Administration Guide

FortiVoice Phone System 7.0.6

April 10, 2025
FortiVoice Phone System 7.0.6 Administration Guide
26-706-877604-20250410

TABLE OF CONTENTS

Change log

Date	Change description
2025-02-14	Initial release of the FortiVoice Phone System 7.0.6 Administration Guide
2025-04-07	Completed minor editing changes.

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 phone 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 user 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 call center console.

This document describes how to configure and use the FortiVoice phone system.

This topic includes:

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

Product offerings

The FortiVoice phone system is available as a hardware appliance and virtual machine (VM).

Procedures in this guide are applicable to both product offerings unless otherwise specified.

For more details about the supported platforms for this release, see the FortiVoice Phone System Release Notes.

Registering your Fortinet product

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

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

For more information, see Licensing in the FortiVoice Cookbook.

Customer service and technical support

Fortinet 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, go to Fortinet Support.

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.

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 Document Library website provides the most up-to-date versions of technical documentation for Fortinet products.

Fortinet Knowledge Base

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

Feedback about Fortinet technical documentation

To provide feedback about this document, you can send an email to techdoc@fortinet.com.

Scope

The majority of procedures in this document use the GUI to configure the FortiVoice unit. A few procedures use the CLI.

Conventions

Fortinet technical documentation uses the following conventions:

- IP addresses on page 13
- Cautions and notes on page 13
- Typographical conventions on page 13

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

The following table lists the typographical conventions used in this document:

Style	Description	Example
Italic font	Used for GUI navigation.	From *Minimum log level*, select *Notification*. Go to *Phone System* > *Setting* > *Location*.

`Courier` font and indentation	Used for CLI input.	`config system dns`
		`   set primary <address_ipv4>`
		`end`

`Courier` font	Used for CLI output.	`FGT-602803030703 # get system Setting`
		`comments : (null)`
		`opmode : nat`

`Courier` font	Used for file content.	`<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>`
`Courier` font	Used for text that you type.	Type a name for the remote VPN peer or client, such as `Central_Office_1`.
Blue font	Used for hyperlinks to websites and publications.	Visit the Fortinet Support website. For details, see the FortiVoice User Portal Guide.

Style	Description	Example
<text_in_angle_brackets>	Describes a variable. Replace the <text_in_angle_brackets> with the required information for your setup. Do not type the angle brackets.	FortiVoice user portal link: https://<IP_address_or_FQDN>/voice

Connecting to the FortiVoice GUI

After physically installing the FortiVoice phone system, you need to connect to the FortiVoice GUI. Review the following table and perform the procedure that applies to your scenario.

Scenario	Procedure
You are connecting to the FortiVoice phone system for the first time.	Perform the steps in Connecting to the FortiVoice GUI using default settings on page 15.
You have reset the FortiVoice phone system configuration to its default state.	Perform the steps in Connecting to the FortiVoice GUI using default settings on page 15.
You are a returning user who has completed the basic configuration of the FortiVoice phone system.	Connect to the FortiVoice GUI using the IP address, administrative access protocol, administrator account, and password that you have already configured, instead of the default settings. Perform the steps in Connecting to the FortiVoice GUI using custom settings on page 16.

Connecting to the FortiVoice GUI using default settings

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

- A computer with an RJ-45 Ethernet network port
- An Ethernet cable
- One of the recommended web browsers:
  - Google Chrome version 132
  - Microsoft Edge version 132
  - Mozilla Firefox Standard Release version 134
  - Apple Safari version 18.2

To connect to the FortiVoice GUI

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 and a subnet mask of 255.255.255.0.
2. Using the Ethernet cable, connect the Ethernet port of the management computer to port1 of the FortiVoice phone system.
3. Start your browser and enter the default URL https://192.168.1.99/admin.
4. To support HTTPS authentication, theFortiVoice phone system ships with a self-signed security certificate, which it presents to users whenever they initiate an HTTPS connection to the FortiVoice phone system. When you connect, your browser may display two security warnings related to this certificate:

   a. 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.
   b. The certificate may belong to another website. The common name (CN) field in the certificate, which usually contains the host name of the website, does not exactly match the URL you requested. This could indicate a server identity theft, but could also simply indicate that the certificate contains a domain name while you have entered an IP address. You must manually indicate whether this mismatch is expected or not.
      Both warnings are normal for the default certificate.

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

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

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

Connecting to the FortiVoice GUI using custom settings

Connect to the FortiVoice GUI using the IP address, administrative access protocol, administrator account, and password that you have already configured, instead of the default settings.

To connect to the FortiVoice GUI using single sign on

Single sign on (SSO) allows you to connect to the FortiVoice GUI and access the user portal without having to do a second sign in.

1. Before using SSO, make sure to complete the configuration. See Configuring single sign on on page 93.
2. Start a web browser and go to the FortiVoice GUI URL.
   The URL format is `https://<IP_address>/admin`
   Where `<IP_address>` is the IP address of the FortiVoice phone system that you want to connect to.
   If the FortiVoice phone system configuration is using a non-default HTTPS port, then add :<port_number> after the IP address, for example:
   `https://<IP_address>:446/admin`.
3. Click *Single Sign On*.
4. Enter the username and password associated with your SSO account.
5. Click *Login*.

6. If the two-factor authentication is set up on FortiAuthenticator:
   a. Check your email or SMS message for the token code.
   b. Enter the token code.
   c. Click *Verify*.
7. If you want to access the user portal, click the User portal icon 👤 in the top banner.
8. From the user portal, you can go back to the FortiVoice GUI by clicking the Administrator icon 👤 in the top banner.

To connect to the FortiVoice GUI without using single sign on

1. Start a web browser and go to the FortiVoice GUI URL.
   The URL format is `https://<IP_address>/admin`

   Where `<IP_address>` is the IP address of the FortiVoice phone system that you want to connect to.

   If the FortiVoice phone system configuration is using a non-default HTTPS port, then add :<port_number> after the IP address, for example:

   `https://<IP_address>:446/admin`.
2. Enter the username and password associated with your account.
3. Click *Login*.
4. If the two-factor authentication is set up on FortiAuthenticator:
   a. Check your email or SMS message for the token code.
   b. Enter the token code.
   c. Click *Verify*.

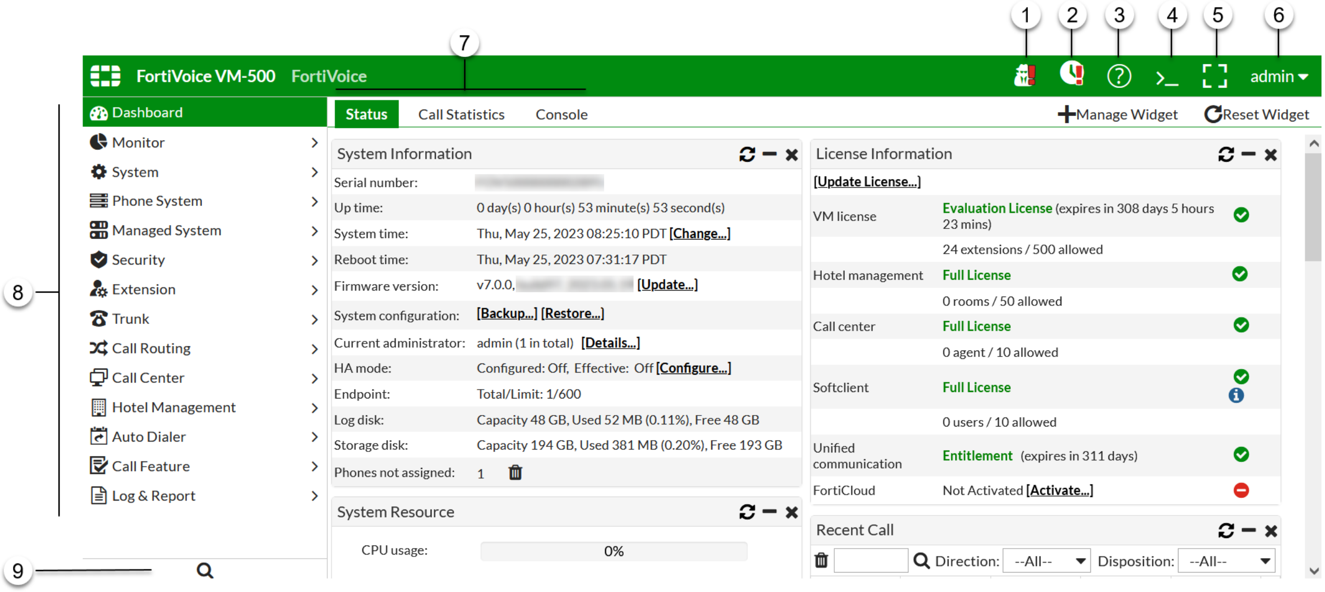
Navigating the FortiVoice GUI

To help you navigate the GUI, this section includes the following topics:

- GUI overview on page 18
- Checking the system security on page 19

GUI overview

When you connect to your FortiVoice phone system using a web browser, you access the following GUI:



System Information

Serial number:	[redacted]
Up time:	0 day(s) 0 hour(s) 53 minute(s) 53 second(s)
System time:	Thu, May 25, 2023 08:25:10 PDT [Change...]
Reboot time:	Thu, May 25, 2023 07:31:17 PDT
Firmware version:	v7.0.0, [redacted] [Update...]
System configuration:	[Backup...] [Restore...]
Current administrator:	admin (1 in total) [Details...]
HA mode:	Configured: Off, Effective: Off [Configure...]
Endpoint:	Total/Limit: 1/600
Log disk:	Capacity 48 GB, Used 52 MB (0.11%), Free 48 GB
Storage disk:	Capacity 194 GB, Used 381 MB (0.20%), Free 193 GB
Phones not assigned:	1

System Resource

CPU usage: 0%

License Information

[Update License...]

VM license	Evaluation License (expires in 308 days 5 hours 23 mins)	✓
	24 extensions / 500 allowed	
Hotel management	Full License	✓
	0 rooms / 50 allowed	
Call center	Full License	✓
	0 agent / 10 allowed	
Softclient	Full License	✓ ℹ
	0 users / 10 allowed	
Unified communication	Entitlement (expires in 311 days)	✓
FortiCloud	Not Activated [Activate...]	⛔

Recent Call

Direction: --All-- Disposition: --All--

No.	Description
1	To access the system security status and security audit details. For more information, see Checking the system security on page 19.
2	To access the phone maintenance for updating phone configurations and rebooting phones. For more information, see Maintaining phones on page 110.
3	To access the context-sensitive help (CSH) which opens the FortiVoice online documentation in HTML format. You can download the PDF file from the HTML page. You can also access the CSH by pressing the F1 key.
4	To access the CLI console.

No.	Description
5	To view the GUI in full screen mode without the top banner and menu items on the left.
6	To access the following functions: • Change password • Reboot • Shut down • Log out
7	To access the tabs associated with a selected sub-menu. The *Dashboard* > *Status* includes areas called widgets (for example, *System Information* and *License Information*).
8	Click a menu item to expand your selection and show related sub-menus.
9	The Search option allows you to search for keywords appearing in navigation menus, sub-menus, and tabs and to quickly access the configuration pages. How to search: **1.** Click the magnifying glass icon 🔍. **2.** Enter the text that you want to find. **3.** In the search results, click on a result to go to the configuration page. How to clear a search: **1.** Go to the Search option. **2.** At the end of the search field, click x.

Checking the system security

To check the system security and display security audit details, click the security alert icon 🛡 at the top right corner of the screen. If there are any security issues, the icon has a red exclamation mark.

For information about security settings, see Configuring security settings on page 176.

GUI field or button	Description
Passwords	
Password Policy	If the SIP password and user PIN policy for administrators and extension users are met, the shield icon is green. Otherwise, it is red. Click *Edit Password Policy* to set password policies. See Setting password policies on page 177.
Empty Admin Password Allowed	If a password is required in the admin password field when logging in to the system, the shield icon is green. Otherwise, it is red. For information about selecting this option, see Setting password policies on page 177.

GUI field or button	Description
Unsafe SIP Password Count	This option counts the unsafe SIP passwords for IP and fax extensions only. If any unsafe SIP passwords are found, the shield icon is red. Otherwise, it is green. Click *Password Auditor* to verify the strength of IP and fax extension passwords. See Auditing the extension passwords on page 178.
Unsafe PIN Count	This option counts the unsafe voicemail PINs for any extension type that has a voicemail PIN. If any unsafe voicemail PINs are found, the shield icon is red. Otherwise, it is green. For information about configuring extensions, see Setting up local extensions on page 183.
Unsafe User Password Count	This option counts the unsafe user passwords set in *IP Extension* > *User Setting* > *Web Access* and includes all extension types except branch page extensions. If any unsafe user passwords are found, the shield icon is red. Otherwise, it is green. For information about setting user passwords, see Configuring IP extensions on page 183.
Unaudited Password Count	This option counts the newly added extensions of which the passwords have yet to be audited. If any unaudited passwords are found, the shield icon is red. Otherwise, it is green. For information about verifying the strength of extension passwords. See Auditing the extension passwords on page 178.
Miscellaneous	
Not Assigned Phone Count	This option counts the number of phones that have not been assigned to extensions yet. If any phones without extensions are found, the shield icon is red. Otherwise, it is green. For information about assigning phones to extensions, see Configuring desk phones on page 159. Clicking the delete icon removes all not assigned phones.
Secure TFTP System	This option monitors if the system TFTP is enabled. If TFTP is enabled, the shield icon is red. If TFTP is disabled, the shield icon is green. Clicking *Edit* allows you to enable or disable the system TFTP, which also enables or disables TFTP settings in *System* > *Advanced* > *Service/Auto Provisioning*. For details, see Configuring the internal ports on page 98 and Configuring auto-provisioning for FortiFone phones and gateways on page 99.
Secure TFTP Interfaces	This option monitors if TFTP is enabled on the port interfaces. If TFTP is enabled, the shield icon is red. If TFTP is disabled, the shield icon is green. If you have TFTP enabled on multiple ports, they will be listed and you can click a link to disable it. For details, see Configuring the network interfaces on page 48.
HTTP Interfaces	This option monitors if HTTP is enabled on the port Interfaces. If HTTP is enabled, the shield icon is yellow (warning). If HTTP is disabled, the shield icon is green. If you have HTTP enabled on multiple ports, they will be listed and

GUI field or button	Description
	you can click a link to disable it. For details, see Configuring the network interfaces on page 48.
Administrator Trusted Hosts	This option monitors if trusted hosts are configured on the system administrator account. If trusted hosts are not configured, the shield icon is red. If trusted hosts are configured, the shield icon is green.
APNS Push Certificate	An iPhone running the FortiFone Softclient for iOS requires the following valid certificates on the FortiVoice phone system: • Apple Push Notification service (APNs): Used to receive notification messages. • VoIP services: Used to receive incoming calls. This option monitors those certificates. For more details, see Managing APNs and VoIP services certificates on page 107.
Send Alert (button)	Click to email the security audit details to recipients configured in *Log & Reports > Alert > Configuration*. For details, see Configuring alert email on page 344.

Configuring setups for phone users

After physically installing the FortiVoice unit and completing the configuration of the unit, you can inform your phone users about how to access the user portal and use the FortiVoice features.

The FortiVoice system provides a user 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 portal. It is included in this guide because:

- Phone users need to know how to access the FortiVoice user 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 FortiVoice user 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:

- Logging in to the user portal on page 22
- Changing the voicemail PIN on page 23
- Receiving and sending faxes on page 23
- Using the operator console on page 23
- Setting user privileges and preferences on page 23
- Setting feature codes on page 24

Logging in to the user portal

When a user has a phone extension on the FortiVoice phone system, the web-based FortiVoice user portal allows this user to perform the following tasks for their extension:

- Check the call history for received, placed, or missed calls.
- Check the voicemail including playing, deleting, forwarding, or saving voicemails.
- Manage the business and personal contacts, and view the business and corporate phone directories.
- Manage how the phone system handles phone calls.
- Check recorded calls including playing, deleting, or saving the voicemails.
- Receive and send faxes.
- Set up reminder events and invite guests.
- Add user conference call events in your calendar and invite attendees by email.
- View device details of desk phones and softclients, and set up programmable keys.
- Configure the extension according to your preferences.

- Use the operator console to process organization calls.
- Use the call center console to process call queues.

To access the FortiVoice user portal, phone users need the following information:

- FortiVoice user portal link: `https://<IP_address_or_FQDN>/voice`

  Where <IP_address_or_FQDN> is the IP address or the FQDN of the FortiVoice phone system.

  If you have changed the access port, then you must also include the port. For example: https://<IP_address_or_FQDN>:446/voice.
- Phone extension
- User password

For more information about how to log in to and use the FortiVoice user portal, see the FortiVoice User Portal Guide.

For information about adding extension numbers and user PINs, see Configuring IP extensions on page 183.

Changing the voicemail PIN

Inform the phone users how to change their default voicemail PIN. For more details, phone users can refer to the FortiVoice User Portal Guide.

Receiving and sending faxes

Inform the phone users that they can receive and send faxes using the user portal. For more information, see Configuring fax on page 315.

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 portal. For more information, see Operator Role on page 152.

Setting user privileges and preferences

The call features each phone user can use is controlled by the user privilege and preferences settings 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 151 and Setting extension user preferences on page 210.

Setting 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 324.

Using the dashboard

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

This section includes:

- Viewing the dashboard on page 25
- Viewing call statistics on page 30
- Using the CLI Console on page 30

Viewing the dashboard

Dashboard > *Status* displays first after you log in to the FortiVoice GUI. 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*.

This section includes the following topics:

- Customizing the dashboard on page 25
- System Information widget on page 26
- License Information widget on page 26
  - Uploading a license file on page 26
  - FortiCloud access on page 27
- System Resource widget on page 29
- Statistics History widget on page 29
- Service Status widget on page 30
- Recent Call widget on page 30

See also Navigating the FortiVoice GUI on page 18.

Customizing the dashboard

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, click *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.

To reset the dashboard to its default view, click *Reset Widget*.

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

System Information widget

The *Dashboard* > *Status* > *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 Managing the firmware on page 360.

Depending on your FortiVoice model, you may see *Deployment mode*. Your choices are the following:

- *PBX*: Select to assign the PBX function to your FortiVoice model.
- *Survivability Branch*: Select to assign the survivability branch function to your FortiVoice model and provide resiliency in a centralized multi-site network deployment. For more details about survivability branches, see the FortiVoice Local Survivable Gateway Deployment Guide.

The number of phones that are auto discovered but have not been assigned extensions are also displayed. If this number is abnormally high, it may mean the FortiVoice unit is under MAC address flooding attack and its performance will be compromised. You can remove the phones.

License Information widget

The *Dashboard* > *Status* > *License Information* widget displays the following details:

- VM license with last queried license statuses for the number of extensions supported, if you use a FortiVoice VM
- Hotel management, if you have purchased this option
- Call center, if you have purchased this option
- Softclient
  - To generate and access the softclient diagnostic report, click ℹ.
  - For information about configuring the FortiVoice phone system and FortiGate to use the FortiFone softclient as a remote SIP client, see the Softclient for mobile and desktop section in the FortiVoice Cookbook.)
- Active and expired entitlements
  - Unified communication
  - Enhanced call center
- FortiCloud activation to manage the FortiVoice remote access (For more information, see FortiCloud access on page 27.)

Depending on the license you have purchased, when you first access the FortiVoice GUI, you need to upload the license to enable the functions you need. For information about purchasing, registering, and uploading a license, see the Licensing section in the FortiVoice Cookbook.

This section includes the following topics:

- Uploading a license file on page 26
- FortiCloud access on page 27

Uploading a license file

1. Place the license file on your management computer.
2. Go to *Dashboard* > *Status*.
3. In the *License Information* widget, click *Update License*.
4. Browse for the license (.lic) file.

5. Select the file, and click *Open*.
6. To confirm the upload, click *Yes*.

FortiCloud access

FortiCloud provides single-pane of glass management for your Fortinet products, including your FortiVoice phone systems (hardware appliances and virtual machines). With FortiCloud enabled on your FortiVoice, remote management becomes easy and convenient because you don't have to remember various IP addresses or fully qualified domain names (FQDN) to access your FortiVoice.

For this task, complete the following sections:

- Enabling FortiCloud access for FortiVoice on page 27
- Accessing FortiVoice from FortiCloud on page 28

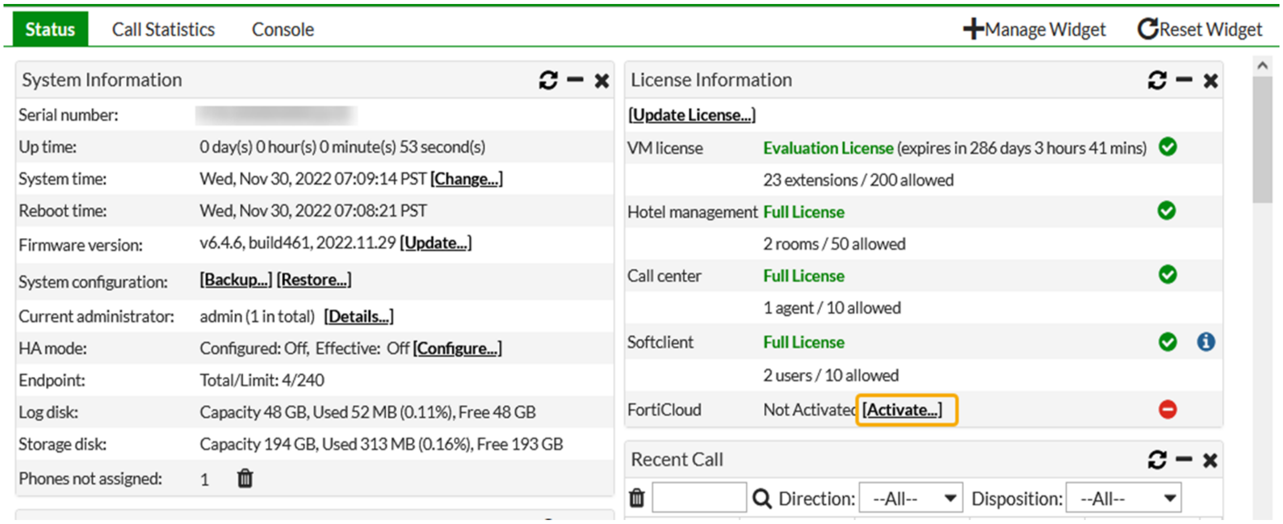
Enabling FortiCloud access for FortiVoice

Before you begin

- Make sure that you have your login credentials for your FortiCloud account. You will need them to complete the steps in this section. If you need to register for an account, go to the Fortinet Support website. For FortiCloud account details, see the New Account Onboarding document in FortiCloud Account Services.
- After purchasing your FortiVoice unit, complete the FortiVoice product registration at the Fortinet Support website. For more information, see Registering a FortiVoice product and downloading the license file in the FortiVoice Cookbook.
- Upload the license to FortiVoice. For more information, see Uploading a license file on page 26.

To enable FortiCloud access

1. In FortiVoice, go to *Dashboard > Status*.
2. In the *License Information* widget, go to *FortiCloud* and click *Activate*.



