVoice unit reverts the configuration to default values for that version of the firmware.

16. Clear the cache of your web browser and restart it to ensure that it reloads the web-based manager and correctly displays all tab, button, and other changes.
17. To verify that the firmware was successfully installed, log in to the CLI and type:
    `get system status`
    The firmware version number appears.
18. Either reconfigure the FortiVoice unit or restore the configuration file from a backup. For details, see Restoring the configuration on page 298.