System Information

Serial number:	[redacted]
Up time:	0 day(s) 0 hour(s) 0 minute(s) 53 second(s)
System time:	Wed, Nov 30, 2022 07:09:14 PST [Change...]
Reboot time:	Wed, Nov 30, 2022 07:08:21 PST
Firmware version:	v6.4.6, build461, 2022.11.29 [Update...]
System configuration:	[Backup...] [Restore...]
Current administrator:	admin (1 in total) [Details...]
HA mode:	Configured: Off, Effective: Off [Configure...]
Endpoint:	Total/Limit: 4/240
Log disk:	Capacity 48 GB, Used 52 MB (0.11%), Free 48 GB
Storage disk:	Capacity 194 GB, Used 313 MB (0.16%), Free 193 GB
Phones not assigned:	1

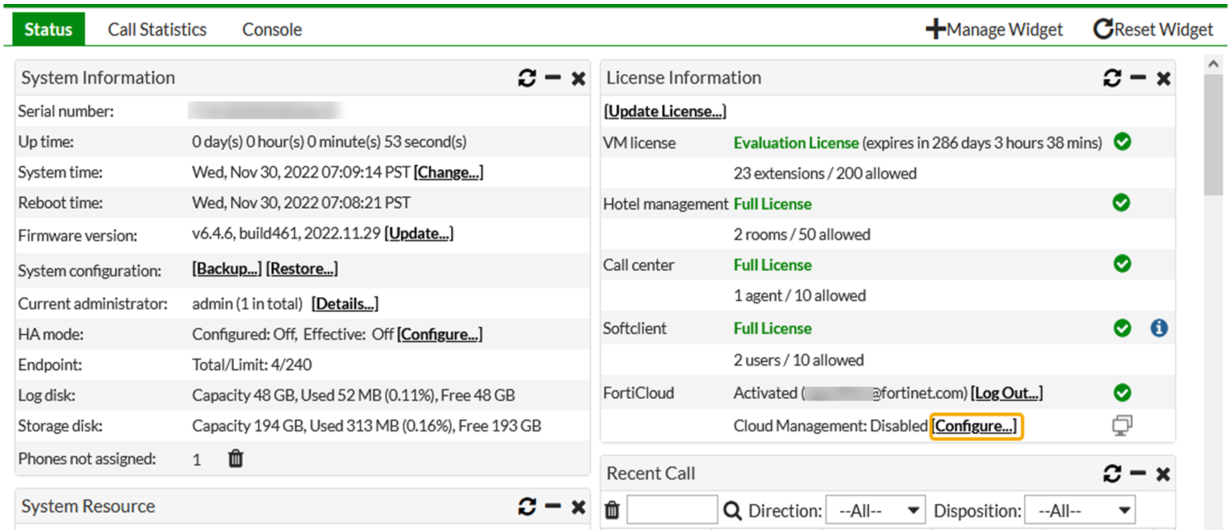
License Information

[Update License...]

VM license	Evaluation License (expires in 286 days 3 hours 41 mins)	✓
	23 extensions / 200 allowed	
Hotel management	Full License	✓
	2 rooms / 50 allowed	
Call center	Full License	✓
	1 agent / 10 allowed	
Softclient	Full License	✓ ℹ
	2 users / 10 allowed	
FortiCloud	Not Activatec [Activate...]	⛔

3. Enter the *Email* and *Password* associated with your FortiCloud account.
4. Click *OK*.
   FortiCloud shows *Activated*.
5. In the *License Information* widget, go to *Cloud Management* and make sure that it displays *Enabled*.

6. If *Cloud Management* shows *Disabled*:
   a. Click *Configure*.



System Information

Serial number:	[redacted]
Up time:	0 day(s) 0 hour(s) 0 minute(s) 53 second(s)
System time:	Wed, Nov 30, 2022 07:09:14 PST [Change...]
Reboot time:	Wed, Nov 30, 2022 07:08:21 PST
Firmware version:	v6.4.6, build461, 2022.11.29 [Update...]
System configuration:	[Backup...] [Restore...]
Current administrator:	admin (1 in total) [Details...]
HA mode:	Configured: Off, Effective: Off [Configure...]
Endpoint:	Total/Limit: 4/240
Log disk:	Capacity 48 GB, Used 52 MB (0.11%), Free 48 GB
Storage disk:	Capacity 194 GB, Used 313 MB (0.16%), Free 193 GB
Phones not assigned:	1

System Resource

License Information

[Update License...]

VM license	Evaluation License (expires in 286 days 3 hours 38 mins) ✓
	23 extensions / 200 allowed
Hotel management	Full License ✓
	2 rooms / 50 allowed
Call center	Full License ✓
	1 agent / 10 allowed
Softclient	Full License ✓
	2 users / 10 allowed
FortiCloud	Activated ([redacted]@fortinet.com) [Log Out...] ✓
	Cloud Management: Disabled [Configure...]

Recent Call

Direction: --All-- Disposition: --All--

   b. Enable *Cloud Management*.
   c. Click *OK*.
   Cloud Management shows *Enabled*.
7. Continue with Accessing FortiVoice from FortiCloud on page 28.

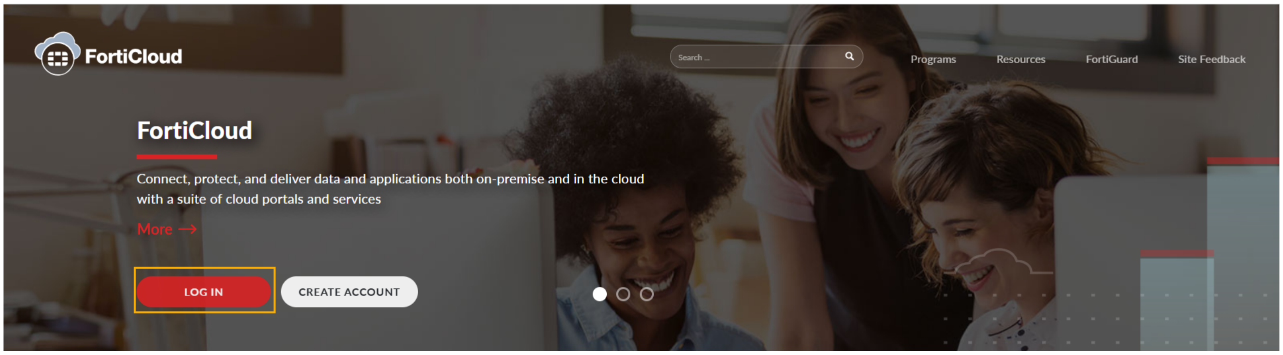
Accessing FortiVoice from FortiCloud

Before you begin

Make sure to complete Enabling FortiCloud access for FortiVoice on page 27.

To access FortiVoice from FortiCloud

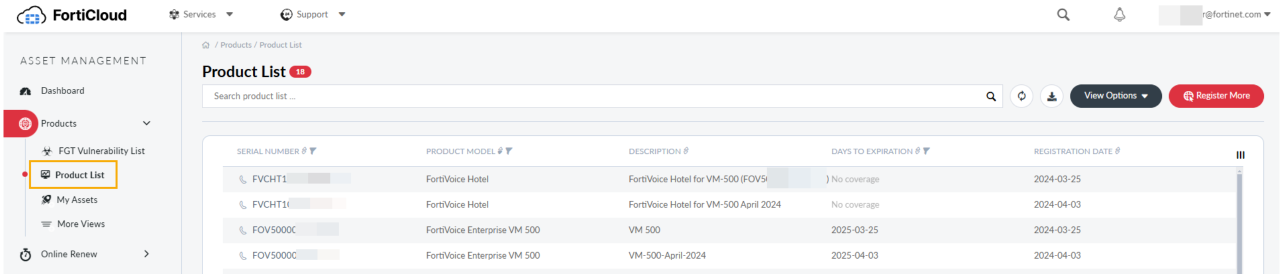
1. Go to the Fortinet Support website.
2. Click *LOG IN*.



Connect, protect, and deliver data and applications both on-premise and in the cloud with a suite of cloud portals and services

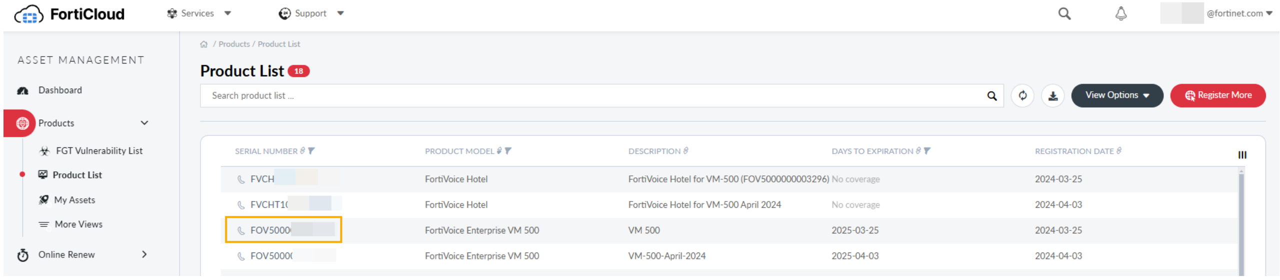
   The FortiCloud login page displays.
3. Enter the *Email* and *Password* associated with your FortiCloud account.
4. Click *LOG IN*.
5. Input your security code available in your email or token application.
6. Click *GO*.

7. Go to *Asset Management* > *Products* > *Product List*.



SERIAL NUMBER	PRODUCT MODEL	DESCRIPTION	DAYS TO EXPIRATION	REGISTRATION DATE
FVCHT1[redacted]	FortiVoice Hotel	FortiVoice Hotel for VM-500 (FOV5[redacted])	No coverage	2024-03-25
FVCHT1[redacted]	FortiVoice Hotel	FortiVoice Hotel for VM-500 April 2024	No coverage	2024-04-03
FOV5000[redacted]	FortiVoice Enterprise VM 500	VM 500	2025-03-25	2024-03-25
FOV5000[redacted]	FortiVoice Enterprise VM 500	VM-500-April-2024	2025-04-03	2024-04-03

8. In the *Serial Number* column, click the FortiVoice instance that you want to access.



SERIAL NUMBER	PRODUCT MODEL	DESCRIPTION	DAYS TO EXPIRATION	REGISTRATION DATE
FVCH[redacted]	FortiVoice Hotel	FortiVoice Hotel for VM-500 (FOV5000000003296)	No coverage	2024-03-25
FVCHT1[redacted]	FortiVoice Hotel	FortiVoice Hotel for VM-500 April 2024	No coverage	2024-04-03
FOV5000[redacted]	FortiVoice Enterprise VM 500	VM 500	2025-03-25	2024-03-25
FOV5000[redacted]	FortiVoice Enterprise VM 500	VM-500-April-2024	2025-04-03	2024-04-03

9. Scroll down to *Manage Cloud Services* and click *Remote Access*.
10. If your web browser asks you to select a certificate, click *OK*.
    The FortiVoice login dialog displays.
11. Enter the *Name* and *Password* associated with the FortiVoice admin account.
12. Click *Log In*.
    The FortiVoice GUI page opens.
13. You can start managing your FortiVoice through FortiCloud which works exactly like managing FortiVoice directly.

System Resource widget

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

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.

If there are any mismatched phones under *Generic phones* > *Mismatched*, you can click *View* to display them. For detailed information, see Viewing mismatched phones on page 36.

Statistics History widget

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

See also Viewing call statistics on page 30.

Service Status widget

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

Recent Call widget

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

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

You can access the CLI without exiting from the GUI by using one of the following methods:

- Go to *Dashboard* > *Console*.
- Go to the top banner and click >_.

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 on page 31
- Viewing extensions and devices on page 33
- Viewing call detail records on page 38
- Viewing generated reports on page 39
- Viewing log messages on page 40
- Viewing call directory on page 43
- Blocking SIP device IP addresses on page 43
- Playing recorded calls and viewing fax storage on page 44

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 on page 31
- Viewing parked calls on page 31
- Viewing conference calls on page 32
- Viewing trunk status on page 32
- Viewing the DHCP client list on page 32

Viewing active calls

Monitor > *Phone System* > *Active Call* 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 about call parking, see Configuring call parking on page 315.

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 302.

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 voice over Internet Protocol (VoIP) or the public switched telephone network (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.

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

The Registration/Connection column indicates if a trunk has been registered with or connected to the VoIP or PSTN service provider. The Registration/Connection column can show the following icons:

- ✓: The trunk is registered. ((This icon is for the SIP trunk, office peer, and gateway only.)
- : The trunk is OK. (This icon is for the PSTN only.)
- : The trunk or trunk channel has a red alarm. (This icon is for the PSTN only.)
- ☎: The trunk or trunk channel is in service. (This icon is for the PSTN only.)
- ⚠: The trunk or trunk channel has an alarm. (This icon is for the PSTN only.)

For more information, see Configuring trunks on page 229.

Viewing the DHCP client list

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

After 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 GUI) 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 53.
  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 53.
- 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 Address	The Media Access Control address (MAC address) of the DHCP client.
Interface	The FortiVoice unit port to which the DHCP client connects. For information about FortiVoice interfaces, see Configuring network settings on page 46.
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 Information	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 about assigning extensions, see Viewing desk phones on page 34.
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, desk phones, FortiFone software phones, and generic SIP phones.

This topic includes:

- Viewing extension status on page 34
- Viewing desk phones on page 34
- Viewing FortiFone softclients on page 36
- Viewing generic SIP phones on page 36
- Viewing mismatched phones on page 36
- Viewing activity details of hot desking extensions on page 36
- Viewing unmanaged gateways on page 36

Viewing extension status

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

To access the registration status of extensions, select one or more extensions and right-click to access *SIP Registration Log*.

For more information, see Configuring extensions on page 183.

Viewing desk phones

Monitor > *Extension & Device* > *Phone* lists the supported phones auto-discovered by the FortiVoice system, assigned or not assigned to any extensions.

After a phone with a *Management* status of *Not Assigned* connects to the FortiVoice system and is auto-discovered, the FortiVoice system 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 183 and Configuring user privileges on page 151.

GUI field	Description
New	Click to add a new desk phone. For details, see Configuring desk phones on page 159.
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 phone with a *Not Assigned* management 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 a Not Assigned phone on page 35. • *Assign to Existing Extension:* Select a phone with a *Not Assigned* management status and click this option to assign this phone to an existing extension. For more information, see To assign a new extension user to a Not Assigned phone on page 35. • *Assign as Auxiliary to Existing Extension:* Select a phone with a *Not Assigned* management status and click this option to assign it to an existing extension as an auxiliary device. For more information, see To assign an existing extension user to a Not Assigned phone as an auxiliary device on page 35 and Configuring IP extensions on page 183. • *View Phone Configuration*: Select a phone with an *Assigned* management status and click this option display its configuration file. If you select a Cisco phone, you can select *Enterprise* or *3PCC*. • *View accounts*: For FortiFone phones to which multiple extensions can be associated, such as FON-850/860/870 and FON-D70/D71/D72, click this option to view the associated extensions. This option is only active when a FortiFone phone has multiple extensions associated with it. • *SIP Registration Log*: View the registration status of phones. • *Export*: Select to save the extension list in CSV format.
Extension	When a phone is registered with an extension, this column shows 👤.

GUI field	Description
	Some phone models, such as the FON-D71, can have multiple registered extensions. In this case, the icon also shows the number of registered extensions. For example, 👤 2 .
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 138.
Management	Displays if the phone has been *Assigned* or *Not Assigned* to an extension.
Number	The extension number of the phone.
Display Name	The name displaying on the phone, such as John Doe.
Status	Displays if the phone is registered with the FortiVoice system. A registered phone is assigned an IP address and basic PBX setup information.
IP	The IP address of the phone assigned by the FortiVoice system.
Phone Info	The model, MAC address, and firmware version of the phone for this extension.
Last Phone Config Update	The date and time of the last configuration update that FortiVoice has completed on the phone.
Version	The firmware version that is installed on the phone.

To assign a new extension user to a *Not Assigned* phone

1. Go to *Monitor* > *Extension & Device* > *Phone*.
2. In the *Management* column, select a *Not Assigned* phone.
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 183.
5. Review the phone details and click *Next*.
6. Review the summary and click *Finish*.

To assign an existing extension user to a *Not Assigned* phone

1. Go to *Monitor* > *Extension & Device* > *Phone*.
2. In the *Management* column, select a *Not Assigned* phone.
3. Click *Action* and select *Assign to Existing Extension.*
4. Select the extension and click *Next*.
5. Review the extension details and click *Next*. For details, see Configuring IP extensions on page 183.
6. Review the phone details and click *Next*.
7. Review the summary and click *Finish*.

To assign an existing extension user to a *Not Assigned* phone as an auxiliary device

1. Go to *Monitor* > *Extension & Device* > *Phone*.
2. In the *Management* column, select a *Not Assigned* phone.
3. Click *Action* and select *Assign as Auxiliary to Existing Extension.*
4. Select the extension and click *Next*.
5. Review the extension details and click *Next*. For details, see Configuring IP extensions on page 183.
6. Review the phone details and click *Next*.
7. Review the summary and click *Finish*.

Viewing FortiFone softclients

Monitor > *Extension & Device* > *Soft FortiFone* lists the FortiFone softclients registered with the FortiVoice system.

To access the registration status of softclients, select one or more extensions and right-click to access *SIP Registration Log*.

Viewing generic SIP phones

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

Viewing mismatched phones

Monitor > *Extension & Device* > *Mismatched Phone* displays the phones of which the registration information does not match the desk phone models and has caused registration failure.

You can select a phone registration failure record and click *Delete* to remove it to avoid the confusion that the system is compromised.

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 (when a phone is identified as *Not Assigned*) 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 settings 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 about configuring hot desking, see Hot-desking on page 154.

Viewing unmanaged gateways

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

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

For detailed deployment instructions, see the applicable gateway guide:

- FortiVoice FXO Gateway Deployment Guide
- FortiVoice FXS Gateway Deployment Guide
- FortiVoice PRI Gateway Deployment Guide

GUI field	Description
Action	• *Create New Device*: Select an unmanaged gateway and click this option to add the gateway to the FortiVoice system. The gateway record disappears from the *Unmanaged Gateway* list. For more information, see To add a gateway to the FortiVoice system on page 37. • *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 38.
Serial number	The serial number of the unmanaged gateway.
Type	The gateway brand and model.
IP	The IP address of the unmanaged gateway assigned by the FortiVoice system.

To add a gateway to the FortiVoice system

1. Go to *Monitor* > *Extension & Device* > *Unmanaged Gateway*.
2. Select an unmanaged gateway.

3. Click *Action* and select *Create New Device.*

GUI field	Description
Enabled	Select to activate the gateway.
Name	Enter a unique name to identify the gateway.
Display Name	Not required. You can leave this field empty.
Hostname/IP address	Enter the hostname or IP address of the gateway. If the FXO gateway is configured to use a non-default HTTPS port, then add `:<port number>` after the IP address. For example, `192.168.1.21:4430`. • *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 gateway to get the serial number and the MAC address of the gateway. This action can confirm that the systems can communicate and that the password is valid. • *Connect Device*: This procedure does not use this button.
Admin user name	Enter the user name of the administrator account for logging in to the gateway. The default is admin.
Admin password	Enter the password associated with the Admin user name. The default is no password.
Serial number	The serial number of the gateway.
Type	The type of gateway that you are adding to the FortiVoice phone system.
MAC address	Enter the MAC address of the gateway.
Description	Optionally, add any applicable 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 detail 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, call recordings, source departments, and destination departments.

From *Monitor* > *Call History* > *Call Detail Record (CDR)*, you can perform the following actions:

- To display the detailed call information including the CDR flow, double-click on a call record.
- To filter call record entries, make choices in the *Direction*, *Disposition*, *Source Department*, and *Destination Department* drop-down lists.
- To add callers or callees to your contact list, make your selection, and use the *More Action* > *Add to Contact* drop-down list.
- To block callers or callees, make your selection, and use the *More Action* > *Block* drop-down list.
- To show a list of flagged CDR calls, use the *More Action* > *Flagged CDR* drop-down list. To save the list in the CSV format, click *Export*.
- To filter the call records display, click the *Search* button and enter criteria that records must match in order to be visible.
- To download call records, select an option under *Download*. If you enable *With call flow*, you can download call records with detailed call flow information.

To play a call recording that is using the low rate (GSM) setting, you must download that recording first and then play it. You cannot play that recording in the web browser directly.

For more information about the file format for recorded calls, see Setting the file format for recorded calls on page 309.

- To play a recorded call, verify that the call entry has a green checkmark in the *Recorded* column, click that row, and click the Play button.
- To download a recorded call, go to the *Recorded* column and click the green checkmark. FortiVoice saves the file to your local system. The file name format is: <from #>-<to #>-<yyyy-mm-dd>_<hh_mm_ss for start time>.wav. For details about feature codes for recording phone calls, see Modifying feature access codes on page 324. For more information, see the Call recording section in the FortiVoice Cookbook.

For information about allowing department administrators or managers to access CDRs associated with their department only, see the Call History section in the FortiVoice Cookbook.

See also Configuring call report profiles and generating reports on page 337.

Viewing generated reports

Monitor > *Call Report* 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 282.

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 or Call Center Report*.

GUI field or button	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, `DeptReport-2022-06-27-154900` is a report named DeptReport, generated on June 27, 2022 at 15:49:00. 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 (Byte)	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 `CallReport-2022-06-27-2112-144843`, then click *Download* and select *Download HTML*. Your browser downloads a file with an archive (`.zip`) 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 Apache OpenOffice Calc, select a report and click *Download.* On the pop-up menu, select *Download CSV*.

Viewing log messages

Monitor > *Log* 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 GUI of the FortiVoice unit. If you want to view logs from the GUI, also enable local storage. For details, see Configuring logs and reports on page 332.

For a description of activities and events displayed in the *Monitor* > *Log* tabs, see the following table.

Tab	Activity or event
System	Admin logins, password changes, firmware upgrades, call center data service, and deletion of local call recordings and unassigned phones
Generic	Logins and logouts (user portal and desktop softclient), phone configuration downloads
Voice	Voice call processing, including phone registration errors

Tab	Activity or event
Fax	Status of received and sent faxes
Queue (with call center license only)	Status of call queues and agents
Hotel (with license only)	Hotel management service and PMS connections
Call Center (with license only)	Status of agent logins and logouts, and IVR
Phone Configuration	Status of phone profile and template changes
SIP Registration Log	Phone registrations (new, expired, and refresh) and unregistrations

For information about phone configuration update and firmware upgrade jobs, see Maintaining phones on page 110.

The log messages vary by levels. For more information, see Configuring logs and reports on page 332.

The log messages are also filtered by subtypes depending on log types.

To view the log files and their contents

1. Go to *Monitor* > *Log* > *System/Generic/Voice/Fax/Queue/Hotel/Call Center/Phone Configuration/SIP Registration Log*.
   The list of the latest 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 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. See Using the right-click pop-up menus on page 42.
3. 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 42.
4. To view all log files, click *List*.
   All log files display. You can select a log file to view, delete, or download it. Click *Back* to go to the list of the latest log files.
5. 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 42.

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/Phone Configuration/SIP Registration Log*.
2. Click *Configure View*(icon) > *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/Phone Configuration/SIP Registration Log*.
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* (icon) > *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/Phone Configuration/SIP Registration Log*.
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.

GUI field	Description
	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.
Status	This field is available for searching Phone Configuration logs. Click + to select the phone configuration log status.
Date	Select the *Start time* 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 settings 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

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

Blocking SIP device IP addresses

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 about configuring security settings, see Configuring intrusion detection on page 176.

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

For auto exempt IP addresses, you may select an IP address to delete it if you find it suspicious.

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

To view the exempted IP addresses, go to *Monitor > Security > Auto Exempt IP.*

Setting the security parameters

You can use the CLI to set the threshold for blocking IP addresses and sending alert email (the default is 50 attempted logins per minute), the time interval to check the phone call activities (the default is 60 seconds), and the maximum notification emails to send after the threshold is reached (the default is 100).

```
config security sip-authentication-failure
   set threshold
   set interval
   set max-notification
end
```

Playing recorded calls and viewing fax storage

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

This topic includes:

- Playing and downloading recorded calls on page 44
- Viewing current fax accounts on page 45
- Viewing archived faxes on page 45
- Viewing fax queues on page 45

Playing and downloading recorded calls

The *Monitor* > *Storage* > *Recorded Call* lists the calls recorded by the FortiVoice unit. You can perform the following actions:

To play a call recording that is using the low rate (GSM) setting, you must download that recording first and then play it. You cannot play that recording in the web browser directly.

For more information about the file format for recorded calls, see Setting the file format for recorded calls on page 309.

- To play a recorded call, double-click a call record folder to open the archived call files. Select a call file and click the *Play* button.
- To download a recorded call, double-click a call record folder to open the archived call files. Select a call file, click the *Download* button, and select an option *(All* or *Selected Files*). FortiVoice saves the file to your local system. The file name format is: <from #>-<to #>-<yyyy-mm-dd>_<hh_mm_ss for start time>.wav.
- To search recorded calls, click *Search,* then *New*, enter the search values, and click *Create*. Note that under *Recording type*, *Conference* refers to calls recorded based on the phone numbers that are conference call numbers. *System* refers to all other type of calls recorded.

For information about configuring recording calls, see Recording calls on page 305.

For details about how to manage the recorded call access by department, see the Managing the access to phone call recordings in the FortiVoice Cookbook.

Viewing current fax accounts

Monitor > *Storage* > *Fax* lists the fax accounts created on the FortiVoice unit. For more information about creating fax accounts, see Configuring fax on page 315.

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 about the faxes it stores.

- *Forward*: Select a fax, click this option and enter the extension to which you want to forward the fax.
- *Download PDF*: Select a fax and click this option to save it.

Viewing archived faxes

Monitor > *Storage* > *Fax Archive* lists the faxes sent and received through the FortiVoice unit. For more information about fax, see Configuring fax on page 315.

To search archived fax, go to *Monitor* > *Storage* > *Fax Archive*, click *Search,* then *New*, enter the search values, and click *Create*.

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

Viewing fax queues

Monitor > *Storage* > *Fax Archive* lists the faxes waiting to be sent or having failed to be sent on the FortiVoice unit. You can download the faxes. For more information about fax, see Configuring fax on page 315.

Configuring system settings

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

This topic includes:

- Configuring network settings on page 46
- Configuring administrator accounts and access profiles on page 55
- Configuring RAID on page 59
- Using high availability on page 61
- Working with system configurations on page 80
- Configuring advanced phone system settings on page 95
- Managing certificates on page 100
- Maintaining the system on page 108

Configuring network settings

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

This topic includes:

- About IPv6 support on page 46
- About the management IP on page 47
- About FortiVoice logical interfaces on page 47
- Configuring the network interfaces on page 48
- Configuring static routes on page 51
- Configuring DNS on page 52
- Configuring DHCP server on page 53
- Capturing voice and fax packets on page 54

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 GUI and the FortiVoice user account using the management IP address. For details, see Connecting to the FortiVoice GUI 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 47
- Redundant interfaces on page 48
- Loopback interfaces on page 48

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 48.

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 48.

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 48.

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 47, and Editing network interfaces on page 49.

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 47.
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 46.
Access	Displays the administrative access and phone user access that are enabled on the network interface, such as HTTPS for the GUI.
Status	Indicates the **up** (available) or **down** (unavailable) administrative status for the network interface. • *Green check mark*: The network interface is up and can receive traffic. • *Red cross mark*: 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 49.
Referenced (icon)	Indicates if a network interface is used by other services, such as DHCP. A green dot means a network interface is used by other services. A gray dot means a network interface is not used by other services.

Editing network interfaces

You can edit the FortiVoice 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 56.

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 47. • *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, click + in the *Interface Member* field to add interface members. 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 GUI, and extension user account through this network interface. • *HTTP*: Enable to allow HTTP connections to the GUI, 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 about further restricting access, or on configuring the network interface that will be the source of traps, see Configuring the network interfaces on page 48. • *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 phones.

GUI field	Description
	This is mainly for backward support of legacy FortiFone phones. ⚠ 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 about further restricting access of administrative connections, see Configuring administrator accounts on page 56.
	• *MTU*: For the maximum transmission unit (MTU), 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 68 and 9000 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 GUI, 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
Enabled	Select to enable the DHCP server.
ID	The system will generate an ID for this configuration. This is view only.
Interface	If this FortiVoice is in HA mode, make sure that the secondary unit has the same interface as the primary unit. For information about HA, see Using high availability on page 61.
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 52.
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.
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.
VCI string	Enter the phone VCI string supplied by the vendor.

GUI field	Description
Option 66	The DHCP option 66 allows you to specify the IP addresses that the DHCP server assigns to the DHCP clients which are the extension phones on the FortiVoice phone system. The phones obtain the configuration files from these addresses.
Auto provisioning settings	Click to configure FortiVoice auto-provisioning. For details, see Configuring auto-provisioning for FortiFone phones and gateways on page 99.
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 (Byte)	The size of the packet capture file.
Status	The status of the packet capture process, *Complete* or *Running*.

2. Click *New*.
3. In *Capture file prefix*, enter a prefix for the file generated from the captured traffic. This will make it easier to recognize the files. This field supports numbers, letters, spaces, underscores, backslashes, dots, hyphens, round brackets, and colons. The file name format is <prefix>_<yyyy-mm-dd>-<hh-mm-ss>.pcap. Example: test-2022-10-06-07-20-55.pcap.
4. In *Duration*, enter the time period for performing the packet capture.
5. For *SIP Connection*, do the following:
   - In *Peers*, click + to add the extension or trunk of which you want to capture the voice packets. You can select up to 3 peers.
   - If you want to limit the scope of traffic capture, in *IP/HOST*, 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.
6. 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.
7. For *Exclusion*, enter the IP addresses or host names and port numbers of which you do not want to capture the voice traffic.
8. Click *Create*.

To delete traffic capture files

1. Go to *System* > *Network* > *Traffic Capture*.
2. Select a traffic capture to delete.
3. Click *Delete*.
4. If the traffic capture file has rollover files, you have two options:
   - To delete the selected file only, select *Selection Only*.
   - To delete the rollover files too, select *Include Rollovers*.
5. Click *OK*.

Configuring administrator accounts and access profiles

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

This topic includes:

- Configuring administrator accounts on page 56
- Configuring administrator profiles on page 58

Configuring administrator accounts

System > *Administrator* > *Administrator* displays a list of the administrator accounts for the FortiVoice system and the trusted host IP addresses administrators use to log in (if configured).

By default, FortiVoice systems 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,LDAP* or *Single Sign On.*
Authentication Profile	The LDAP authentication profile. For more information, see Configuring LDAP settings on page 130.
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
Enabled	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.
Associate extension	If the *Authentication type* is *Single Sign On*, select an extension. Single sign on (SSO) allows you to connect to the FortiVoice GUI and access the user portal without having to do a second sign in. For more details about using SSO, see Connecting to the FortiVoice GUI on page 15. Click *Edit* to modify the selected extension or click *New* to configure a new one. For more information about extensions, see Configuring IP extensions on page 183.

GUI field	Description
	For more information about the SSO configuration , see Configuring single sign on on page 93.
Admin profile	Select the name of an admin profile that determines which functional areas the administrator account may view or affect. For the default *admin* account, Fortinet recommends that you keep the *super_admin_prof* admin profile. If you do not want the administrator account to have the *super_admin_prof* admin profile, create another admin account and select the admin profile that you want. Click *New* to create a new profile or *Edit* to modify the selected profile. For details, see Configuring administrator profiles on page 58.
Access mode	Specify the access privilege: CLI, GUI, or REST API. REST API is needed for the security fabric configuration. See Configuring FortiVoice to join the Security Fabric on page 94.
Authentication type	Select an administrator authentication type: *Local*, *RADIUS*, *LDAP* or *Single Sign On*. For information about single sign on, see Configuring single sign on on page 93.
New password	This setting is available when the *Authentication type* is *Local*. Enter a secure password for this account. The password can contain any character except spaces. Enter a FortiVoice administrator password that is at least six characters in length. 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 system.
Confirm password	Enter the password again to confirm it. This setting is available when the *Authentication type* is *Local*.
LDAP profile	If you select *LDAP* for *Authentication type*, select an LDAP authentication profile. For more information, see Configuring LDAP settings on page 130.
Trusted hosts type	Select a trusted host type: • *User defined*: Add details about the hosts in *Trusted Hosts*. • *RFC 1918 predefined*: FortiVoice allows connections from any private IP addresses specified by the request for comment 1918 (RFC 1918).
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 system 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 system from your private network by typing `192.168.1.0/255.255.255.0`.

GUI field	Description
	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 about restricting administrative access protocols that can be used by these hosts, see Editing network interfaces on page 49. 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 GUI.
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	Click the + sign to add the department to which the administrator belongs. This option is only available if you select *Department only*.

4. Click *Create*.

Configuring administrator profiles

System > Administrator > Admin Profile displays a list of administrator access profiles.

Administrator profiles govern which areas of the GUI 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

The following FortiVoice unit models can be configured to use redundant array of independent disks (RAID) with their hard disks:

- FVE-2000F
- FVE-5000F

If your FortiVoice unit model does not support RAID, the UI will not display the *RAID* menu.

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

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 59.

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 332, and Configuring alert email on page 344.

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 61.

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 type of the 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	

GUI item	Description
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 59.
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	
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.

GUI item	Description
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 about creating a backup, see Backing up the configuration on page 109.

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 FortiVoice GUI 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 64.

This section contains the following topics:

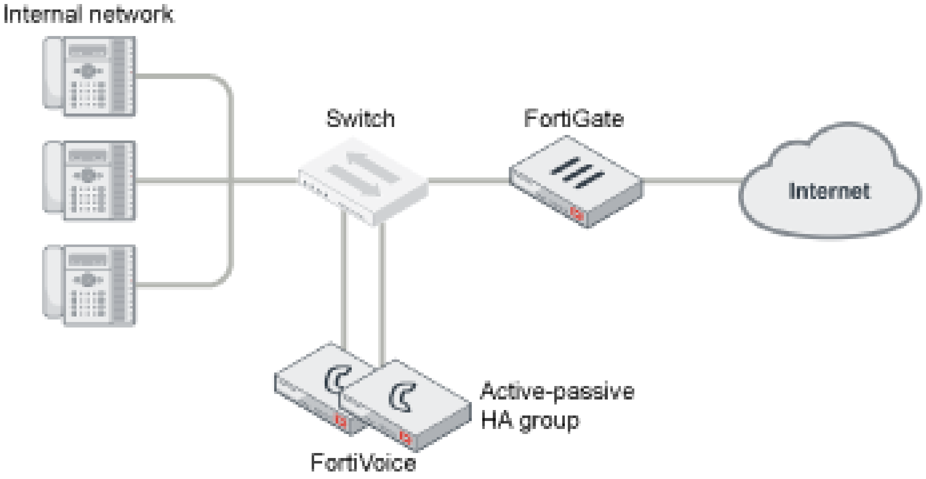
- About high availability on page 62
- About the heartbeat and synchronization on page 63
- Enabling and configuring HA on page 64
- Monitoring the HA status on page 65
- Configuring service-based monitoring on page 73
- Failover scenario examples: on page 74

About high availability

FortiVoice units operate in an 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 63.)
- 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 63.

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 63.

For instructions of how to enable and configure HA, see Enabling and configuring HA on page 64.

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 70.

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 63.
- 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 67. 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 75.

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 76.

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 77 and Configuring alert email on page 344.

Unsynchronized HA Setting

All configuration settings 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 51).

GUI item	Description
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 48. 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 *Primary* or *Secondary*), 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 68.
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 73. 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 62.
   - 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 73.
4. Monitor the status of each group member. For details, see Monitoring the HA status on page 65. 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 334.

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 64.

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*.
Mode Status	
Configured Operating Mode	Displays the HA operating mode that you configured, either: • *Primary*: Configured to be the primary unit of an active-passive group. • *Secondary*: Configured to be the secondary unit of an active-passive group. For information about configuring the HA operating mode, see Mode of operation on page 69. After a failure, the FortiVoice unit may not be acting in its configured HA operating mode. For details, see Effective Operating Mode on page 66.

GUI item	Description
Effective Operating Mode	Displays the mode that the unit is currently operating in, either: • *Primary*: Acting as primary unit. • *Secondary*: 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 69. • *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 69. 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 67. For information about 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 67.
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 69.
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. The message `secondary unit is currently synchronizing` appears when the HA daemon is synchronizing the configuration. For information about items that are not synchronized, see Unsynchronized HA Setting on page 63.
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 `secondary unit is currently synchronizing` appears when the HA daemon is synchronizing data.
Actions	

GUI item	Description
Click HERE to Start a Configuration/Data Sync	Click to manually initiate synchronization of the configuration and call data. For information about items that are not synchronized, see Unsynchronized HA Setting on page 63.
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
primary	primary	Normal for the primary unit of an active-passive HA group.
secondary	secondary	Normal for the secondary unit of an active-passive HA group.
primary	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.
secondary	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 HA mode of operation becomes *Primary*.
primary	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 *secondary*, or to match the configured HA mode of operation, depending on the *On failure* setting.

Configured operating mode	Effective operating mode	Description
primary	secondary	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.
secondary	primary	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 settings, with the exception of *Virtual IP Address* settings, 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 about heartbeat and synchronization, see About the heartbeat and synchronization on page 63.

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 68
   - Configuring HA advanced options on page 69
   - Configuring interface monitoring on page 71
   - Configuring service-based monitoring on page 73
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. • *Primary*: The FortiVoice unit is the primary unit in an active-passive HA group. • *Secondary*: 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 67 and Click HERE to Restore Configured Operating Mode on page 67). • *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 Secondary Role*: On recovery, the failed primary unit’s effective HA mode of operation becomes *secondary*, and the secondary unit continues to assume the *primary* role. The primary unit then synchronizes with the current primary unit. The new primary unit can then deliver phone calls. For information about manually restoring the FortiVoice unit to acting in its configured HA mode of operation, see Click HERE to Restore Configured Operating Mode on page 67. In most cases, you should select the *Wait for Recovery Then Restore Secondary 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 67. For information about configuring service/interface monitoring, see Configuring service-based monitoring on page 73. This option appears only if Mode of operation on page 69 is *Primary*.
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

GUI item	Description
	In addition to configuring the heartbeat, you can configure service monitoring. For details, see Configuring service-based monitoring on page 73. 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 67.
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. This option is not available if you select *Off* for *Mode of operation* under *HA Configuration.*
Survivability service interface	Select the interface port for a local survivable gateway (LSG) to communicate with this FortiVoice unit. In an LSG setup, when the central FortiVoice HA is enabled without a virtual IP, the primary and secondary units need to identify their service interface ports for the LSG to communicate with them. For more information about LSG, see FortiVoice Local Survivable Gateway Deployment Guide. In any other cases, this value is ignored by the system.
Primary Override External Media Host	Enter the host/IP address to override the default external host/IP address for media stream on the primary HA unit.
Secondary Override External Media Host	Enter the host/IP address to override the default external host/IP address for media stream on the secondary HA unit.

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 *Primary* or *Secondary* 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.
Port monitor enabled	Enable to monitor a network interface for failure. If the port fails, the primary unit will trigger a failover.

GUI item	Description
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 63. 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 63. 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 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 63.
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 *Primary* . 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.

GUI item	Description
	• *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 73. • *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 *primary*. For information about the *On failure* option, see Configuring the HA mode and group on page 68. For information about the effective HA operating mode, see Monitoring the HA status on page 65.

To configure service monitoring

1. Go to *System* > *High Availability* > *Configuration*.
2. Select *Primary* or *Secondary* 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
Enabled	Select to enable connection responsiveness tests for SMTP.
Name	Displays the service name.
Remote IP	Enter the peer IP address.

GUI item	Description
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
Enabled	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:

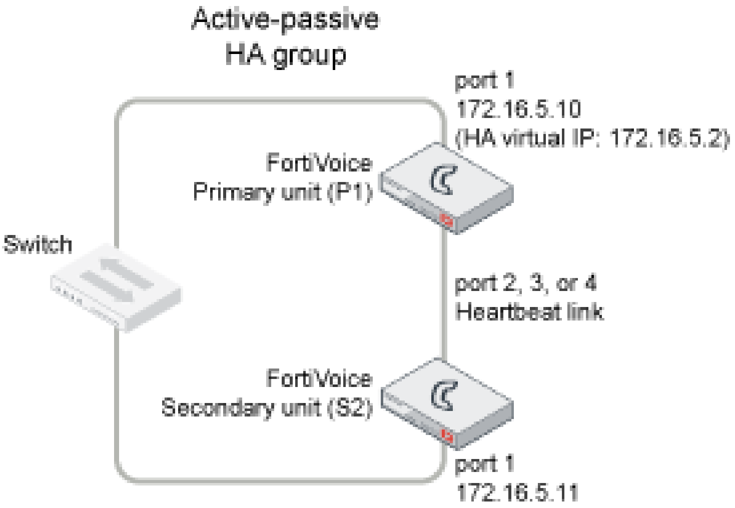
GUI item	Description
Enabled	Select to enable local hard drive monitoring. Interface monitoring is enabled when you configure interface monitoring. See Configuring interface monitoring on page 71. Network interface monitoring tests all active network interfaces whose: Virtual IP action on page 72 setting is **not** *Ignore* Configuring interface monitoring on page 71 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 74. 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 75
- Failover scenario 2: System reboot or reload of the primary unit on page 76
- Failover scenario 3: System reboot or reload of the secondary unit on page 77
- Failover scenario 4: System shutdown of the secondary unit on page 77
- Failover scenario 5: Primary heartbeat link fails on page 78
- Failover scenario 6: Network connection between primary and secondary units fails (remote service monitoring detects a failure) on page 79

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 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 *primary*.
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 *primary*.

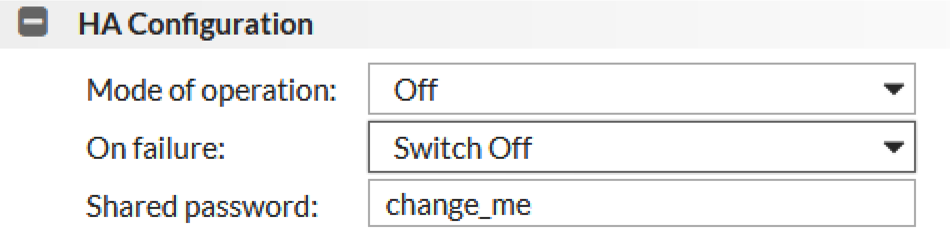
```
This is the HA machine at 172.16.5.11.

The following event has occurred
‘primary heartbeat disappeared’
The state changed from ‘Secondary’ to ‘Primary’
```

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 *PRIMARY*.

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



HA Configuration

Mode of operation: Off

On failure: Switch Off

Shared password: change_me

- *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 67).
- *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
  'SECONDARY asks us to switch roles (recovery after a restart)'
  The state changed from 'PRIMARY' to 'SECONDARY'.

  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 secondary role*
  On recovery, P1's effective HA operating mode becomes *secondary*, and S2 continues to assume the *primary* role. P1 then synchronizes with the current primary unit, S2. For information about manually restoring the FortiVoice unit to acting in its configured HA mode of operation, see Click HERE to Restore Configured Operating Mode on page 67.

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, you can use one of the following methods:

- CLI command: `execute reboot` or `execute reload`
- GUI: In the right corner of the GUI, click admin, and select *Reboot*. To confirm the reboot, click *OK*.

The P1 and S2 behaviors include the following sequence:

- 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 ‘SECONDARY’ 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 ‘SECONDARY’.
- 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, you can use one of the following methods:

- CLI command: `execute reboot` or `execute reload`
- GUI: In the right corner of the GUI, click admin, and select *Reboot*. To confirm the reboot, click *OK*.

The behavior of P1 and S2 includes the following sequence:

- 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: SECONDARY 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 GUI of S2 to restore its effective HA operating mode to *secondary*.

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 *primary*.
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 *primary*.
   This is the HA machine at 172.16.5.11.

   The following event has occurred
   ‘PRIMARY heartbeat disappeared’
   The state changed from ‘SECONDARY’ to ‘PRIMARY’
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 *primary*.

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 *primary*, 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

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

   The state changed from 'PRIMARY' 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 *primary* and the effective HA operating mode of P1 is *off*.

   The configured HA mode of operation of S2 is *secondary* and the effective HA operating mode of S2 is *primary*.
4. Connect to the GUI 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 GUI 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 74, 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 secondary role*. For information about the *On failure* setting, see On failure on page 69. For information about remote service monitoring, see Configuring service-based monitoring on page 73.

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 *secondary* 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 *primary*.
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 *primary*.
   This is the HA machine at 172.16.5.11.

   The following event has occurred
   'PRIMARY remote service disappeared'

The state changed from ‘SECONDARY ’ to ‘PRIMARY’

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 *primary*.
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
   'SECONDARY asks us to switch roles (user requested takeover)'

   The state changed from 'PRIMARY' 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 *secondary*.
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 *secondary*.
   This is the HA machine at 172.16.5.10.

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

   The state changed from 'FAILED' to 'SECONDARY'.
6. Connect to the GUI 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 GUI of S2, go to *System* > *High Availability* > *Status* and select *click HERE to restore configured operating mode*.
9. Connect to the GUI 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.

Working with system configurations

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

This topic includes:

- Configuring the time and date on page 81
- Configuring system options on page 82
- Configuring SNMP queries and traps on page 82
- Configuring email setting on page 88
- Customizing the GUI appearance on page 89
- Selecting the call data storage location on page 91
- Configuring single sign on on page 93
- Configuring FortiVoice to join the Security Fabric on page 94

Configuring the time and date

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

You can either manually set the FortiVoice system time or configure the FortiVoice system 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 systems 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 system'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 system 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.
Set date	Select this option to manually set the date and time of the FortiVoice system'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*. *Server*: Enter the IP address or domain name of an NTP server. You can add a maximum of 10 NTP servers. The FortiVoice system 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.

GUI field	Description
	To find the NTP servers that you can use, see http://www.ntp.org. Depending on your network traffic, it may take some time for the FortiVoice system to synchronize its time with the NTP server.

3. Click *Apply*.

Configuring system options

The *System* > *Configuration* > *Option* tab lets you set the following global settings:

- system idle timeout
- originating host name or IP address used for email notifications
- 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 system 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 voicemail 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 voicemail 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 119.
Administration Ports	Specify the TCP ports for administrative access on all interfaces. Default port numbers: HTTP port number: 80 HTTPS port number: 443 SSH port number: 22 TELNET port number: 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 87.

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 system. For more information, see Editing network interfaces on page 49.

This topic includes:

- Configuring an SNMP threshold on page 83
- Configuring email setting on page 88
- Configuring an SNMP v3 user on page 85

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 system.
Description	Enter a descriptive name for the FortiVoice system.
Location	Enter the location of the FortiVoice system.
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.
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 SNMP agent counts the number of triggers that occurred.

GUI field	Description
	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 about configuring a community, see either Configuring email setting on page 88 or Configuring an SNMP v3 user on page 85.
Enabled	Displays the status of the SNMP community and allows you to change it.
Name	Displays the name of the SNMP community. The SNMP Manager must be configured with this name.
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 about configuring a v3 user, see Configuring an SNMP v3 user on page 85.
Enabled	Displays the status of the SNMP v3 user and allows you to change it.
Name	Displays the name of the SNMP v3 user. The SNMP Manager must be configured with this name.
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 system 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
Enabled	Enable to send traps to and allow queries from the community’s SNMP managers.
Name	Enter a name to identify the SNMP community. If you are editing an existing community, you cannot change the name.

GUI field	Description
	You can add up to 16 communities.
Community Hosts	Lists SNMP managers that can use the Setting in this SNMP community to monitor the FortiVoice system. 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 system. 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 system 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 system should send traps to the SNMP managers in this community. Not all events will trigger traps because FortiVoice checks its status in 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*.

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 system 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
Enabled	Enable to send traps to and allow queries from the user's SNMP managers.
User name	Enter a name to identify the SNMP user. If you are editing an existing user, you cannot change the name.
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 (button)	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 system. 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 system uses to send SNMP v3 traps to the SNMP managers. Select the *Enable* check box to activate traps. Enable each SNMP event for which the FortiVoice system should send traps to the SNMP managers. Not all events trigger traps because the FortiVoice system 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 Management Information Base (MIB) 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 system configuration.

The FortiVoice MIBs are listed in FortiVoice MIBs on page 87. 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

FortiVoice traps

The FortiVoice system’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 system 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 the system performs actions such as shutting down, rebooting, and upgrading.
fmlTrapHAEvent	Trap sent when an HA event occurs.

The Fortinet MIB contains fields reporting current FortiVoice system 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 serial number.
fvSysVersion	The firmware version currently running on the FortiVoice system.
fvSysCpuUsage	The current CPU usage (%).
fvSysMemUsage	The current memory utilization (%).
fvSysLogDiskUsage	The log disk usage (%).
fvSysStorageDiskUsage	The storage disk usage (%).
fvSysEventCode	System component events.

MIB field	Description
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 system 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 183.

To configure email setting

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

GUI field	Description
Local Host	
Host name	Enter the host name of the FortiVoice system, such as `fortivoice-500F`.
Local domain name	Enter the local domain name of the FortiVoice system, 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 system periodically retries to send the message. After it reaches the maximum time, the FortiVoice system 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 system 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).

GUI field	Description
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 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 system account on the SMTP relay. • *Password*: Enter the password for the FortiVoice system 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 challenge and response mechanism)
Test (button)	After you have entered the relay server information, you can click the *Test* button to test if the relay server is accessible. To further test mail delivery, click *Advanced Group*, and enter the sender (MAIL FROM) and recipient (RCPT TO) email addresses. EHLO (Extended HELO) information is filled in by default. Click *Test* to display the test results.
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 119.

3. Click *Apply*.

Customizing the GUI appearance

The *System > Configuration > Appearance* tab lets you customize the default appearance of the GUI 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 *User Portal Interface*.
3. Configure the following:

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 GUI.

GUI field	Description
Product icon	Click *Change* to browse for the product icon. The icon must use the .ico format and size (width x height) 16 x 16 pixels.
Top logo	Click *Change* to upload a graphic that will appear at the top of all pages in the GUI. The image size (width x height) must be 460 x 36 pixels. 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 FortiVoice system does not retain previous 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.
Default UI language	Select the default language for the display of the GUI. You can configure a separate language preference for each administrator account. For details, see Configuring administrator accounts on page 56.
Default theme	Select the default theme for the GUI.
User Portal Interface	
User Portal login	Enter a word or phrase that will appear on top of the user portal login page, such as User Portal 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.
User Portal theme	Select a theme for the user portal GUI.
Default UI language	Select the language in which user portal pages will be displayed. By default, the FortiVoice system will use the same language as the GUI.
User Portal top logo	Click *Change* to upload a graphic that will appear at the top of all user portal pages. The image size (width x height) must be 460 x 36 pixels. 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 FortiVoice system 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 the 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 voicemails.

FortiVoice systems can store call data either locally or remotely. FortiVoice systems 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 system loses connectivity.

If the FortiVoice system 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 68.

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 the configuration on page 109.

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

Unsupported 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 system'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 NAS server: • *NFS*: To configure a network file system (NFS) server. For this option, enter the

GUI field	Description
	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. The range is from 0 to 65535. • *Directory*: The directory path of the NFS export on the NAS server where the FortiVoice system will store call data. • *iSCSI Server*: To configure an Internet Small Computer Systems Interface (iSCSI) 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 system account on the iSCSI server. • *Username*: The user name of the FortiVoice system account on the iSCSI server. • *Password*: The password of the FortiVoice system 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. The range is from 0 to 65535. • *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 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. If *Not mounted* appears, the iSCSI share was not successfully mounted. Verify that the iSCSI server is responding and the FortiVoice system 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 system 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	If the iSCSI disk has never been formatted, the FortiVoice system 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. 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.

Configuring single sign on

Fortinet Single Sign-On (FSSO) is the authentication protocol by which users can transparently authenticate to Fortinet devices. The authentication system (FortiAuthenticator, ADFS, or Centrify) identifies and authenticates users based on their authentication from a different system.

The FortiVoice SSO configuration involves the participation of a network authentication system, such as FortiAuthenticator. The network authentication system can be integrated with the FortiVoice system to poll administrator logon information and send it to the FortiVoice system.

FortiAuthenticator is used as the example authentication system here. For more information, see FortiAuthenticator Administration Guide.

For other systems, refer to their user manuals for configuration information.

You need to have both systems open and switch between the two to exchange authentication information.

After you complete the FortiVoice SSO configuration and log into the FortiVoice system, the *Single Sign On* button will appear on the login page. You can click it and enter the login credential of the FortiAuthenticator user account created for the FortiVoice administrator with single sign on authentication type.

Note that after SSO is enabled:

- All administrator login authentication is controlled by the FortiAuthenticator system. Disabled administrator accounts should not be authenticated by FortiAuthenticator.
- The FortiVoice administrator portal must be accessed using HTTPS (such as https://fortivoice_ip_or_hostname).
- Logging out of FortiVoice administrator portal will also log out of the FortiAuthenticator system.

To configure FortiVoice SSO

a. On the FortiAuthenticator system:

   i. Go to *Authentication* > *SAML IdP* > *General* and enable SAML IDP (Identity Provider).

   ii. Go to *Authentication* > *SAML IdP* > *Service Providers*.

   iii. Click *Create New* to add a SAML service provider and click the *Copy idp_entity_id* icon.

b. On the FortiVoice system:

   i. Go to *System* > *Configuration* > *Single Sign On.*

   ii. Select *Enabled*.

   iii. Click *Retrieve from URL* and paste the IDP entity ID you copied.

   iv. Click *OK* to get the IDP metadata from the FortiAuthenticator.

   v. Refresh your browser. The FortiVoice service provider metadata is generated.

   vi. Click *Download* to save the FortiVoice service provider metadata.

   vii. Click *Apply*.

   viii. Go to *System* > *Administrator* to create an administrator account with single sign on as the authentication type. For more information, see Configuring administrator accounts on page 56.

c. On the FortiAuthenticator system:

   i. Go to the SAML service provider you have created.

   ii. Click Import *SP metadata* and browse for the FortiVoice service provider metadata you saved and click *OK*.

   iii. Enable *SAML request must be signed by SP*.

   iv. Click *OK* to save the service provider configuration.

   v. Open the SAML service provider you have created.

   vi. Click *Create New* under *SAML Attribute*.

   vii. In *SAML attribute*, enter "urn:oid:0.9.2342.19200300.100.1.3".

   viii. In *User attribute*, select an option and click *OK*, then *OK*.

ix. Go to *User Management* > *Local Users* and create a user account for the FortiVoice administrator with single sign on authentication type and use the FortiVoice administrator name as the account user name.

Configuring FortiVoice to join the Security Fabric

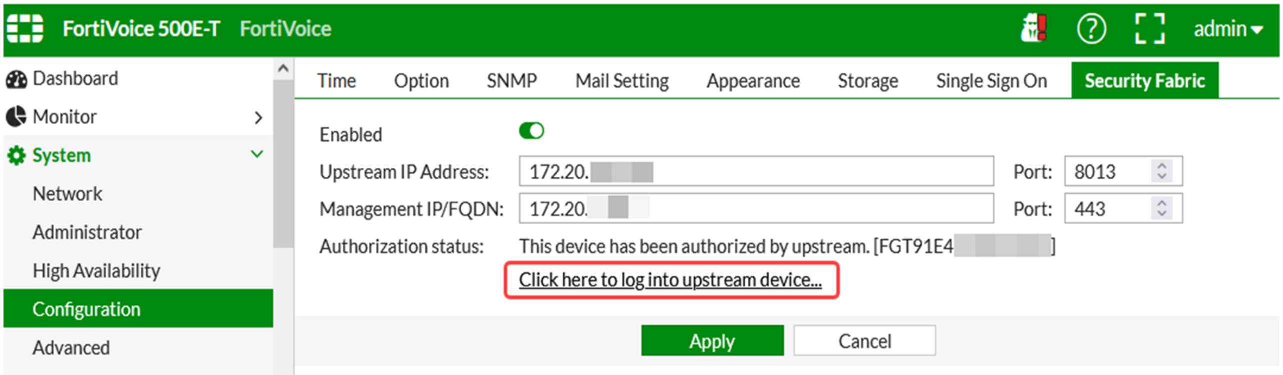
The FortiVoice system can connect to an upstream FortiGate device and become an integrated cluster member of the Security Fabric. This integration allows you to access FortiFone phone details from two FortiGate GUI menus.

Prerequisites

- Verify that the account that you are using to log in to the FortiVoice GUI has the REST API access mode enabled in *System* > *Administrator* > *Administrator*.
- Verify that the FortiGate device is using version 7.2.2 or later.
- Verify that the FortiGate device is operating in NAT mode.

To configure FortiVoice to join the Security Fabric

1. In the GUI of the FortiVoice phone system, go to *System* > *Configuration* > *Security Fabric*.
2. Select *Enabled* to allow the FortiVoice system to become a Security Fabric member.
3. For *Upstream IP Address*, enter the IP address and port number of the root FortiGate device.
4. For *Management IP/FQDN*, enter the IP address and port number of the FortiVoice system.
5. Click *Apply*.
   If the connection is successful, the *Authorization status* shows *This device has been authorized by upstream*. The Security Fabric FortiGate establishes a connection with the FortiVoice system using the IP address and port number specified.
6. The FortiGate admin GUI needs to authorize the FortiVoice system to join the Security Fabric. See details in the FortiVoice section of the FortiOS Administration Guide.
7. After configuring and authorizing the FortiVoice system, FortiVoice sends all information about provisioned FortiFone phones to the FortiGate device.
8. To log in to the FortiGate device, click the *Click here to log into upstream device* link.



Enabled ●

Upstream IP Address: 172.20.[redacted] Port: 8013

Management IP/FQDN: 172.20.[redacted] Port: 443

Authorization status: This device has been authorized by upstream. [FGT91E4[redacted]]

Click here to log into upstream device...

9. You can access FortiFone phone details from the following FortiGate GUI menus. For more details, see the FortiOS Administration Guide.
   - *Security Fabric* > *Asset Identity Center*
   - *Policy & Objects* > *Addresses*

Configuring advanced phone system settings

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

This topic includes:

- Configuring SIP settings on page 95
- Configuring the internal ports on page 98
- Configuring external access on page 98
- Configuring auto-provisioning for FortiFone phones and gateways on page 99

Configuring SIP settings

FortiVoice units support SIP communications.

To configure FortiVoice SIP Setting

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

GUI field	Description
SIP Transport and 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). The WebSocket Secure (WSS) protocol establishes a WebSocket over an encrypted TLS connection. The default port is 8089. 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 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 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.

GUI field	Description
	The default range is from 1 to 480. The start of the range is from 1 to 60 and the end of the range is from 30 to 1440.
Internal extension registration interval	Enter the 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 from 10 to 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.
External extension registration interval	Enter the registration time interval for the extensions on other subnets as required by the FortiVoice unit in seconds. The default is 300 and the range is from 30 to 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.
Subscription Interval	If this is a dynamic account with the VoIP provider, enter the subscription interval as required by the VoIP provider. After each subscription interval, the FortiVoice unit renews the subscription of the account with the VoIP provider.
Extension subscription interval range	To keep the extensions' subscription status with the FortiVoice unit, enter the range of extension subscription time interval as required by the FortiVoice unit in minutes. An extension's subscription timeout setting is overridden by the FortiVoice unit's extension subscription time interval range if it is out of the range. The default range is from 1 to 480. The start of the range is from 1 to 60 and the end of the range is from 30 to 2880.
Extension subscription interval	Enter the subscription time interval for the extensions on your subnet as required by the FortiVoice unit in minutes. The default is 30 and the range is from 1 to 1440. Set a proper value for this option. If it is too low, the performance of the FortiVoice unit is compromised due to frequent subscription. 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 type*: 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.* • *User defined*: Configure your own internal network designated for phone calls on the FortiVoice unit. • *RFC 1918 predefined*: Private IPv4 addresses used for internal traffic that does not

GUI field	Description
	route via the Internet.
SIP timer T1	Enter the SIP T1 in milliseconds. This is an estimate of the Round Trip Time (RTT) of transactions between a client and server. For example, when a SIP Client attempts to send a request to a SIP Server, the time it takes between sending out the request to the point of getting a response is the SIP T1 timer. By default the timer is set to 500 milliseconds. The SIP Timer object is used as specific timing attribute to the SIP Signaling object. Use caution when adjusting these timers because undesired outcomes from lengthy SIP retransmits to an increase in traffic across the network may result.
SIP timer B	This is the INVITE transaction timeout timer. It changes based on the SIP timer T1 value.
ICE support	When the FortiFone softclient is located behind a Network Address Translator (NAT) or FortiFone softclients are on different networks (without internetwork routing), configure the interactive connectivity establishment (ICE) support to allow the FortiVoice phone system to establish a valid audio path with the FortiFone softclient. To configure the ICE support, you have the following two options: • *Static mapping*: Uses the internal and external IP addresses of the FortiVoice phone system. • *STUN server*: Uses the IP address of a Session Traversal Utilities for NAT (STUN) server. Decide which option you want to configure for ICE support. For information about configuring the static mapping, see Configuring the static mapping for ICE support on page 97. For information about configuring the STUN server, see Configuring the STUN server for ICE support on page 98.

3. Click *Apply*.

Configuring the static mapping for ICE support

1. Go to *System* > *Advanced* > *SIP.*
2. Expand *Advanced Setting*.
3. In *ICE Support*, select *Static mapping*.
4. Click *New*.
5. Make sure that *Enabled* is selected.
6. Enter the internal and external FortiVoice IP addresses used in your deployment.
7. Click *Create*.

⚠ Changing the ICE static mapping restarts the voice process and interrupts all ongoing calls. The call system takes a minute to resume service.

8. To continue, click *Yes*.
9. Click *Apply*.

Configuring the STUN server for ICE support

1. Go to *System* > *Advanced* > *SIP.*
2. Expand *Advanced Setting*.
3. In *ICE Support*, select *STUN server*.
4. For *STUN server*, enter the IP address or host name of a Fortinet or third-party STUN server.
5. 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 auto-provisioning for FortiFone phones and gateways on page 99.

Extensions are defined as external in extension configuration. For more information, see Configuring IP extensions on page 183.

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 auto-provisioning for FortiFone phones and gateways

System > *Advanced* > *Auto Provisioning* can allow the FortiVoice unit to discover FortiFone phones and gateways on your network and send the configuration files to them.

With auto-provisioning enabled and configured, when a supported FortiFone phone or gateway is connected to the network and powered on, it is automatically discovered and receives the configuration file from the FortiVoice unit. The FortiFone phone or gateway reboots with the pushed-in configuration file and registers with the FortiVoice unit.

The FortiVoice unit can auto-provision the supported FortiFone phones and gateways only.

To configure auto-provisioning settings

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

GUI field	Description
Auto Provisioning	
Enabled	Select to activate the auto-provisioning function for FortiFone phones and gateways.
Not assigned phone (Generate default configuration for not assigned Desktop FortiFone)	This option is only available after *Auto Provisioning* is enabled. Select to generate basic phone configuration files for the supported not assigned SIP desk FortiFone phones. For details, see Viewing desk phones on page 34. 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 server port information reflects the FortiVoice network interfaces. For details, see Configuring the network interfaces on page 48. • *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 the 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 53. 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, a secondary account can be added to an extension. The addition of a secondary account can be useful to a person that has more than one role in a company and wants a different extension assigned to each one or needs to assist/monitor another extension. When you add a secondary account to your extension, make sure that the SIP profile of the main device on the secondary account **MUST** be the same as the SIP profile of the primary account device. For more information about SIP profiles, see Configuring SIP profiles on page 138. Select this option to allow the addition of a secondary account when configuring extensions. For more information about adding a secondary account to an extension, see Advanced on page 187.
Administrator PIN to provision phone	Click and enter a global password to be used by an administrator to connect a FortiFone phone 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 120. For example, you can press the default Configure Phone feature code *17 (See Modifying feature access codes on page 324) on any FortiFone phone 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.
Backward support of legacy FortiFone (FON 470/870/360/460/ 560) (Obsolescent)	If you have legacy FortiFone phones, select this option for backward provisioning support. *TFTP provisioning server* contains phone auto-provisioning information for the phones. *mDNS multicast address* allows the connected phones to find the provisioning server contained in the mDNS multicast server message.

2. Click *Apply*.

Managing certificates

This section explains how to manage X.509 security certificates using the FortiVoice GUI. Using the *System* > *Certificate* menu, 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 GUI (HTTPS connections only) • phone user portal (HTTPS connections only) • phone and FortiVoice unit (TLS and SRTP connections only), see Configuring SIP profiles on page 138. For details, see Managing local certificates on page 101.
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 106.
Personal certificates	Phone users' personal certificates are used for S/MIME encryption.
OCSP server certificates	View and import the certificates of the online certificate status protocol (OCSP) servers of your certificate authority (CA). For details, see Managing OCSP server certificates on page 107.
APNs certificates	View and import the Apple Push Notification service (APNs) and VoIP services certificates. For details, see Managing APNs and VoIP services certificates on page 107.

This section contains the following topics:

- Managing local certificates on page 101
- Obtaining and installing a local certificate on page 102
- Managing certificate authority certificates on page 106
- Managing the certificate revocation list on page 107
- Managing OCSP server certificates on page 107
- Managing APNs and VoIP services certificates on page 107

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 GUI (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.

GUI field	Description
Generate	Click to generate a local certificate request. For more information, see Generating a certificate signing request on page 102.
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 104. • *Download PKCS12 File*: Download a PKCS #12 (.p12) file. For details, see Downloading a PKCS #12 certificate on page 106.
Assign to	Assign a local certificate to a service. For details, see Assigning a local certificate to a service on page 106.
Import	Click to import a signed certificate for local use. For more information, see Importing a certificate on page 104.

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 104 and Assigning a local certificate to a service on page 106.
- 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 102
- Downloading a certificate signing request on page 104
- Submitting a certificate request to your CA for signing on page 104
- Importing a certificate on page 104
- Assigning a local certificate to a service on page 106

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 102.

To generate a certificate request

1. Go to *System* >*Certificate* > *Local Certificate*.
2. Click *Generate*.

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* 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 GUI 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 48 and Configuring DNS on page 52. 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), and click >>. You may enter more than one organizational unit name.
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)
State/Province	Type the name of the state or province where the FortiVoice unit is located. (Optional)

GUI field	Description
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 104.

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 102.

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 102.

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 104.

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.

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 102.

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 102.
   - *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.
4. For *Certificate*, configure the following:
   - *Certificate name:* Enter the name of the certificate.
   - *Certificate file*: Click *Import* to locate and import the file.
   - *Key file*: Click *Import* to locate and import the file.
   - *Password*: Enter the password that was used to encrypt the file, enabling the FortiVoice unit to decrypt and install the certificate.
5. Click *OK*.

Assigning a local certificate to a service

You can assign a local certificate to one or more services (HTTPS, LDAPS, SIP TLS, and SIP WSS), as applicable.

1. Go to *System* > *Certificate* > *Local Certificate*.
2. To select the certificate, click the row in the certificate table.
3. Click *Assign to*.
4. From the *Predefined* list, select the service, and click >> to move this service to the *Selected* list.
5. Click *OK*.
6. If the change is for an LDAPS, SIP TLS, or SIP WSS service, all active calls will be disconnected to apply the certificate change. To confirm the service change, click *Yes*.
7. If the change is for the HTTPS service, the FortiVoice GUI asks you to perform the following steps:
   a. To confirm the service change, click *Yes*.
   b. To reload the FortiVoice GUI, press *OK*.
   c. Wait for a few seconds.
   d. If the reload is unsuccessful, reload the FortiVoice GUI in your web browser.

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 about importing a PKCS #12 file, see Importing a certificate on page 104.

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.

Managing OCSP server certificates

Go to *System > Certificate > Remote* to view and import the certificates of the online certificate status protocol (OCSP) servers of your certificate authority (CA).

OCSP lets you revoke or validate certificates by query, rather than by importing certificate revocation lists (CRL). For information about importing CRLs, see Managing the certificate revocation list on page 107.

Remote certificates are required if you enable OCSP for PKI users.

To view the list of remote certificates, go to *System > Certificate > Remote*.

GUI field	Description
View	Select a certificate and click *View* to display certificate details including the certificate name, issuer, subject, and the range of dates within which the certificate is valid.
Download	Click the row of a certificate in order to select it, then click *Download* to save a copy of the OCSP server certificate (.cer).
Import	Click to import an OCSP server certificate.
Name	Displays the name of the OCSP server certificate.
Subject	Displays the Distinguished Name (DN) located in the *Subject* field of the certificate.

Managing APNs and VoIP services certificates

An Apple iPhone using the FortiFone softclient for iOS requires a connection to the Apple Push Notification service (APNs).

To connect with APNs, FortiVoice supports the following methods:

- Token-based connection: This method is the default.
- Certificate-based connection: FortiVoice can use this method as a fallback. If you need to disable the token-based connection, use the following CLI commands:
  ```
  config system notification-service
     set ios-notification-token disable
     show full
  end
  ```

If FortiVoice uses a certificate-based connection, the FortiFone softclient for iOS requires the following certificates on the FortiVoice phone system:

- Apple Push Notification service (APNs): Used to receive notification messages. The certificate name is fortifone.push.
- VoIP services: Used to receive incoming calls. The certificate name is fortifone.voip.

To view the list of APNs and VoIP services certificates, go to *System* > *Certificate* > *APNS Push Certificate*.

GUI field	Description
Name	Displays the certificate name (fortifone.push or fortifone.voip).
Subject	Displays details of the entity associated with the certificate.
Expiration	Indicates the expiration status of the certificates: • Green icon: The certificate is valid. • Orange icon: The certificate expires in 30 days. • Red icon: The certificate is expired.

To view details about APNs and VoIP services certificates

1. Go to *System* > *Certificate* > *APNS Push Certificate*.
2. Select a certificate and click *View*.
   You can access the following details:
   - *Certificate Name* is either fortifone.push or fortifone.voip.
   - *Issuer* is the authority who has signed and issued the certificate.
   - *Subject* is the entity associated with the certificate.
   - *Valid from* and *Valid to* specifies the period that the certificate is valid.

To import APNs and VoIP services certificates

1. Prior to the expiry of the certificates, contact Fortinet Support to start the process to obtain new certificates (fortifone.push and fortifone.voip).

   Importing an APNs certificate or a VoIP services certificate replaces an existing certificate. You cannot delete a certificate.

2. With your assistance, a Fortinet Support representative will remotely access the FortiVoice phone system (*System* > *Certificate* > *APNS Push Certificate*) to import the new certificates.

Maintaining the system

The *System* > *Maintenance* submenu allows you to perform the scheduled maintenance of FortiVoice and the phone firmware.

This topic includes:

- Maintaining the system configuration on page 109
- Maintaining phones on page 110
- Viewing configuration jobs of managed devices on page 113

Maintaining the system configuration

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

This section includes the following topics:

- Backing up the configuration on page 109
- Restoring the configuration on page 110
- Restoring the firmware on page 110
- Downloading a trace file on page 110

Backing up the 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.

System configuration includes the configurations that make the FortiVoice phone system work. User data includes user-configured settings, such as voicemail greetings and reminders.

You can back up the system configuration and user data.

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.

In a system configuration backup, FortiVoice includes the following data:

- Configuration (configuration file only)

In a user data backup, FortiVoice includes the following data:

- Contacts: Includes business and directory contacts, not personal contacts.
- Prompts: Includes all prompts, auto attendant greetings, and music on hold.
- Reminders: Includes system and user reminders.
- Voicemail greetings: Includes the voicemail greeting(s) for each user.

In a user data backup, FortiVoice excludes the following data:

- Voicemail messages
- Call recordings
  Note that FortiVoice stores call recordings in *Monitor > Storage > Recorded Call* (see Playing and downloading recorded calls on page 44). You can archive recorded calls to a remote FTP or SFTP storage server (see Archiving recorded calls on page 308).
- Faxes
  Note that FortiVoice stores faxes in *Monitor > Storage > Fax Archive* (see Viewing archived faxes on page 45). You can archive faxes to a remote FTP or SFTP storage server (see Archiving faxes on page 321).

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 110.

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. You can select a backup type to view, restore, download, or delete a configuration file.
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* under the *System* > *Maintenance* > *Configuration* > *Trace Log*, you can restore the backup FortiVoice configuration from your local computer. For details, see Restoring the configuration on page 366.

Restoring the firmware

In the *Restore Firmware* area under *System* > *Maintenance* > *Configuration* > *Trace Log*, you can install a FortiVoice firmware from your local computer. For details, see Upgrading the firmware on page 362.

Downloading a trace file

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

Trace logs 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* settings.
3. Click *Prepare* to make the trace log file ready before downloading it.
4. Click *Download trace log*.
5. Find the downloaded file and send the file to Fortinet Technical Support.

Maintaining phones

This section includes the following topics:

- You can use one of the following methods to update the configuration on the phones:
  - To update the phone configuration using the phone maintenance icon in the top banner on page 111
  - To update the phone configuration using the Phone Maintenance Job menu on page 111
- To upgrade the phone firmware on page 112

To update the phone configuration using the phone maintenance icon in the top banner

1. After changing the phone configuration (such as a phone profile), click ! in the top banner.
   The Phone Configuration Maintenance dialog opens with *Type* as *Configuration update*.
2. Configure the following:

GUI field	Description
Configuration Change Summary	Gives you access to the following details: • Messages to be processed • Devices affected
Extension Selection	
All related devices (enabled)	You want to update phone configurations for all devices.
All related devices (disabled)	You want to update phone configurations for selected devices. • *Phone model*: Select the phone model of the extensions of which you want to perform the operation. • *Extensions*: Click in the plus sign to select the extensions for the selected phone model.
Schedule	Schedule the time to update phone configurations.

3. Click *OK*.
4. To view the progress and completion of the configuration update, go to *System* > *Maintenance* > *Phone Maintenance Job*.

To update the phone configuration using the *Phone Maintenance Job* menu

1. After changing the phone configuration (such as a phone profile), go to *System* > *Maintenance* > *Phone Maintenance Job*.
2. Click *New* and select *Configuration update*.
3. Configure the following:

GUI field	Description
Name	Enter a name for the operation.
Extension Selection	
All related devices (enabled)	You want to update phone configurations or upgrade phone firmware for all devices.
All related devices (disabled)	You want to update phone configurations or upgrade phone firmware for selected devices. • *Phone model*: Select the phone model of the extensions of which you want to perform the operation. • *Extensions*: Click in the plus sign to select the extensions for the selected phone model.
Schedule	Schedule the time to update phone configurations or upgrade phone firmware.

4. Click *Create*.

To upgrade the phone firmware

For the complete sequence to upgrade the phone firmware, see the FortiFone firmware upgrades section in the FortiVoice Cookbook.

To view a phone maintenance job

1. Go to *System* > *Maintenance* > *Phone Maintenance Job*.
2. Select a row in the main table.
3. To view details, you have four options:

- Click the *View* button. The Phone Maintenance Job dialog box opens.
- Double-click the selected row. The Phone Maintenance Job dialog box opens.
- Go to the *Progress* column and hover over the percentage link. The popup window opens.
- Go to the *Progress* column and click the percentage link. The Progress Detail dialog box opens.

To view phone upgrade details

You can view details about phone upgrade.

1. Go to *System* > *Maintenance* > *Phone Maintenance Job*.
2. Click the *Phone Configuration* button.

To view details of the phone firmware upgrade

You can view the following details about the phone firmware file:

- File name
- Firmware version
- Size of the firmware file
- File date
- Status

1. Go to *System* > *Maintenance* > *Phone Maintenance Job*.
2. Click the *Phone Firmware* button.
3. For information about uploading the firmware on the phones and doing the upgrade, see Managing the firmware on page 174.

To view log details of the phone upgrade

1. Go to *System* > *Maintenance* > *Phone Maintenance Job*.
2. Go to the *Log* column and click *View*.

To reboot phones

1. Go to *System* > *Maintenance* > *Phone Maintenance*.
2. Click *New* > *Phone Force Reboot*.

3. Configure the following:

GUI field	Description
Name	Enter a name for the phone reboot operation.
Extension Selection	Select the extensions of which you want to perform the operation.
All devices	You want to reboot all of the phones registered with the FortiVoice unit.
Selected devices	You want to reboot some phones registered with the FortiVoice unit. • *Phone Model*: Select the phone model of the extensions of which you want to perform the operation. • *Extension*: Click the plus sign to select the extensions for the selected phone model.
Schedule	Schedule the time to reboot the phones.

4. Click *Create*.

Viewing configuration jobs of managed devices

The *System* > *Maintenance* > *Managed Device Configuration Job* tab lets you view details about the jobs that you initiated on your managed devices from *Managed System* > *Gateway* or *Managed System* > *Survivability*.

For more information about updating the configuration on multiple gateways or branches at the same time, see the *Actions* > *Start Config Job* option in the following sections:

- Managing FXO gateways on page 170
- Managing FXS gateways on page 170
- Managing PRI gateways on page 172
- Configuring local survivability on page 173

Configuring the phone system

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

This topic includes:

- Configuring phone system settings on page 114
- Creating contacts on page 123
- Managing phone audio settings on page 125
- Configuring LDAP settings on page 130
- Working with FortiVoice profiles on page 138
- Configuring devices on page 158
- Reviewing system configuration on page 168

Configuring phone system settings

The *Phone System* > *Setting* menu lets 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 settings that affect them, such as number setting and speed dial setting.

This topic includes:

- Setting FortiVoice location, contact, and emergency information on page 114
- Configuring FortiVoice options on page 116
- Customizing call report and notification email templates on page 119
- Configuring system capacity on page 120

Setting FortiVoice location, contact, and emergency information

Identify FortiVoice system settings such as the location, emergency number, main number, contact information, and emergency settings.

To set the FortiVoice location, contact, and emergency information

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.

GUI field	Description
Emergency number	Click the default number (911) to enter the emergency call number of the selected country.
Long-distance prefix	Click the *Edit* icon to enter the prefix for dialing long-distance calls.
International prefix	Click the *Edit* icon to enter the prefix for dialing international calls.
Outside line prefix	Click the *Edit* icon to enter the prefix for making outbound calls.
Area code	Click the *Edit* icon 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 voicemail. 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 more details, see Managing phone audio settings on page 125.
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 156.
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	
Do Nothing	The FortiVoice unit will not send an alert email when an extension dials the emergency number.
Sent Alert Email	The FortiVoice unit will send an alert email when an extension dials the emergency number.
Emergency contact emails	FortiVoice sends an alert email when a user makes an emergency call. You can add up to 30 email addresses.
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 119.
Emergency barge number	Enter an authorized user's extension number to be dialed. When an ongoing emergency call is in progress, the phone of the authorized user also rings. This user can listen to the call and talk, if necessary.
Emergency message group number	Select a message group number for emergency contact. This number is dialed when an emergency call is made. For more information about message groups, see Creating message groups on page 222.

GUI field	Description
DID callback hold time	FortiVoice keeps the callback number of the emergency caller in memory for the specified time period. If the emergency operator calls back before the hold time expires, FortiVoice routes the call to the emergency caller. If the emergency operator calls back after the DID callback hold time has expired, FortiVoice uses the inbound DID mapping to route the call. The range is from 10 to 480 minutes. The default is 30 minutes. FortiVoice uses this setting if the Emergency zone profile has *DID callback type* as *Emergency caller*. For more details, see Configuring emergency zone profiles on page 156.

3. Click *Apply*.

Configuring FortiVoice 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 settings. These settings apply to all extensions unless you change them when configuring the extensions. For details, see Configuring IP extensions on page 183.

Pattern-matching syntax

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.
[ ] (square brackets)	Matches any digits in the brackets. For a range of numbers, use a dash. Example: [15-7]. In this example, the pattern matches 1, 5, 6, and 7.
. (period)	Acts as a wildcard that matches any digit and allows for any number of digits to be dialed. Example of a pattern matching rule: XX. In this example, the system looks for a dialed number match that has three or more digits.
! (exclamation point)	Acts as a wildcard that matches any digit (including no digits) and allows for any number of digits to be dialed. Example of a pattern matching rule: XX! In this example, the system looks for a dialed number match that has two or more digits.

Pattern-matching examples

Pattern	Description
X.	Matches any dialed number.
NXXXXXX	Matches any seven-digit number, as long as the first digit is 2 or higher.
NXXNXXXXXX	Matches any dialed number that has 10 digits.
1NXXNXXXXXX	Matches any dialed number that matches this pattern: 1 + area code (between 200 and 999) + seven-digit number (first digit is 2 or higher).
011.	Matches any number that starts with 011 and has at least one more digit.
XX!	Matches any two or more digits.

To configure FortiVoice 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 183.
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 301.
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 to be used by the operator of the FortiVoice unit.
Supporting extension	Enter the extension to be used for the technical support of the FortiVoice unit.
FXS Gateway start extension	Enter an analog extension number to start the numbering for the range of 1000 extensions. The default is 7801. When you add your first FXS gateway to your deployment, the FortiVoice phone system creates default managed extensions (4 for the GS04, 16 for the GS16, and 24 for the GS24). GS16 gateway example: The FortiVoice phone system creates 16 extensions from 7801 to 7816. With any subsequent FXS gateway addition, the FortiVoice phone system continues to add a range of 16 extensions to the existing managed extension list. For example, the FortiVoice phone system adds extensions 7817 to 7832 for the second FXS gateway.

GUI field	Description
	If the FortiVoice phone system already has an extension that is included in the range of default managed extensions to be created, the numbering of new extensions will account for the existing extension. For example, the FortiVoice phone system has extension 7812. With the addition of the first GS16 gateway, the FortiVoice phone system would create 16 managed extensions from 7801 to 7817 (not 7816). If your FortiVoice deployment includes more than 250 GS04 gateways, 62 GS16 gateways, or 41 GS14 gateways (1000 analog extensions), enter the start of the next analog extension range, for example 9801. This configuration change makes another 1000 extensions available and allows you to add more FXS gateways.
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 address to access it from the web. This password appears when you add an extension. For details, see Configuring IP extensions on page 183. • *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 portal access. This password appears when you add an extension. For details, see Configuring IP extensions on page 183. • *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 voicemail and the user portal. This password appears when you add an extension. For details, see Configuring IP extensions on page 183. If you select *Specified*, the default password is 123123.
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 183.
Default ring duration	Use this option to set phone ringing time for extensions and FortiFone softclient for mobile phones. • *Adaptive*: This is recommended for extensions with mobile softclients. Select this option and both the extensions and mobile softclients will ring for 40 seconds before the call is processed (for example, the call is sent to voicemail). This setting is to ensure that mobile softclients will not miss any calls due to possible network transmission delays. You do not need to enter any ring

GUI field	Description
	duration value. Any ring duration value already entered will be ignored. • *Fixed*: This is recommended for extensions without mobile softclients. Select this option and enter the ring duration value in seconds. The extensions will ring for the ring duration value you entered before the call is processed (for example, the call is sent to voicemail). The default is 20.
Internal calls ring pattern	Select the system defined distinctive ring pattern for internal calls.
External calls ring pattern	Select the system defined distinctive ring pattern for external calls.

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 call report profiles and generating reports on page 337) 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 settings, and configure queue logs.

To configure system capacity

1. Go to *Phone 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 auto-provisioning for FortiFone phones and gateways on page 99.
PBX identification	Enter a unique name for the FortiVoice unit.
Local authentication type	Select the method to access the user portal and softclient. 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 183. • *User Password or Voicemail PIN*: Both personal password and user PIN can be used to access the user portal and softclient. • *User Password Only:* The user personal password to access the user portal and softclient.
Notification expiry (Hours)	Enter the email notification expiry time in hours. The range is from 1 to 2160.
QR code expiry (Hours)	Enter the QR code expiry time in hours. The range is from 1 to 2160.
System block list	Enable to block phone numbers on the system level. **To block a number on the system level** 1. Go to *Monitor* > *Call History* > *Call Detail Record (CDR)*. 2. Select the number you want to block from the CDR list. 3. Select *More Action* > *Block* > *Block Caller/Callee* as required. 4. Go to *Security* > *Blocked Number*. The number you selected is added to the block list.

GUI field	Description
	5. Click *Setting*. **6.** Enable *System block list*. **7.** Click *Apply*. Future calls from the number you selected to any extensions on the FortiVoice unit will be blocked.
Personal block list	Enable to block phone numbers on a personal basis. **To block a number on a personal basis** **1.** Go to *Phone System* > *Setting* > *Miscellaneous*. **2.** Enable *Personal block list*. **3.** Click *Apply*. **4.** Log in to the user portal. **5.** Click *Call History*. **6.** Select the number you want to block from the list. **7.** Select *More Action* > *Block*. **8.** Go to *Contact* > *Personal Contact*. **9.** Click *Personal Block List* to verify that the blocked number is listed. Future calls from the number you selected to your extension will be blocked.
Match personal contact	Enable to show the unique name added to a number in the personal contacts on your extension display. **To match a personal contact** **1.** Go to *Phone System* > *Setting* > *Miscellaneous*. **2.** Enable *Match personal contact*. **3.** Click *Apply*. **4.** Log in to the User Portal. **5.** Click *Call History*. **6.** Select the number you want to match to a personal contact. **7.** Click *More Actions* > *Add to Contact*. **8.** Enter a unique display name and other contact information for the number **9.** Click *Create*. **10.** Go to *Contact* > *Personal Contact*. **11.** Verify the number is listed with the unique name you entered. When the number you selected calls, the unique display name you entered will show on your extension screen.
Business Group	This option is available on FVE-500F and larger models only. Select *Disabled* to hide the Business Group tab in *Extensions* and select *Automatic* to show it. For more information, see Creating business groups on page 224.
Caller ID	Select *Format incoming caller id numbers* if you want the FortiVoice unit to display the incoming caller ID in the right format. For example, 12223334444 will be formatted to 1-222-333-4444.
Schedule Override	Select *Allow admin user to override schedule* if required.

GUI field	Description
	An administrator with the privilege can dial *821, *822, or *823 followed by the administrator PIN to temporarily replace the original system level schedule profile with one of the three default ones. You may also modify the temporary schedule by clicking the link following *821, *822, or *823. Dial *820 to go back to the original schedule. The system level phone schedule profiles are used when configuring dial plans, auto attendant, or virtual numbers. The following list includes the schedule priority from the highest (1) to the lowest (3): **1.** Anytime schedule (full day for every day) **2.** Override schedule **3.** Regular schedule For information about the phone system schedule profile, see Scheduling the FortiVoice unit on page 158.
Voicemail	Enter the maximum message length, greeting length, voicemail volume, and greeting 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 from 3 to 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.
Read name sequence	Select if you want a person's name to be read out after you check the directory by dialing the person's first or last name. *One by one*: All names matching your dialed directory checking pattern are read out one by one. *Menu group listing*: For efficiency, the FortiVoice unit breaks all names matching your dialed directory checking pattern into groups of 8 if applicable, and reads them out group by group.
List options	Select the type of extension numbers to be included in the directory.
Include directory	Select to allow users to view all extension entries in the directory.
Include subdirectory	To include department entries in the directory, select Department. If your FortiVoice unit supports the functionality, you may be able to include additional subdirectories (Business Group and Survivability Branch) but make sure to also complete the configuration. See also: Creating business groups on page 224 and FortiVoice Local Survivable Gateway Deployment Guide. For complete details about directory filtering, see the Filtering the phone directory section in the FortiVoice Cookbook.
CDR	For information about call log/CDR, see Viewing call detail records on page 38.

GUI field	Description
CDR retention time	Enter the time in months that you want to keep the call log/call detail record. The range is from 0 to 72.
CDR max records	Enter the maximum number of CDR records to keep. The range is from 0 to 2000 (in thousands).
Queue Log	For information about queue logs, see Viewing log messages on page 40.
Queue log retention time	Enter the time in months that you want to keep the queue log. The range is from 0 to 72.
Queue log max records	Enter the maximum number of log records to keep. The range is from 0 to 2000 (in thousands).
Call Center Report	This function requires that you upload the Call center license to your FortiVoice system.
Retention time	Enter the time in months that you want to keep the call center reports. The range is from 0 to 72.
Max records	Enter the maximum number of call center reports to keep. The range is from 0 to 1000 (in thousands).
Integration Service	If you are integrating Microsoft Teams with the FortiFone Softclient for Desktop, enable this function. This function requires the FortiVoice Unified Communication license.

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. This is compulsory.
Mobile number	Enter the contact’s cellphone number.
Home number	Enter the contact’s home phone number.

GUI field	Description
Description	Enter any notes for the address book.
Upload/Delete (icons)	Click to add or remove a picture of the business contact. This option is only available when you edit a business contact. By adding a picture of the business contact, when there is an incoming call from that contact, the caller/contact's picture/photo ID displays on the callee's phone, if the phone model supports this feature.

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*.

Viewing contacts retrieved from the LDAP server

Phone System > *Contact* > *LDAP Contact* displays the contact information retrieved from the LDAP server.

If you have contact or employee information in your LDAP server, you can configure the LDAP attribute mapping templates to retrieve the information and add it to the contact and extension lists. For details, see Configuring the LDAP connector on page 134.

Configuring speed dials

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

For information about setting speed dial number pattern, see Configuring FortiVoice options on page 116.

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 (for example, #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* menu lets you upload, record, and play phone sound files that can be used as voicemail greetings, announcements, and music on hold. The following default sound files are available and ready to use:

- *callback_prompt_default*: Includes an announcement about a callback and asks the user to wait for the next available representative.
- *greeting_default*: Includes a generic greeting asking the user to press an extension or the number sign (#) to reach the directory.
- *musicOnHold*: Includes recorded instrumental music that can play for on-hold calls, conference calls, and auto attendants.
- *welcome_default*: Congratulates the user for successfully completing the set up of the FortiVoice phone system.

The *Phone System* > *Audio* > *Music On Hold* menu lets you select a sound file and settings. The sound file can be used when configuring music on hold for conference calls, call queues, and call parking. See Configuring music on hold on page 126.

The *Phone System* > *Audio* > *Prompt Language* menu is used to set for FortiVoice unit’s voice greetings, such as auto attendant and voicemail. The FortiVoice phone system includes eight prompt languages. The default prompt language is English. For more information about setting the default prompt language, see Setting FortiVoice location, contact, and emergency information on page 114.

This section includes the following topics:

- Uploading or recording sound files on page 125
- Configuring music on hold on page 126
- Uploading a prompt language file on page 127
- Recording sound files using an audio software on page 127

Uploading or recording sound files

The *Phone System* > *Audio* > *Prompt* menu lets you upload a sound file or place a call to an extension to record a sound file to be used as voicemail greetings, announcements, and music on hold.

To use an audio software to create your own sound file, see Recording sound files using an audio software on page 127.

Before you begin

If you want to upload a sound file, make sure that the file meets the following requirements:

- WAVE file (WAV) in PCM format or an MP3 file
- For a prompt sound file, the maximum size is 10 MB.
- For a music on hold file, the maximum size is 50 MB.

To upload or record sound files

1. Go to *Phone System > Audio > Prompt*.
2. Click *New*.
3. Enter a *File name*
4. You can leave the *File ID* empty or enter a number with a maximum of 6 digits.
5. Select a file *Type* (*Prompt Sound File* or *Music on Hold*).
6. Optionally, enter a *Description* for the file.
7. For *Voice language*, you have two options (*Upload* or *Record*).
8. To upload a sound file:
   a. Click *Upload*.
   b. Select a file.
   c. Click *Open*.
9. To record a sound file:
   a. 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 183.
   c. When the extension rings, record the sound file and hang up.
   d. On the FortiVoice GUI, click *Yes* on the *Voice recording request sent to specified extension* dialog box.
10. Click *Create*.

Configuring 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 entry.
Mode	
Files	If you select to use existing sound files, do the following: • For *Sound files*, click + and select the sound files. For details about adding a sound file, see Uploading or recording sound files on page 125. • 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 *Sound files* field, select *Sequential*.

GUI field	Description
Stream	Before deciding to use streaming files, make sure to only use legal stream sources. 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.
Volume	Set the music sound volume.
Description	Optionally, enter a description for the entry.

4. Click *Create*.

Uploading a prompt language file

The *Phone System* > *Audio* > *Prompt Language* menu includes 10 languages (English, French, Spanish, Polish, Chinese, Italian, Portuguese (Brazil), Portuguese (Portugal), Russian, Arabic). It's possible to add other prompt languages (Cantonese, Japanese, Korean).

1. Contact Fortinet Support to obtain the FortiVoice language package format (FVL) file for the language that you want to add.
2. Save the FVL file to your management computer.
3. Go to *Phone System* > *Audio* > *Prompt Language*.
4. Click *New*.
5. Click *Upload* and locate the FVL file.
6. Click *Create*.

Recording sound files using an audio software

You can use an audio software and a microphone to record a sound file. This section uses the Audacity software version 3.3.3 as an example to help you choose the correct settings.

If you prefer to place a call to an extension to record a sound file, see Uploading or recording sound files on page 125.

Before you begin

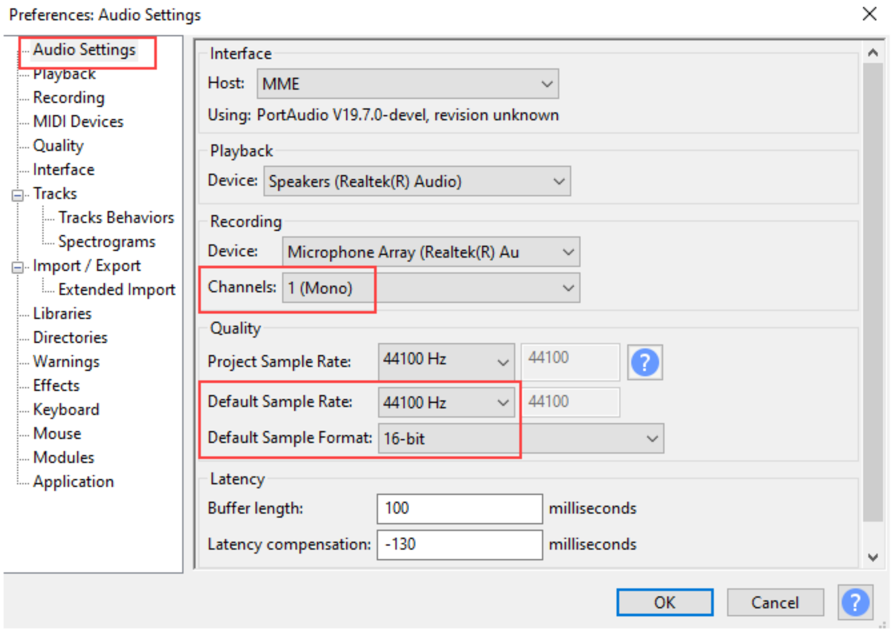
Make sure that the sound file meets the following requirements:

- WAVE file (WAV) in PCM format or an MP3 file
- For a prompt sound file, the maximum size is 10 MB.
- For a music on hold file, the maximum size is 50 MB.

To record a sound file

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

4. In *Quality*, make the following choices:
    a. In *Default Sample Rate*, select 44100 Hz.
    b. In *Default Sample Format*, select 16 bit.



Interface

Host: MME

Using: PortAudio V19.7.0-devel, revision unknown

Playback

Device: Speakers (Realtek(R) Audio)

Recording

Device: Microphone Array (Realtek(R) Au

Channels: 1 (Mono)

Quality

Project Sample Rate: 44100 Hz 44100

Default Sample Rate: 44100 Hz 44100

Default Sample Format: 16-bit

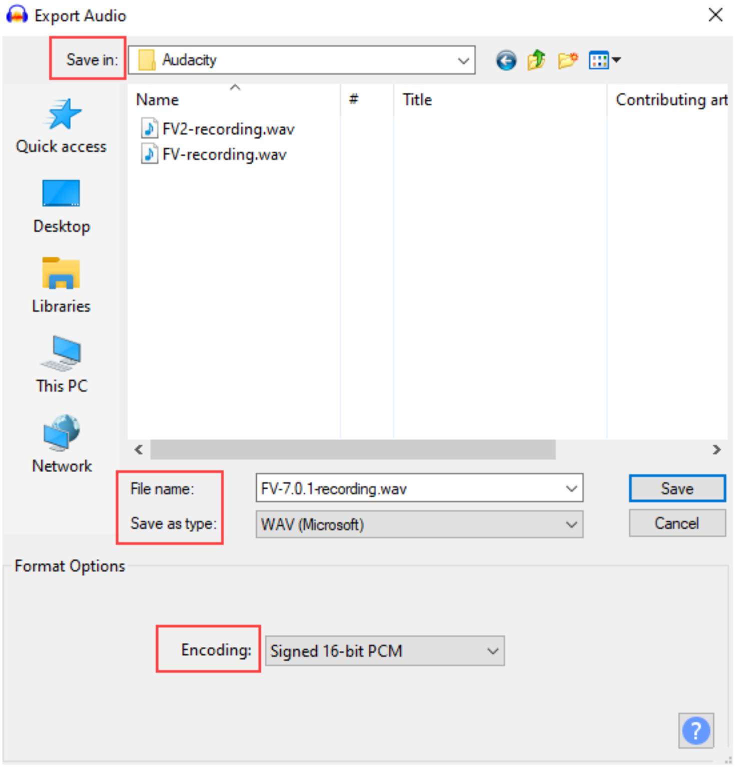
Latency

Buffer length: 100 milliseconds

Latency compensation: -130 milliseconds

1. Click *OK*.
2. When you are ready, record your message.
3. 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 *WAV (Microsoft)* or *MP3 Files*.

e. If you selected *WAV (Microsoft)*, then in *Encoding*, select *Signed 16-bit PCM*.



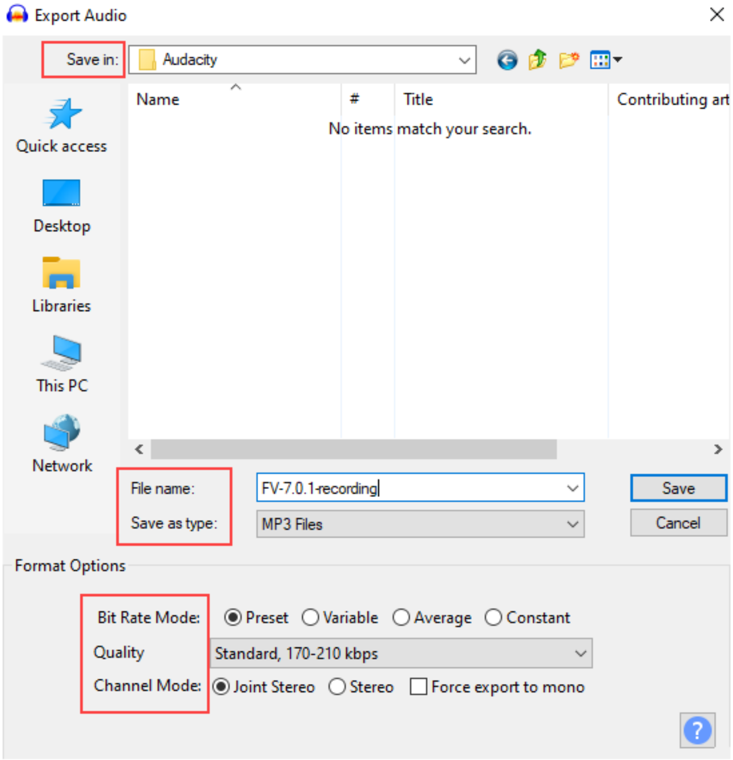
Save in: Audacity

File name: FV-7.0.1-recording.wav

Save as type: WAV (Microsoft)

Encoding: Signed 16-bit PCM

f. If you selected *MP3 Files*, then set the Format Options as shown in the following image.



Save in: Audacity

File name: FV-7.0.1-recording

Save as type: MP3 Files

Bit Rate Mode: ● Preset ○ Variable ○ Average ○ Constant

Quality: Standard, 170-210 kbps

Channel Mode: ● Joint Stereo ○ Stereo □ Force export to mono

g. Click *Save*.

h. If the *Edit Metadata Tags* dialog appears, you can add tags and click *OK*.
The recording is in a format that you can upload onto the FortiVoice unit (see Uploading or recording sound files on page 125).

Configuring LDAP settings

Phone System > LDAP lets you configure LDAP profiles and connectors.

This topic includes:

- Configuring LDAP profiles on page 130
- Configuring the LDAP connector on page 134
- Viewing LDAP contact list on page 137

Configuring LDAP profiles

The *LDAP Profile* 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 > LDAP > LDAP Profile*.

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.
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 > LDAP > LDAP Profile*.
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 134.
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`. 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 132
    - Configuring advanced options on page 133
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 about testing queries, see Testing LDAP profile queries on page 134.

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 settings on page 130.

1. Go to *Phone System* > *LDAP* > *LDAP Profile*.
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: • Active Directory • Lotus Domino • Open LDAP 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.

GUI field	Description
	- *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 settings on page 130.

1. Go to *Phone System* > *LDAP* > *LDAP Profile*.
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.

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* > *LDAP* > *LDAP Profile*.
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.

To clear the LDAP query cache

1. Go to *Phone System* > *LDAP* > *LDAP Profile*.
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 the LDAP connector

If you have contact or employee information in your LDAP server, you can configure the LDAP attribute mapping templates to retrieve the information and add it to the contact and extension lists. Before doing so, you must configure your LDAP server. For details, see Configuring LDAP settings on page 130.

To view the list of LDAP connectors and take some actions (sync and purge), go to *Phone System* > *LDAP* > *LDAP Connector*.

GUI field	Description
Clone	Click to duplicate an LDAP connector configuration.
Actions	• *Sync-Incremental* : Select an LDAP connector and click this button to display the newly-added and existing entries for that connector on the LDAP server. Select *New* or *Existing* to view the respective entries, and click *Import* let the FortiVoice unit synchronize the newly-added and existing entries from the LDAP server. If any existing entries are deleted on the LDAP server, they will not be removed on the FortiVoice unit during the synchronization. • *Sync-Full*: Select an LDAP connector and click this button to display the newly-added and existing entries for that connector on the LDAP server. Select *New* or *Existing* to view the respective entries, and click *Import* let the FortiVoice unit synchronize the newly-added and existing entries from the LDAP server. The FortiVoice unit retrieves all of the newly-added and existing entries from the LDAP server. • *Sync Report:* Select an LDAP connector and click this button to display the synchronization report between the FortiVoice unit and your LDAP server. • *Purge sync data*: Select an LDAP connector and click this button to remove the connector from the FortiVoice unit. You cannot remove a connector if the extension associated with it is used in other places.
Extension	Click to view the extensions generated based on the data retrieved from your LDAP server and non-LDAP extensions.
Name	Name of the LDAP connector.
LDAP Profile	The name of the LDAP profile that has your LDAP server information. For details, see Configuring LDAP settings on page 130.
Type	The type of the LDAP connector: extension or contact.
Schedule	The synchronization schedule between the FortiVoice unit and your LDAP server.
Last Sync Time	The latest synchronization time between the FortiVoice unit and your LDAP server.

To configure extension/contact connectors

1. Go to *Phone System* > *LDAP* > *LDAP Connector*.
2. Click *New* > *Extension Connector/Contact Connector* and configure the following:

GUI field	Description
Enabled	Select to enable the connector.
Name	Enter a name for the extension/contact connector.
LDAP profile	Select the LDAP profile that has your LDAP server information. You can add a new profile or modify the selected one. For details, see Configuring LDAP settings on page 130. The FortiVoice unit queries the LDAP server based on the information contained in the LDAP profile.

GUI field	Description
Schema	This option appears after you select the LDAP profile. Select the LDAP schema that defines the rules to govern the types of data that the LDAP server can hold. If you select *Active directory* or *Open LDAP*, the fields under *Search Criteria* and *Mapping* are populated. However, you can change them as needed.
Description	Click to enter any notes you have for this connector.
Search Criteria	You can use the auto-populated search attributes or enter your own search attributes for the data you want the FortiVoice unit to retrieve from the LDAP server.
Search base	Enter or browse for the search base to define the search starting point in the LDAP directory tree.
Search filter	Enter the complete query filters.
Scope	Select the LDAP search scope indicating the set of entries at or below the BaseDN that may be considered potential matches for a SearchRequest.
Max results	Enter the search size limit for the returning records.
Mapping	The mapping enables the FortiVoice unit to convert the data retrieved from the LDAP server into the FortiVoice extension or contact lists. You can use the auto-populated contact attributes or enter the contact attributes used in your LDAP server that match the FortiVoice attributes for extensions or contact lists. For example, you may enter "name" for *Display name* if that is what you have for display name in your LDAP server. You can click the *Retrieve LDAP attribute* icon (✎) beside each field to choose an LDAP server attribute. This section includes the following attributes: • *User ID*: This attribute supports letters, numbers, dots (.), and hyphens (-). • *Display name*: The extension name. For example, you may enter "name" for *Display name* if that is what you have for display name in your LDAP server. • *Number*: The extension number. • *Status*: The extension status. If we use an Active Directory (AD) setup as an example, this field can include *userAccountControl*. • *Value for enabled status*: FortiVoice uses this field to determine if the imported extensions need to be enabled or disabled. If we use an AD setup as an example, common values are *512* for enabled and *514* for disabled. If you use 512, it means that when you import extensions from your LDAP server and the AD returns a *userAccountControl* value of 512, FortiVoice enables the extension. If the AD returns any other value, FortiVoice disables the extension. If you leave the *Value for enabled status* field empty, FortiVoice disables the imported extensions. • *Email*: The extension email.
More	For extension connectors, under *More*, you can configure the *Time zone* and *Voicemail PIN* attributes based on the synchronization results with the LDAP server. • *Time zone*: • *Add entry*: Use this option to configure the **new** time zone attribute retrieved from the LDAP server.

GUI field	Description
	• *Fixed*: You can select your own time zone from the list. This value will not be updated with the value from the LDAP server during synchronization. • *Sync*: The current time zone value will be updated with the value from the LDAP server during synchronization. If the time zone value is not available on the LDAP server, the FortiVoice unit time zone (*Phone System* > *Setting* > *Location* > *Default time zone*) will be used by default. • *Update entry*: Use this option to configure the **existing** time zone attribute on your FortiVoice unit. • *Skip*: The current time zone attribute is ignored and will not be updated with the value from the LDAP server during synchronization. • *Sync*: The current time zone value will be updated with the value from the LDAP server during synchronization. If the time zone value is not available on the LDAP server, the FortiVoice unit time zone (*Phone System* > *Setting* > *Location* > *Default time zone*) will be used by default. • *Voicemail PIN*: • *Add entry*: Use this option to configure the **new** voicemail PIN attribute retrieved from the LDAP server. • *Fixed*: You can enter your own voicemail PIN. This value will not be updated with the value from the LDAP server during synchronization. • *Sync*: The current voicemail PIN value will be updated with the value from the LDAP server during synchronization. • *Generate*: Click to let the system generate a voicemail PIN. This value will not be updated with the value from the LDAP server during synchronization. • *Update entry*: Use this option to configure the **existing** voicemail PIN attributes on your FortiVoice unit. • *Skip*: The current voicemail PIN attribute is ignored and will not be updated with the value from the LDAP server during synchronization. • *Sync*: The current voicemail PIN value will be updated with the value from the LDAP server during synchronization.
Schedule	Set the time schedule for data retrieving and mapping.

3. Click *Create*.

Viewing LDAP contact list

After you have configured the LDAP contact connector and synchronized the FortiVoice unit with it, the generated FortiVoice contact list appears in *Phone System* > *LDAP* > *LDAP Contact*.

You can select a contact to view, modify, or delete it.

Clicking *LDAP* opens the *LDAP Connector* page.

For details about configuring contact connectors, see Configuring the LDAP connector on page 134.

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 profiles.

This topic includes:

- Configuring SIP profiles on page 138
- Modifying caller IDs on page 140
- Configuring phone profiles on page 142
- Configuring programmable key profiles on page 146
- Configuring RADIUS authentication profiles on page 150
- Configuring user privileges on page 151
- Configuring emergency zone profiles on page 156
- Scheduling the FortiVoice unit on page 158

Configuring SIP profiles

Configure the common SIP settings that can be applied to every SIP trunk and SIP device in your network.

Communicate with your VoIP service provider because the profile settings 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 about extensions, see Configuring extensions on page 183.

For information about SIP trunks, see Configuring trunks on page 229.

To configure a SIP profile

1. Go to *Phone System* > *Profile* > *SIP* and click *New.*
2. Select the SIP profile type.

3. 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, and Info.
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.
NAT	Select if the VoIP service provider supports SIP NAT translation.
T.38	Select if the VoIP service provider supports fax over VoIP network. This option is not available for every profile type.
Registration interval	To keep the extension registration status with the FortiVoice unit, keep the default value of extension registration time interval or enter the value in seconds as required by the FortiVoice unit. The default is 1800. The range is from 10 to 28800. For details about the priority of this setting, see Understanding the priority of extension registration and subscription interval settings on page 140.
Subscription interval	To keep the extensions’ subscription status with the FortiVoice unit, keep the default value of extension subscription time interval or enter the value in minutes as required by the FortiVoice unit. The default is 60. The range is from 10 to 1440. For details about the priority of this setting, see Understanding the priority of extension registration and subscription interval settings on page 140.
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 settings. For more information, see Configuring SIP settings on page 95. ⚠ The Zycoo X10 SIP Paging Gateway does not support secure RTP. *Secure RTP*: Select to provide encryption, message authentication and integrity, and replay protection to the FortiVoice Real-time Transport Protocol data. This option is not available for every profile type.
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.

4. Click *Create*.

Understanding the priority of extension registration and subscription interval settings

As there are multiple areas where you can modify the extension registration and subscription intervals within the FortiVoice UI, the following table shows the available setting options from the highest priority (1) to the lowest priority (3).

For example, if you configure the registration and subscription intervals using a SIP profile (priority 1) and survivability branch (priority 2), the FortiVoice unit uses the settings in the SIP profile because this option has a higher priority.

Priority	GUI path	Setting
1	*Phone System > Profile > SIP*	• Registration interval • Subscription interval For information about the settings, see Configuring SIP profiles on page 138.
2	*Managed System > Survivability > Survivability Branch > Survivability*	• SIP phone registration interval • SIP phone subscription interval For information about the settings, see the FortiVoice Local Survivable Gateway Deployment Guide.
3	*System > Advanced > SIP*	• Registration interval • Extension registration interval range • Internal extension registration interval • External extension registration interval • Subscription interval • Extension subscription interval range • Extension subscription interval For information about the settings, see Configuring SIP settings on page 95.

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 248.

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.
Match 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.

GUI field	Description
Number Modification	If you have entered a number or number pattern in *Match 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 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 or plus sign (+) before an extension. You can enter 15 digits or less. 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 183.
Map to new caller ID name	Enter the new caller ID name that you want to map to the one entered in the *Match caller ID name* 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 *Match number* field, enter the pattern of the extensions, such as 81xx.
4. In the *Match option* field, select *Match Number or Name*.
5. In the *Map to new caller ID name* field, enter the caller ID name to which you want to map, such as “Support”.
6. 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 183.

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

You cannot delete a default phone profile.

To view the list of phone profiles

1. Go to *Phone System* > *Profile* > *Phone*.
2. You can review the Name, Phone Model, and Description of the phone profiles.
3. The last column (Referenced) indicates if a phone profile is used by an extension.
   - A green dot means that at least one extension uses the phone profile.
   - A gray dot means that none of the extensions use the phone profile.

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 about phone directories, see Creating contacts on page 123.
Phone language	Select the language display on the phone.
Description	Enter any notes you have for this profile.

GUI field	Description
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 FortiFone phones have two network ports: LAN and PC. The recommended solution is to connect FortiFone phones to the switch using LAN port and connect the computer to the PC port of FortiFone phones. 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. *Priority for voice*: Enter the traffic service level recommended by the IEEE. Each number represents a traffic type. The range is from 0 to 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. *Data 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 to 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. *Enable LLDP transmit status*: Enable or disable the LLDP transmit status to allow listening or learning LLDP-MED from the switch only. This option applies to FortiFone FON-175, 375 ,475, 575, 670, 675, H25, and H35.
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.

GUI field	Description
	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 FON-175, 375, or 475 for *Phone model*, you can enable intercom barge to allow intercom drop-in in a phone conversation.
Screensaver timer	Select the screen saver time for the phone model you selected. This option varies for different phone models and is not available for all phone models.
Button transparency	Select the percentage of phone buttons' background color transparency. This option does not apply to all models.
Backlight time	Set the phone backlight time to illuminate the screen in low light conditions.
Hangup delay	Set the delay time to disconnect calls after hanging up. This option does not apply to all models.
Popup missed call	Enable if required. This option does not apply to all models.
Keep alive	Enter a value for FortiFone to send a packet to the FortiVoice unit at the interval of the entered keep alive value to keep the firewall ports open at all time. This is to ensure that calls are not missed due to the registration time change for external IP extensions. For example, if you enter 40, FortiFone will send a 2 byte packet every 40 seconds to keep the firewall ports open. This option does not apply to all models.
External keep alive	This option is available when you select FortiFone FON-x80 for *Phone model*. For external FortiFone FON-x80 extensions, the default keep alive option is 40 seconds. This is to ensure that calls are not missed due to the registration time change for external IP extensions.
DST type	Set the daylight saving time (DST) for the phone. This option does not apply to all models. • *Disabled*: DST on the phone is disabled. • *Automatic*: DST on the phone is automatically set based on your location.
Appearance Transfer	Choose the call transfer mode for the extension appearance programmable key of FortiFone FON-x80 phones. The default is *Blind*. • *Blind*: Allows you to transfer a call without speaking to the person receiving the transfer. • *Attended*: Allows you to announce the call to the person receiving the transfer before completing the transfer. For information about extension appearance programmable keys, see Configuring programmable key profiles on page 146.
Registration retry interval	This option applies to FON-x80/x80B phones only. Select the setting to specify the time interval for sending another registration retry after a phone registration failure: • *Phone Defined*: The phone resends another registration retry using its own default value. This default value is not visible to the user or administrator. • *Automatic*: The phone resends another registration retry and adjusts the interval

GUI field	Description
	dynamically. • *Custom*: Select the number of seconds for sending another registration retry. The range is from 120 to 600 seconds.
Use pound(#) as dial or send key	Select to enable this option. If you enable this option, users can use the pound key (#) to invoke dialing. For example, when the user presses 19001#, the phone calls extension 19001. If you disable this option, users can use the pound key (#) as a phone number prefix such as #19002. This option does not apply to all models.
Call Busy Tone	This option is enabled by default. This option applies to FON-x80/x80B phones only. • When this option is enabled and the caller's phone receives a busy signal, the phone plays a busy tone, and the screen displays "Busy". • If you disable this option and the caller's phone receives a busy signal, the phone displays the main screen instead of playing a busy tone.
TCP auto switch	This option applies to FON-x80/x80B phones only. If the phone uses TCP, this option does not have any impact on sending SIP requests. If the phone uses UDP and you enable this option, you allow the phone to send SIP requests that are larger than 1300 bytes using TCP. However, this switch is not permanent meaning that the phone will use UDP to send any subsequent SIP requests that are 1300 bytes or smaller.
Call Waiting Tone	This option applies to FON-x80/x80B phones only. Select to enable this call waiting tone option. To allow the phone to use this option, you need to also enable *Call waiting* on the extension (see Setting extension user preferences on page 210). • If you enable this option, the following behavior applies: When a second incoming call comes in while the phone user is already on a call, the phone displays the new call information about the screen and plays a beep (call waiting tone). • If you disable this option, the following behavior applies: When a second incoming call comes in while the phone user is already on a call, the phone displays the new call information about the screen but does not play a beep (call waiting tone).
Phone Image Setting Background image	This option allows you to change the background image on FortiFone FON-x80 and FortiFone FON-W80B. This option only appears when you edit a phone profile. Click *Change* to upload the image. Click *Reset* to restore the default image setting. File requirements for a background image: • Supported format: JPEG • Supported sizes (width x height): • FON-280B: 320 x 240 pixels • FON-380/380B: 480 x 320 pixels

GUI field	Description
	- FON-480/480B: 480 x 272 pixels - FON-580/580B: 480 x 272 pixels - FON-W80B: 240 x 320 pixels
Hotel	If you select FortiFone FON-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.
Soft Button In Idle Status	Optionally, enable the four soft buttons and make them functional in idle status. This option does not apply to all models.
Phone Password	Enter a password for the phone users to access their phone web GUIs and configure the advanced settings on the phones. This only applies to the supported phones.

3. Click *Create*.

Configuring programmable key profiles

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

After 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 key 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
Name	The name of the profile.
Phone model	The phone model of the profile.
Description	Notes for this profile.
Number of Reserved Line keys	Select the phone lines you want to reserve. For example, if you select 2 for this phone, programmable keys 1 and 2 become reserved for phone lines.
Mode	
Number of pages to be used on this phone	Select the number of pages for the programmable keys. This option appears for certain FortiFone models only.
Page (tab)	Fields display depending on the phone model.
Option	The programmable key number of the phone.
Mode	- User: Allows the user to set a programmable key using the FortiVoice user portal and endpoints (FortiFone desk phone and FortiFone softclient for desktop).

GUI field	Description
	- Admin (with User Assigned function): Allows the user to set a programmable key using a FortiFone desk phone. - Admin: Allows you to set a programmable key with a function, resource and label, as applicable. The user cannot make changes to that programmable key.
Function	Select the function assigned to this key. For more information, see Programmable key descriptions on page 147.
Resource	For some functions, you need to enter 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. For more information, see Programmable key descriptions on page 147.
Label	For some functions, you can add an explanatory label for the key. For more information, see Programmable key descriptions on page 147.
Push to talk (tab)	This option appears for the FON-W80B model only.
Mode	- *User*: Allows the user to set the push-to-talk button using the FortiVoice user portal, FON-W80B phone, and FortiFone softclient for desktop. - *Admin (with User Assigned function)*: Allows the user to set the push-to-talk button using the FON-W80B phone. - *Admin*: Allows you to set the push-to-talk button with a function, resource and label, as applicable. The user cannot make changes to that key.
Function	Select the function for the push-to-talk button. Your choices are: - System speed dial - User speed dial - Speed dial - Redial For more information, see Programmable key descriptions on page 147.
Resource	For some functions, you need to enter information in this field based on your phone configuration. For more information, see Programmable key descriptions on page 147.
Label	For some functions, you can add an explanatory label for the key. For more information, see Programmable key descriptions on page 147.

5. Click *OK*.

Programmable key descriptions

Function	Description	Resource	Label
Call forward	Enables or disables and configures the call forward function.	Stays blank.	Edit the label or keep the default label (Call forward).

Function	Description	Resource	Label
DTMF	The DTMF function is only available during a call. DTMF (dual-tone multi-frequency) refers to the touch tone digits on the keypad of your desk phone. When you are on a call and you press the DTMF key, the system dials the configured DTMF digits. This key is useful when you need to enter consistent codes at an interactive voice response (IVR) system.	Enter the DTMF digits to dial when you press this programmable key on your phone.	Edit the label or keep the default label (DTMF).
Extension appearance	Allows you to do the following actions: • Monitor the status of the selected extension (idle, ringing, in use, DND, and on hold). • On FortiFone FON-x80 phones, you can transfer a call to the selected extension using one of the following transfer types: • Blind: Allows you to transfer a call without talking to the person receiving the transfer. • Attended: Allows you to announce the call to the person receiving the transfer and then complete the transfer. • You set the transfer type in Configuring phone profiles on page 142. The default is Blind (in Appearance Transfer).	Select an extension from the list.	Edit the label or keep the one associated with the selected extension. This field supports 63 characters or less.
Intercom	The intercom function works for internal extensions (not for external extensions). Uses the phone speaker of a local extension as an intercom.	Stays blank.	Edit the label or keep the default label (Intercom).
Line appearance	Monitors the status of a line (available, busy, or on hold).	Select a line.	Edit the label or keep the one associated with the selected line (or trunk).
Park	Places the call into the first available call park slot. You hear a prompt telling you which slot the call has been parked in.	Stays blank.	Edit the label or keep the default label (Auto park).

Function	Description	Resource	Label
Park appearance	Allows the following actions: • Monitor the selected call park slot to know when there is a call parked. • Retrieve a parked call.	Select the park slot to monitor.	Edit the label or keep the one associated with the selected line (or slot).
Private Hold	Puts a call on hold.	Stays blank.	Stays blank to use the Private Hold label.
Record	Before using the Record function, make sure to apply a profile (with the personal recording function enabled in Monitor/Recording) to the extension. For more information, see Configuring user privileges on page 151. Records a phone call.	Stays blank.	Stays blank to use the Record label.
Redial	Available for the FortiFone FON-W80B (push-to-talk button) only. Places a call to the last dialed extension or phone number.	Stays blank.	Stays blank.
Reserved for line	By default, the FortiVoice phone system reserves the first two programmable keys for lines on the phone to allow extension users to monitor their own calls on those lines. You can use the Reserved for line function to program the appearance of additional accounts (lines).	Choose an account.	Edit the label or keep the one associated with the selected account.
Shared line appearance	For information about shared line appearance (SLA), see Appendix A: Shared line appearance on page 370.		
Speed dial	Places a call to the specified extension or phone number.	Enter an extension or phone number.	Edit the label or keep the default (Speed dial).

Function	Description	Resource	Label
System speed dial	Places a call to the specified extension or phone number.	Make a selection from the configured Mapping speed dials on page 301.	FortiVoice shows the same name as the selection in Resource.
Twinning	Before using the Twinning function, make sure to apply a profile (with the twinning function enabled in Basic Setting) to the extension. For more information, see Configuring user privileges on page 151. Rings an external phone along with office phone, so you can answer the call at either phone. Enables or disables the twinning feature. With the twinning feature enabled, an external phone rings along with an office phone, so you can answer the call at either phone.	Stays blank.	Edit the label or keep the default label (Twinning).
User speed dial	Places a call to the specified extension or phone number. Phone users configure this key using the FortiVoice user portal.	For more information, see the FortiVoice User Portal Guide.	

Configuring RADIUS authentication profiles

The FortiVoice unit supports RADIUS authentication method by using the RADIUS profiles that you configure.

To configure a RADIUS profile

1. Go to *Phone System* > *Profile* > *RADIUS*.
2. Click *New.*
3. Configure the following:

GUI field	Description
Profile name	Enter a name for this profile.
Server name/IP	Enter the fully qualified domain name (FQDN) or IP address of a server that will use RADIUS method to authenticate users.
Server port	Enter the port number on which the authentication server listens. You must change this value if the server is configured to listen on a different port number, including if the server requires use of SSL. The default port is 1812.
Protocol	Select the authentication scheme for the RADIUS server.

GUI field	Description
Server secret	Enter the secret required by the RADIUS server. It must be identical to the secret that is configured on the RADIUS server.
Server requires domain	Enable if the authentication server requires that users authenticate using their full email address (such as user1@example.com) and not just the user name (such as user1).

4. Click *Create*.

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 about extensions, see Configuring extensions on page 183.

To configure a user privilege

1. Go to *Phone System* > *Profile* > *User Privilege*.
2. Click *New*.
3. 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 auto-provisioning for FortiFone phones and gateways on page 99. 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.
Configure programmable phone feature key/PFK	Select to enable configuring the feature access codes. For more information, see Modifying feature access codes on page 324.
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 210.

GUI field	Description
Softclient API login	Select to enable FortiVoice softclient to log into the FortiVoice unit.
Auxiliary Extensions	When you add an auxiliary phone to your extension, you have two phones with the same extension number. The phones will ring at the same time but you can only use one phone to answer the call. This function is useful when you want to access the same extension from two different locations. For more information, see Configuring auxiliary phones on page 197.
Call forward	Select to enable the call forward function on an extension's user privilege. When you configure this function, you enter the number that you want your calls to be forwarded to. For more information about setting call forward on an extension, see Setting extension user preferences on page 210. If you want to disable the PIN, see Call forwarding PIN on page 156.
Call park	Select to enable the call park function on an extension's user privilege. When you park a call, the call is on hold and any other local extension can retrieve that call. For more information, see Configuring call parking on page 315.
Voicemail schedule greeting	Select to enable the option to set a voicemail greeting according to a schedule. The extension user can complete the configuration using the FortiVoice user portal (see the Setting voicemail options section in the FortiVoice User Portal Guide).
Video call	Select to enable the video call function on an extension.
Operator Role	Select to enable an extension user to process phone calls using the operator console accessible from the FortiVoice user portal. 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 appears at the top of the FortiVoice user portal window for that extension. Clicking the button lets the user process phone calls on the web.
Voicemail	Select to enable the voicemail service.
Maximum messages	Enter the number of voicemails allowed.
Voicemail retention days	Enter the number of days to keep the voicemails.
Voicemail password	If enabled, phone users must enter a password to access their voicemail. If disabled, phone users can access their voicemail without entering a password.
Voicemail email format	Select the voicemail file format. When an extension receives a voicemail, FortiVoice can send an email notification with the voicemail as an attachment. For notification options, see Setting extension user preferences on page 210.
Music	
Music on hold	Select a music on hold file or stream, or create a new one. For more information, see Managing phone audio settings on page 125.

GUI field	Description
Early media	Select a music on hold file or stream, or create a new one. FortiVoice plays your selection instead of the ringback tone which is the audio that the caller hears while waiting for the called destination to answer their call. For more information, see Managing phone audio settings on page 125.
Fax	Select to set the fax rules for users. For information about fax, see Configuring fax on page 315.
Maximum incoming messages	Enter the number of incoming faxes allowed.
Maximum incoming fax retention days	Enter the number of days to keep the incoming faxes.
Maximum outgoing messages	Enter the number of outgoing faxes allowed.
Maximum 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 about account code, see Configuring account codes on page 179. 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 179. 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.
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.** Select *Enabled* to activate this restriction. **3.** Enter a name for this call restriction. The name can contain numbers, letters, and underscores. The maximum length is 63 characters. **4.** Enter the area code that you want to set the restriction. The area code can contain numbers 0 to 9, +, *, and # followed by an optional sequence of $. The maximum length is 63 digits. **5.** Select the permission for the area code. For more information, see Call Restriction on page 153. **6.** Click *Create*.
Miscellaneous	*Maximum concurrent calls*: Set the maximum number of concurrent incoming and outgoing calls on the extension. The range is 1 to 10. The default is 4.

GUI field	Description
Monitor/Recording	
Personal recording	Select to allow users to configure personal recording of their incoming and outgoing calls on the FortiVoice user portal.
System recording	Select to allow administrators to configure system recording of their incoming and outgoing calls on the FortiVoice GUI.
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. For information about how to barge a call, see Listen/Barge on a call on page 326.
Call barge option	If you select *Allow barging*, choose a barging method. For information about how to barge a call, see Listen/Barge on a call on page 326.
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 36. • *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). By selecting this option, the old extension is taken over by the new extension on this phone. After logging out the phone with the hot-desking phone authentication, the old extension is recovered. However, outgoing calls still display the hotd-esking extension 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 about programmable phone keys, see Configuring phone profiles on page 142.
User Portal	Enable or disable the user portal and select the features for it. Only the selected ones will appear for the extension to which this user privilege is applied.
Directory	
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.

GUI field	Description
Lookup directory	Select to enable a user to view the phone directory of the local office.
Lookup directory in remote office(s)	Select to enable a user to view the phone directories of remote offices.
Directory/subdirectory	Select the directory or subdirectory that you want to include in the user privilege. If you select a subdirectory, make sure to also make your selection in the *Include subdirectory* setting in Configuring system capacity on page 120.
Entitlement	This option controls the use of unified communication and enhanced call center features. • *Unified communication*: Select to allow the use of third-party communication applications, including: • Microsoft Teams • Presence for desktop application • Instant messaging service and clients on endpoints • Video conferencing service and client on endpoints • Screen sharing • File sharing • *Enhanced call center*: Select to allow the use of enhanced call center features, including: • Agent console for desktop application • Enhanced FortiVoice IVR • Salesforce integration
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 297.
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 about paging, see Configuring auto attendants on page 297.
Trusted hosts type	Select the type of the subnet that can register with the SIP server. Only extensions on the specified subnet can register with the SIP server. If you select *User defined*, enter the information in *Trusted hosts*.

GUI field	Description
Trusted hosts	Enter the IP address and netmask of the subnet that can register with the SIP server. You can add multiple trusted hosts.
Permitted outgoing rules	Enable or disable all available outbound calling rules. For more information about calling rules, see Configuring outbound dial plans on page 254.
Do not disturb	If enabled, you allow extensions with this user privilege to use this function. If disabled, you do not allow extensions with this user privilege to use this function. If you want to enable this function on an extension, see Setting extension user preferences on page 210.
Call forwarding PIN	If enabled, phone users must enter their voicemail PIN to set up call forwarding. If disabled, phone users can set up call forwarding without entering their voicemail PIN. To enable the call forwarding function in a user privilege, see Call forward on page 152.

4. Click *Create*.

Configuring emergency zone profiles

You configure an emergency zone profile to include detailed caller ID, contact, and network information.

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.
Primary Caller ID	Enter a number to display on the destination phone when a user dials the emergency number, such as 911.
Secondary Caller ID	Enter a number to display on the destination phone when a user dials the emergency number, such as 911. This number can be used for concurrent calls.
DID callback type	Select how you want FortiVoice to route the inbound callback from an emergency operator: • *None*: FortiVoice follows the inbound DID mapping. • *Default Extension*: FortiVoice calls the extension that you specify in *Default DID extension*. • *Emergency Caller*: FortiVoice calls the extension of the emergency caller. FortiVoice keeps this extension in memory for the time period specified in *DID callback hold time* (see Setting FortiVoice location, contact, and emergency information on page 114). If the emergency operator calls back after the DID callback hold time has expired, FortiVoice uses the inbound DID mapping to route the call. • The default is *None*.

GUI field	Description
Default DID extension	FortiVoice uses this option to route inbound callbacks from an emergency operator. If you selected *Default Extension* in *DID callback type*, enter a phone number (maximum of 16 digits). FortiVoice dynamically generates the direct inward dialing (DID) mapping.
Description	Enter any notes you have for this profile.
Setting	
Do Nothing	Select this option if you do not want the FortiVoice phone system to send an alert email when an extension user makes an emergency call.
Send an Alert Email	Select this option if you want the FortiVoice phone system to send an alert email when an extension user makes an emergency call.
Emergency contact emails	If you selected *Send Alert Email*, enter the email address of the emergency contact. You can click + and add more addresses.
Emergency barge number	Enter an authorized user's extension number to be dialed. When an ongoing emergency call is in progress, the phone of the authorized user also rings. This user can listen to the call and talk, if necessary.
Emergency message group number	Select a message group number for emergency contact. This number is dialed when an emergency call is made. For more information about message groups, see Creating message groups on page 222.
Contact Information	Enter the emergency contact information for the profile.
Dynamic Network Match	When you enable this function, you allow the FortiVoice phone system to identify where the phone of the emergency caller is on the network. When a phone user calls an emergency number, the FortiVoice phone system checks where the calling phone is and assigns a matching emergency zone profile to the phone. This assignment is useful when phone users move their phones to different places on the network. When you enable this function, make sure to complete the following requirements: • Fill in the *Network location match* settings. See the following table row. • Set the *Emergency zone type* as *Dynamic* in the following sections, if they apply to your network deployment: • IP extensions: Configuring IP extensions on page 183 • Auxiliary phones: Configuring auxiliary phones on page 197 • Managed extensions: Modifying managed extensions on page 199 • Fax extensions: Configuring fax extensions on page 207
Network location match	Select either *IP mask* or *IP range*.
IP/Netmask	If you selected *IP mask* as the *Network location match*, enter the IP address and netmask.
Start IP	If you selected *IP range* as the *Network location match*, enter the start IP address.
End IP	If you selected *IP range* as the *Network location match*, enter the end IP address.

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 auto attendant on the system level. You can modify the default schedules, namely *after_hour*, *business_hour* , and *holiday*, except for the *any_time*. You cannot delete default schedules.

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

For information about dial plan, see Configuring call routing on page 248.

For information about virtual numbers, see Working with virtual numbers on page 227.

For information about call management, see Setting extension user preferences on page 210.

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 FortiFone desk phones (including Cisco CP-7841 and CP-8841 phones with version number 12.x) and multi-cell FortiFone phones in a central place for easy management.

This topic includes:

- Configuring desk phones on page 159
- Configuring multicell-phone FortiFone phones on page 161
- Configuring single-cell FortiFone phones on page 164

Configuring desk phones

You can configure desk phones 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 desk phones, go to *Phone System* > *Device* > *Phone*.

GUI field	Description
Delete	Select one or more phone records and click this button to remove them all at once.
Action	• *Assign to New Extension*: Select a phone with a *Not Assigned* management 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 phone to new extension on page 160. • *Assign to Existing Extension* :Select a phone with a *Not Assigned* management status, click this option to assign this phone to an existing extension. For more information, see To assign a phone to an existing extension on page 160. • *Assign to Multi-cell Device*: Select a multi-cell device (for example, FortiFone 870i) with a *Not Assigned* management status and click this option to add an extension and assign this phone to the extension at the same time. For more information, see Configuring multicell-phone FortiFone phones on page 161. • *Assign as Auxiliary to Existing Extension:* Select a phone with a *Not Assigned* management status and click this option to assign it to an existing extension as an auxiliary device. For more information, see To assign a phone as an auxiliary to an existing extension on page 160. • *View Phone Configuration*: Select a phone with an *Assigned* management status and click this option display its configuration file. If you select a Cisco phone, you can select *Enterprise* or *3PCC*. • *View accounts*: For phones to which multiple extensions can be associated, such as FON-850/860/870 and FON-D70/D71/D72, click this option to view the associated extensions. This option is only active when a phone has multiple extensions associated with it. • *Export*: Select to save the phone list in `csv` format.
Extension	When a phone is registered with an extension, this column shows 👤. Some phone models, such as the FON-D71, can have multiple registered extensions. In this case, the icon also shows the number of registered extensions. For example, 👥 2.
MAC Address	The Media Access Control address (MAC address) of the phone.
Phone Model	The phone brand and model.
Phone Profile	The profile for this phone. See Configuring phone profiles on page 142.
Management	Displays if the phone has been *Assigned* or *Not 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.

GUI field	Description
Phone Info	The model, MAC address, and firmware version of the phone for this extension.
Last Phone Config Update	The date and time of the last configuration update that FortiVoice has completed on the phone.
Version	The firmware version of the phone.

To add a desk phone

1. Go to *Phone System* > *Device* > *Phone*.
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 phone profiles on page 142.
Description	Enter any notes about the phone.

3. Click *Create*.

To assign a phone to new extension

1. Go to *Phone System* > *Device* >*Phone*.
2. Go to the *Management* column and select a phone identified as *Not Assigned*.
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 183.
5. Review the phone details and click *Next*.
6. Review the summary and click *Finish*.
7. If the phone does not show the extension after a few minutes, reboot the phone.

To assign a phone to an existing extension

1. Go to *Phone System* > *Device* > *Phone.*
2. Go to the *Management* column and select a phone identified as *Not Assigned*.
3. Click *Action* and select *Assign to Existing Extension.*
4. Select the extension to associate with the phone and click *Next*.
5. Review the extension details and click *Next*. For details, see Configuring IP extensions on page 183.
6. Review the phone details and click *Next*.
7. Review the summary and click *Finish*.
8. If the phone does not show the extension after a few minutes, reboot the phone.

To assign a phone as an auxiliary to an existing extension

1. Go to *Phone System* > *Device* > *Phone*.
2. Go to the *Management* column and select a phone identified as *Not Assigned*.
3. Click *Action* and select *Assignas Auxiliary to Existing Extension.*
4. Select the extension to associate with the phone and click *Next*.
5. Review the extension details and click *Next*. For details, see Configuring IP extensions on page 183.
6. Review the phone details and click *Next*.

7. Review the summary and click *Finish*.
8. If the phone does not show the extension after a few minutes, reboot the phone.

Configuring multicell-phone FortiFone phones

The FortiVoice unit supports the following two types of multi-cell FortiFone phones:

- FortiFone-870i
- FortiFone-D72

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).

Each base FortiFone-D72 can support up to 8 handsets. You can configure a FortiFone-D72 to work with the FortiVoice unit by adding a FON-D72-M manager, at least one FON-D72-B base, and one FON-D71-H handset.

Prerequisites

The following prerequisites must be met for the FortiFone-870i and FortiFone-D72 configuration to work:

Multi-cell phone	Prerequisites
FortiFone-870i	• FortiVoice v6.0 build 127 or later. • FortiVoice auto provisioning is enabled (see Configuring auto-provisioning for FortiFone phones and gateways on page 99). • FortiFone-870i firmware 3.23 or later. • Network connectivity available between FortiFone-870i and the FortiVoice unit.
FortiFone-D72	• FortiVoice v6.0.7 build 253 or later. • FortiVoice auto provisioning is enabled (see Configuring auto-provisioning for FortiFone phones and gateways on page 99). • Network connectivity available between FortiFone-D72 and the FortiVoice unit.

Follow the FortiFone-870i and FortiFone-D72 guides to configure the phones first. After you connect the phone to the network, you can configure it on the FortiVoice unit.

Configuring the FortiFone-870i

Configure the FortiFone-870i on multiple GUI pages.

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* > *Phone.*
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 phone to new extension on page 160.

8. For *Assign to Existing Extension*, see To assign a phone to an existing extension on page 160.
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* > *Phone*.
11. Go to the *Management* column, select the FortiFone 870i station that is identified as *Not Assigned*, and 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.

Configuring the FortiFone-D72

You can configure a FortiFone-D72 to work with the FortiVoice unit by adding a FON-D72-M (manager), at least one FON-D72-B (base), and one FON-D71-H (handset). This solution includes the following four steps:

- To configure the FON-D72-M on page 162
- To configure the FON-D72-B on page 163
- To configure the FON-D71-H handset as an extension with the FortiFone-D72 on page 163
- To activate the FON-D72-M and register handsets on page 164

For more information about the FortiFone-D72, see FON-D72 User Guide.

To configure the FON-D72-M

1. Connect the FON-D72-M to the network using a POE connection.
2. Log in to the FortiVoice GUI.
3. Go to *Phone System* > *Device* > *Phone*.
   The FON-D72 is auto discovered and displays as a device with the *Not Assigned* management status.
4. Right-click the FortiFone-D72 and select *Assign to Multi-cell Device*.
5. Configure the following:

GUI field	Description
Enable	Select to activate the phone.
Device role	Select *DECT Manager* for FON-D72-M.
IP address	Enter the IP address of the FON-D72-M if it is not automatically filled out.
Default manager	Enable to make the FON-D72-M as the default manager of the FortiFone-D72 configuration.
Description	Enter any notes about the phone.

6. Click *OK*.

In the *Phone Model* column, a green icon appears beside FortiFone-D72 indicating that it is the DECT Manager.

To configure the FON-D72-B

1. Connect the FON-D72-B to the network using a POE connection.
2. Log in to the FortiVoice GUI.
3. Go to *Phone System* > *Device* > *Phone.*
   A new FON-D72 is auto discovered, displays as a device with the *Not Assigned* management status, and has a different MAC address than the DECT Manager.
4. Right-click the FortiFone-D72 and select *Assign to Multi-cell Device*.
5. Configure the following:

GUI field	Description
Enable	Select to activate the phone.
Device role	Select *Base* for FON-D72-B.
Sync cluster	Select the ID for a phone group. A sync cluster is comprised of a number of base stations within the DECT multi-cell system that synchronize with each other to enable handover, roaming, list access, and load balancing. Only phones in the same cluster can talk with each other. For detailed information, see FON-D72 User Guide.
Sync level	Select the sync level for a phone group. Each base station is assigned to a corresponding sync level. Sync level is based on the distance between bases. Only one base can be sync level 1, then every other base would be 2-10, based on where they are located. For detailed information, see FON-D72 User Guide.
Primary	Select the MAC address of the default DECT Manager if it is not automatically populated.
Default manager	Enable to make the FON-D72-M as the default manager of the FortiFone-D72 configuration.
Description	Enter any notes about the phone.

6. Click *OK*.

   In the *Phone Model* column, a gray icon appears beside FortiFone-D72 indicating that it is the base.

To configure the FON-D71-H handset as an extension with the FortiFone-D72

1. Log in to the FortiVoice GUI.
2. Go to *Phone System* > *Device* > *Phone.*
3. Right-click the FortiFone-D72 that is the DECT Manager and select *Assign to New Extension*.
4. Configure the following:

GUI field	Description
Number	Enter the extension number of the FON-D71-H.

GUI field	Description
	For information about extension configuration, see Configuring IP extensions on page 183.
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 notes about the phone.
User Setting	Do not do anything.

5. Click *Next*.
6. Verify the information and click *Next*.
7. Review the summary.
8. Click *Finish*.

To activate the FON-D72-M and register handsets

1. Enter the IP address of the FON-D72-M in a web browser.
2. Log in using `admin` as the username and `23646` as the password.
3. Go to *Handset & Account* > *Registration Center*.
4. Click *Start Now*.
5. Power on the FON-D71-H handset and press the *Reg* button.
   The handset will search and find the FON-D72-M, register, and display the created extension number and name.

Configuring single-cell FortiFone phones

The FON-D71 is a single-cell digital enhanced cordless telecommunications (DECT) solution.

A FortiFone-D71-B base can support up to eight FortiFone-D71-H handsets.

The FON-D71-B base registers with the FortiVoice phone system. You configure a FortiFone-D71-H handset as an extension with the FON-D71-B base.

Internal and external extensions

When the FON-D71-B base and FortiVoice phone system are on the same network, you are configuring an internal extension. The FON-D71 phone supports a plug-and-play installation and automatically downloads its configuration from the FortiVoice phone system.

When the FON-D71-B base and FortiVoice phone system are on different networks, you are configuring an external extension. You are manually connecting the FON-D71-B base with the FortiVoice phone system.

Prerequisites

Make sure to meet the following prerequisites:

- Make sure that the FortiVoice phone system is using version 5.3.18 or later.
- Make sure that the FortiVoice auto provisioning is enabled (see Configuring auto-provisioning for FortiFone phones

and gateways on page 99).

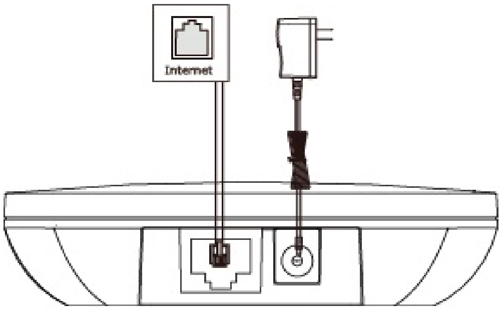
- Install the battery in the FortiFone-D71-H handset.

Workflow

To complete the configuration of a single-cell FortiFone phone, perform the following procedures:

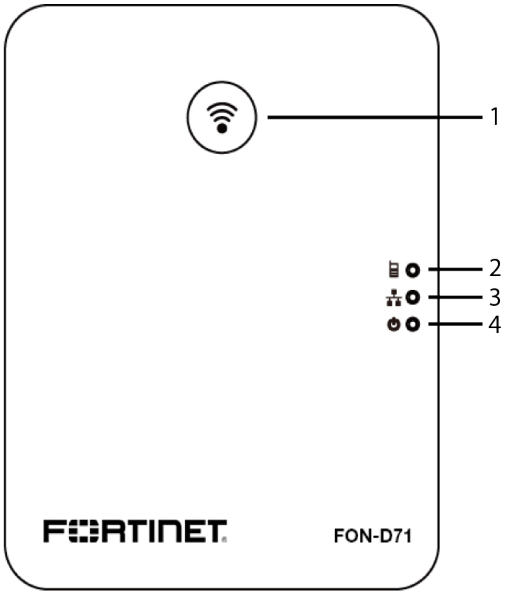
1. To add the FON-D71-B base on page 165
2. To register the FON-D71-H handset with the FON-D71-B base on page 165
3. To connect the FON-D71-B base with the FortiVoice phone system for an external extension on page 166
4. To configure the FON-D71-H handset as an internal or external extension to use with the FON-D71-B base on page 167

To add the FON-D71-B base



1. On the FON-D71-B base, connect the Ethernet cable to the internet port.
2. Connect the other end of the Ethernet cable to your router, switch, or other internet source.
3. If your network supports power over Ethernet (PoE), a power adapter is not required.
4. If your network does not support PoE, you need a DC power adapter (5 V and 600 mA).
   a. Connect the power adapter to the power jack on the FON-D71-B base.
   b. Connect the other end of the power adapter to the power outlet.
5. If the FON-D71-B base and FortiVoice phone system are on the same network, verify that the FON-D71-B base is connected to the FortiVoice phone system:
   a. Log in to the FortiVoice GUI.
   b. Go to *Phone System* > *Device* > *Phone*.
   c. Review the list of phones to make sure that it includes the newly added FortiFone-D71 and the Management column shows a *Not Assigned* status.
6. If the FON-D71-B base and FortiVoice phone system are on different networks, you will connect both systems later in the workflow.

To register the FON-D71-H handset with the FON-D71-B base



No.	Item	Description
1	Paging key	• Locates a misplaced handset. • Toggles the registration mode. • Resets the base to factory settings.
2	Registration LED	Indicates the mode of the base station: • Fast flashing green — paging mode. • Slow flashing green — registration mode. • Solid green — at least one handset is registered to the base.
3	Network status LED	Indicates the network status: • Slow flashing green — network is unavailable. • Solid green — network is available. • Off — base station is powered off.
4	Power indicator LED	Indicates the power status of the base station: • Slow flashing green — firmware is updating. • Solid green — base station is powered on. • Off — base station is powered off.

1. Turn on the FON-D71-H handset.
   The handset displays *Searching for the base*.
2. On the base, press and hold the *Paging* key until the registration LED is flashing to enter the registration mode.
   The handset discovers and registers with the base.
3. After the registration is complete, the phone displays the handset ID (such as *Handset 1*).

To connect the FON-D71-B base with the FortiVoice phone system for an external extension

If you are using an internal extension, the FON-D71-B base is already connected to the FortiVoice phone system. Skip this procedure and go To configure the FON-D71-H handset as an internal or external extension to use with the FON-D71-B base on page 167.

1. On the FON-D71-H handset, press the *Down* navigation button.
2. Select *Base* and press *OK*.
3. Take note of the IP address of the FON-D71-B base.
4. Go to your web browser and enter:
   ```
   https://<ip_address>
   ```
   Where <ip_address> is the IP address of the FON-D71-B base.
5. In *Username*, enter `admin`.
6. In *Password*, enter `23646`.
7. Go to *Settings* > *Auto Provision*.
8. In the *Server URL*, enter the public IP address or FQDN of the FortiVoice phone system.
9. Click *Confirm*.
   The FON-D71-B base connects to the FortiVoice phone system.

To configure the FON-D71-H handset as an internal or external extension to use with the FON-D71-B base

1. Log in to the FortiVoice GUI.
2. Go to *Phone System* > *Device* > *Phone.*
3. Right-click *FortiFone-D71* (this is the base) and select either *Assign to Existing Extension* and the extension, or *Assign to New Extension*.
4. Configure the following:

GUI field	Description
Enabled	Select to activate the extension.
Number	Enter the extension number of the FON-D71-H. For more information about the extension configuration, see Configuring IP extensions on page 183.
User ID	Displays the user ID.
Display name	Enter the name displaying on the extension. This is usually the name of the extension user. You can click + to add a caller ID for external calls or emergency calls.
Description	Enter any notes about the phone.
User Setting	Do not change the settings.

5. Click *Next*.
6. Go to *Location*. For an internal extension, click *Internal* or for an external extension, click *External*. Verify that the *Handset ID* is correct. For example, if you are configuring the first handset, the Handset ID must be 1.
7. Click *Next*.
8. Review the summary.
9. To save the changes, click *Finish*.

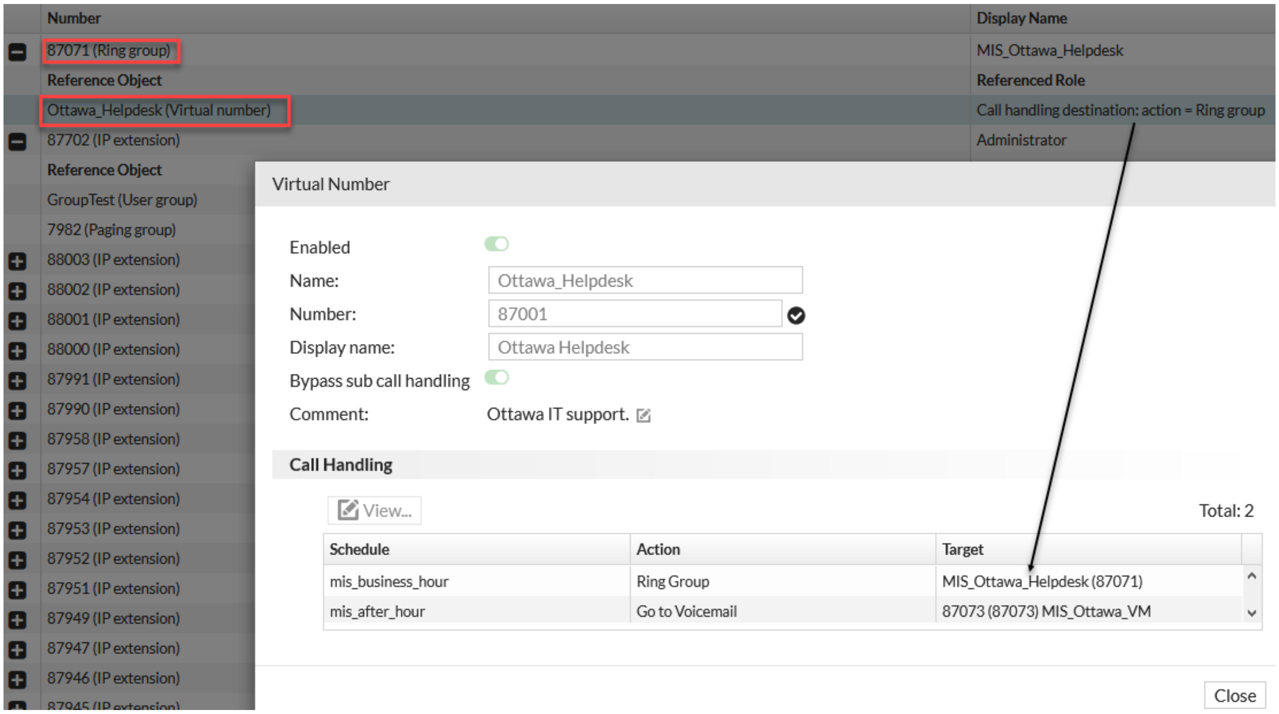
Reviewing system configuration

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:

- *Number*: You can double-click an extension to modify it. For modification information, see Configuring IP extensions on page 183.
- *Departments*: This section lists departments with one or more groups.
- *MWI Auditor*: This section lists message waiting indicator (MWI) entries. You can double-click a record to view the voicemail source, including the user ID, extension number, and extension type.
- *Network Summary*: This section shows the IP address of each subnet and the number of devices connected to it.
- *DID Handling*: For detailed information, see Configuring direct inward dialing on page 251.
- *Call Queue*: This section is available for FortiVoice units with the Call Center license. For modification information, see Creating call queues on page 261.
- *Agent*: This section is available for FortiVoice units with the Call Center license. For modification information, see Configuring agents on page 268.
- *Referenced Extension*: This section includes extension that are used by other objects and their roles in the objects. You can double-click a referenced object to view the object details and the extension role in the object.

  In the following example, extension 87071 is used in the *Ottawa_Helpdesk (Virtual Number)* as a call handling destination.



Number	Display Name
87071 (Ring group)	MIS_Ottawa_Helpdesk
Reference Object	**Referenced Role**
Ottawa_Helpdesk (Virtual number)	Call handling destination: action = Ring group
87702 (IP extension)	Administrator
Reference Object	
GroupTest (User group)	
7982 (Paging group)	
88003 (IP extension)	
88002 (IP extension)	
88001 (IP extension)	
88000 (IP extension)	
87991 (IP extension)	
87990 (IP extension)	
87958 (IP extension)	
87957 (IP extension)	
87954 (IP extension)	
87953 (IP extension)	
87952 (IP extension)	
87951 (IP extension)	
87949 (IP extension)	
87947 (IP extension)	
87946 (IP extension)	
87945 (IP extension)	

Virtual Number

Enabled

Name: Ottawa_Helpdesk

Number: 87001

Display name: Ottawa Helpdesk

Bypass sub call handling

Comment: Ottawa IT support.

Call Handling

Total: 2

Schedule	Action	Target
mis_business_hour	Ring Group	MIS_Ottawa_Helpdesk (87071)
mis_after_hour	Go to Voicemail	87073 (87073) MIS_Ottawa_VM

Managing FortiVoice gateways, local survivability, and firmware

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.

FVE-100F and larger systems can manage gateways.

FVE models and maximum number of managed gateways

Model	Maximum number of managed gateways
FVE-100F and FVE-VM-100	5
FVE-200F8 and FVE-VM-200	5
FVE-300E-T	15
FVE-500F and FVE-VM-500	20
FVE-VM-1000	25
FVE-2000F and FVE-VM-2000	80
FVE-5000F and FVE-VM-5000	150
FVE-VM-10000	300
FVE-VM-20000	500
FVE-VM-50000	1000

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.

You can manage the firmware of FortiVoice units and FortiFone phones from the GUI.

This topic includes:

- Managing FXO gateways on page 170
- Managing FXS gateways on page 170
- Managing PRI gateways on page 172
- Configuring local survivability on page 173
- Managing the firmware on page 174

Managing FXO gateways

The FortiVoice foreign exchange office (FXO) gateway works in conjunction with the FortiVoice phone system to expand resources and support additional analog phone lines. With the FortiVoice FXO gateway, you connect your analog phone lines to your FortiVoice phone system.

FXO 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.

The supported Fortinet FXO gateway models are FortiVoice Gateways GO04 and GO08.

To deploy a FXO gateway

For detailed instructions about deploying a FXO gateway, see the FortiVoice FXO Gateway Deployment Guide.

To view and manage added FXO gateways

1. Go to *Managed System* > *Gateway* > *FXO Gateway*.
2. Select one of the following actions:

GUI field	Description
View Config Job	Click this button to display more details about the updates triggered by *Actions > Start Config Job*.
Actions	
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 36.
Fetch Device Info	Select a branch FortiVoice unit from the list and click this option to retrieve its information.
Upgrade	
Now	Select a gateway and this option to upgrade it now.
Custom Time	Select a gateway and this option to upgrade it later.
Start Config Job	Use this option to update the configuration on multiple gateways at the same time. To update the configuration on all gateways, select *All*. To update the configuration on selected gateways only, select *Selected*. To get details about the job, click the *View Config Job* button.

Managing FXS gateways

The FortiVoice foreign exchange subscriber (FXS) gateway works in conjunction with the FortiVoice phone system to expand resources and support additional analog phone extensions. With the FXS gateway, you can connect your traditional analog phones and fax machines to a FortiVoice phone system.

FXS 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.

The supported Fortinet FXS gateway models are the following:

- FVG-GS04 is a FXS gateway with 4 ports. When you add this gateway, the FortiVoice unit creates 4 extensions.
- FVG-GS16 is a FXS gateway with 16 ports. When you add this gateway, the FortiVoice unit creates 16 extensions.
- FVG-GS24 is a FXS gateway with 24 ports. When you add this gateway, the FortiVoice system creates 24 extensions.

To deploy a FXS gateway

For detailed instructions about deploying an FXS gateway, see the FortiVoice FXS Gateway Deployment Guide.

To edit gateway extensions

Each port has an extension number.

For detailed instructions about editing a managed extension, see Modifying managed extensions on page 199.

To view and manage added FXS gateways

1. Go to *Managed System > Gateway > FXS Gateway*.
2. Select one of the following actions:

GUI field	Description
View Config Job	Click this button to display more details about the updates triggered by *Actions > Start Config Job*.
Actions	
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 36.
Fetch Device Info	Select a branch FortiVoice unit from the list and click this option to retrieve its information.
Upgrade	
Now	Select a gateway and this option to upgrade it now.
Custom Time	Select a gateway and this option to upgrade it later.
Start Config Job	Use this option to update the configuration on multiple gateways at the same time. To update the configuration on all gateways, select *All*. To update the configuration on selected gateways only, select *Selected*. To get details about the job, click the *View Config Job* button.
Start Extension	Shows the start of the analog extension numbering for up to 1000 extensions. Click the *Edit* icon to access the *FXS Gateway start extension* setting. For more details about the *FXS Gateway start extension* setting, see Configuring FortiVoice options on page 116.

Managing PRI gateways

The FortiVoice primary rate interface (PRI) gateway works in conjunction with your FortiVoice phone system to expand resources and support additional phone lines. With a PRI gateway, you connect your legacy telephony infrastructure composed of PRI (T1 or E1) digital lines to a FortiVoice phone system.

PRI 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.

The supported Fortinet PRI gateway models are the FortiVoice Gateway GT01 and GT02.

To deploy a PRI gateway

For detailed instructions about deploying a PRI gateway, see the FortiVoice PRI Gateway Deployment Guide.

To view and manage added GT01/02 gateways

1. Go to *Managed System* > *Gateway* > *PRI Gateway*.
2. Select one of the following actions:

GUI field	Description
View Config Job	Click this button to display more details about the updates triggered by *Actions > Start Config Job*.
Actions	
Apply Configuration	Select a gateway from the list and click this option to apply the FortiVoice PRI 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 36.
Fetch Device Info	Select a branch FortiVoice unit from the list and click this option to retrieve its information.
Upgrade	
Now	Select a gateway and this option to upgrade it now.
Custom Time	Select a gateway and this option to upgrade it later.
Start Config Job	Use this option to update the configuration on multiple gateways at the same time. To update the configuration on all gateways, select *All*. To update the configuration on selected gateways only, select *Selected*. To get details about the job, click the *View Config Job* button.

Configuring local survivability

In a centralized multi-site network deployment, a FortiVoice local survivability solution provides resiliency with survivability branches. A survivability branch is a FortiVoice local survivable gateway (LSG) unit with local extensions. A FortiVoice LSG unit is located in a branch office. A FortiVoice phone system in a main office manages one or more FortiVoice LSG units (survivability branches).

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. If you add an extension, 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 FortiVoice unit and the branch office FortiVoice units stops, branch office FortiVoice units (survivability branches) will kick in to provide access to lines until the communication is restored between the central unit and the extensions.

To deploy a survivability branch

For detailed instructions about deploying a survivability branch, see the FortiVoice Local Survivable Gateway Deployment Guide.

Supported models

The following FortiVoice phone system models can manage one or more survivability branches:

- FVE-300E-T and larger
- FVE-VM-500 and larger

The supported FortiVoice survivability branch models are:

- FVE-20E2
- FVE-20E4
- FVE-50E6
- FVE-50G2
- FVE-100F
- FVE-200F8
- FVE-500F

The FortiVoice phone system continues to support FVE-100E as a FortiVoice LSG model. However, this model has reached its end-of-order (EOO) date.

The FortiVoice LSG solution supports the following gateways at the branch office:

- FortiVoice Gateway GO04 and GO08, foreign exchange office (FXO) gateways
- FortiVoice Gateway GS04, GS16, and GS24 foreign exchange subscriber (FXS) gateways
- FortiVoice Gateway GT01 and GT02, primary rate interface (PRI) gateways

FVE models and supported number of survivability branches

FVE model	Number of survivability branches supported
FVE-300E-T	10
FVE-500F and FVE-VM-500	15
FVE-VM-1000	25
FVE-2000F and FVE-VM-2000	80
FVE-VM-3000	80
FVE-5000F and FVE-VM-5000	150
FVE-VM-10000	300
FVE-VM-20000	500
FVE-VM-50000	10000

To view the list of added survivability branches

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

GUI field	Description
View Config Job	Click this button to display more details about the updates triggered by *Actions > Start Config Job*.
Actions	
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	
Now	Select a branch FortiVoice unit and select this option to upgrade it now.
Custom Time	Select a branch FortiVoice unit and select this option to upgrade it later.
Start Config Job	Use this option to update the configuration on multiple branches at the same time. To update the configuration on all branches, select *All*. To update the configuration on selected branches only, select *Selected*. To get details about the job, click the *View Config Job* button.

Managing the firmware

Managed System > Firmware allows you to manage the firmware of the FortiVoice devices and FortiFone phones.

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

FortiFone phones are those connected to this FortiVoice unit.

To manage FortiFone firmware

1. Go to *Managed System* > *Firmware* > *FortiFone Firmware.*
2. You have access to the following functions:

GUI field	Description
Upload	Click to upload a firmware file. You can select a phone model or FortiFone desktop app, select the firmware file, enter the firmware version number, and click *OK* to upload the firmware. Note that if you selected *FortiFone-DesktopApp*, the *Firmware version* option is only available when editing an existing firmware file. For FortiFone-380, 480, and 580, there is a *Forced* option. If necessary, enable this option to force a new build onto the phone regardless of the firmware version already on the phone.
Download	Select a firmware file and click this button to download it.
Action	Select a firmware file and click this button to enable or disable a firmware upgrade for the FortiFone phones managed by this FortiVoice unit.
Statistics	Click to display the phone model, firmware version, and phone count of the managed FortiFone phones.
Upgrade	Select a firmware and click *Upgrade* to upgrade the FortiFone firmware: • *Name*: Enter a name for the firmware upgrade job. • *Extension Selection*: Select *All related devices* if you want to upgrade all of the devices to which the firmware applies to. Otherwise add individual devices that you want to upgrade. • *Schedule*: Schedule the upgrade. The firmware will be pushed to the managed FortiFone phones at the scheduled time.
View upgrade job	Click to display the FortiFone upgrade records. See Maintaining phones on page 110.

To upgrade the phone firmware

For the complete sequence to upgrade the phone firmware, see the FortiFone firmware upgrades section in the FortiVoice Cookbook.

To manage FortiVoice firmware

1. Go to *Managed System* > *Firmware* > *FortiVoice Firmware.*
2. You have access to the following functions:

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 settings

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

This topic includes:

Configuring intrusion detection

Security > *Intrusion Detection* lets you manually add IP addresses to be exempted from being blocked and configure intrusion detection settings.

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

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

For information about viewing system added exempt IPs, see Blocking SIP device IP addresses on page 43.

To add an exempt IP

1. Go to *Security* > *Intrusion Detection* > *Exempt IP.*
2. Click *New*.
3. Enter the IP address or netmask of the network interface that you want to add to the exempt list.
4. Click *Create*.

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 IP addresses) to the FortiVoice unit.

GUI field	Description
Initial block period	Enter the time in minutes to initially block every new device/IP address 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 about setting SIP password and user PIN, see Configuring IP extensions on page 183.

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	Select to enable or disable the SIP password and user PIN policy for administrators and extension users.
Password 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 portal access passwords. If any password does not conform to the policy, require that user to change the password at the next login.
PIN policy	• *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.

GUI field	Description
	- *PIN special*: Select to include special characters in the PIN. - *Apply PIN policy to*: Select *Voicemail users* to apply the policy to 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. - *PIN expiration*: Select the voicemail PIN expiration options. - *Never*: Users set their voicemail PIN and the PIN never expires. - *Default Only*: Extension users using the default voicemail PIN is prompted to change the PIN when accessing their voicemail for the first time. For information about voicemail PIN, see Configuring IP extensions on page 183. - *All*: Extension users are prompted to change the voicemail PIN when accessing their voicemail for the first time and regularly according to the PIN expiration time. - *PIN expiration time*: If you selected *All* for *PIN expiration*, select the PIN expiry time in days.
Allow empty admin password	Select to allow leaving the admin password field empty when logging in to the system. This option only appears when you disable *Password / PIN Policy*.

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 183.
4. Click *OK*.

Auditing the extension passwords

You can verify the strength of IP and fax extension passwords. For information about setting IP extension and fax extension passwords, user passwords, and voicemail PINs, see Configuring IP extensions on page 183 and Configuring fax extensions on page 207.

To audit a SIP extension password

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

GUI field	Description
Edit	Select an extension and click *Edit* to modify the extension configuration. See Configuring IP extensions on page 183.
Audit Now	Click to check the strength of the extension passwords. The time is displayed when last audit was done.

GUI field	Description
	If a password warning (red check mark) appears, double-click the extension to view and modify the password based on the policy. See Configuring IP extensions on page 183. If the password strength of an extension shows the *Weak* (black check mark) icon, double-click the extension to view and modify the password based on the policy until the password strength shows the *Strong* (green check mark) icon. See Configuring IP extensions on page 183.
Download	Click to save a copy of the password audit result.

Configuring user privileges

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

The following menus include the same user privilege information:

- *Security* > *User Privilege*
- *Phone System* > *Profile* > *User Privilege*

For detailed information, see Configuring user privileges on page 151 in the *Phone System* > *Profile* > *User Privilege* section.

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 151.

To set an account code

1. Go to *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 detail records on page 38.
Access Code Set	1. Click *New*. 2. Enter the account code with a minimum of 3 digits and a maximum of 10 digits.

GUI field	Description
	3. Enter a display name for the code such as Finance. **4.** Add any notes for the code. **5.** Click *Create*.

3. Click *Create*.

Blocking phone numbers

For security reasons, you can block an inbound call by entering its number. This will block future calls from this number.

To block a number

1. Go to *Security* > *Blocked Number*.
2. Click *New*.
3. Enter the number you want to block.
4. Click *Create*.
5. Click *Setting*.
6. In *PBX Setting*, enable *System block list*.
7. Click *Apply*.
   Future calls from the number will be blocked. For more information, see Configuring phone system settings on page 114.

To unblock a number

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

Configuring web service settings

You want to prevent the FortiVoice system from being overloaded with external connections by setting limits for concurrent connections, active admin portal and REST API sessions, and repeated offender requests.

To enable the REST API support

To allow the FortiVoice system to use REST APIs, you must enable the feature. By default, this feature is disabled on the FortiVoice system. To enable it, use the following CLI commands:

```
config system global
   set rest-api enable
end
```

For details about accessing the CLI console, see Using the CLI Console on page 30.

For more details about REST APIs, see the FortiVoice Phone System REST API Reference Guide.

To view and configure the web service settings

1. Go to *Security* > *Rate Limit* > *Web Service*.
2. Configure the following:

GUI field	Description
Rate Control	If you use zero (0) as a value, it means that there is no limit. The ranges and default values vary depending on the FortiVoice model.
Maximum Concurrent Request	
Web Server	Specifies the total maximum number of simultaneous connections to the FortiVoice system that the FortiVoice built-in web server allows to process.
Per IP	Specifies the total maximum number of simultaneous connections to the FortiVoice system from an IP address that you allow FortiVoice to process. If you want to exempt IP addresses from the concurrent connection, click *Exempt IP* and add those IP addresses.
Admin Portal	Specifies the total maximum number of simultaneous HTTP connections to the admin portal that you allow FortiVoice to process.
User Portal	Specifies the total maximum number of simultaneous HTTP connections to the user portal that you allow FortiVoice to process.
REST API	Specifies the maximum number of simultaneous RESTful connections that you allow FortiVoice to process. This field is visible when you enable the REST API support. For details, see To enable the REST API support on page 180.
Maximum Login Session	
Admin Portal	Specifies the maximum number of login sessions to the admin portal that can be active at the same time. An active session is a successful login (admin/password) with a valid cookie or token.
REST API	Specifies the maximum number of active RESTful sessions. This field is visible when you enable the REST API support. For details, see To enable the REST API support on page 180.
Maximum Request Rate (Per Second)	
Admin Portal	Specifies the maximum number of HTTP connections (per second) to the admin portal that you allow FortiVoice to process.

GUI field	Description
User Portal	Specifies the maximum number of HTTP connections (per second) to the user portal that you allow FortiVoice to process.
REST API	Specifies the maximum connection rate (per second) for the REST API. This field is visible when you enable the REST API support. For details, see To enable the REST API support on page 180.
Repeat Offender Control	Enable to block the IP addresses that keep sending bad HTTP requests to FortiVoice and causing FortiVoice to return HTTP 404 or 405 errors.
Block after request count	Specify the number limit of bad requests within a specified period of time that will trigger an offender IP blocking. If you want to exempt IP addresses from the repeat offender control, click *Exempt IP* and add those IP addresses.
Time period	Specify the period of time (in minutes) to block the bad requests. Here is an example using the *Block after request count* with a value of 3 and the *Time period* with a value of 5: If within a 5-minute interval, bad requests from an IP address reach 3, the IP address will be blocked for the remaining of the 5-minute interval. After the interval expires, the counter restarts for the next interval.

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 183
- Creating extension groups on page 217
- Setting up a general voicemail on page 224
- Working with virtual numbers on page 227

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 183
  - Batch editing extensions on page 192
  - Auditing SIP extension password on page 195
  - Auditing extension numbers and MAC addresses on page 196
  - Importing a list of extensions on page 196
  - Configuring auxiliary phones on page 197
- Modifying managed extensions on page 199
- Modifying analog extensions on page 202
- Configuring remote extensions on page 204
- Configuring fax extensions on page 207
- Setting extension user preferences on page 210

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 local IP extensions, go to *Extension* > *Extension* > *IP Extension*.

GUI field	Description
LDAP Connector	When you select *Filter* > *Source* > *LDAP* to list the extension users with LDAP authentication, you can click this option to see the LDAP connector information. See Configuring LDAP settings on page 130.
Actions	• *Batch Edit*: Select to modify a group of extensions all at the same time. For more information, see Batch editing extensions on page 192.

GUI field	Description
	• *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 196. • *View Phone Configuration:* Select a FortiFone extension and click this option to view the configuration file of the phone, desktop app, or mobile. • *Phone*: This option appears when a phone is associated with an extension. In this case, the FortiVoice unit generates a configuration file for the phone. If you select a Cisco phone, you can select *Enterprise* or *3PCC*. For details about creating an extension, see To create or edit an IP extension on page 185. • *Desktop App* and *Mobile*: These options appear when an extension is allocated with FortiFone softclient licenses. In such cases, desktop app and mobile phone configuration files are generated. • *Apply Configuration (Main Phone)*: If you have edited an extension configuration and want to apply it to the desk phones and softclients associated with this extension, select the extension and click this option. This action will not apply the configuration to the auxiliary phones associated with this extension. The selected phone 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 auto-provisioning for FortiFone phones and gateways on page 99. • Phone type and MAC address are correctly configured. See To create or edit an IP extension on page 185. • Auto-provisioning is enabled for the extension associated with the phone through the user privilege applied to it. See Configuring user privileges on page 151. • *Password Auditor*: See Auditing SIP extension password on page 195. • *Number Auditor*: See Auditing extension numbers and MAC addresses on page 196 • *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 portal. See Auxiliary Phone on page 189 and Notification Options on page 212. • *Maintenance*: Select an extension and click this button to manage a user's voicemail box and faxes. You can check the size of the mailbox or fax folder and empty them if required. Click *Back* to return to the *IP Extension* tab. • *SIP Registration Log*: Select to display the registration status of a selected extension or all extensions.
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 caller ID for internal calls. This is usually the name of the extension user.

GUI field	Description
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 156.
Survival Branch	If the extension belongs to a FortiVoice survivability branch, the branch information is listed. For information about survivability branch, see Configuring local survivability on page 173.
Department	If the extension belongs to an extension department, the department information is listed. For information about departments, see Creating extension departments on page 217.
Business Group	If the extension belongs to a business group, the group information is listed. For information about business groups, see Creating business groups on page 224.
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 about phone profile, see Configuring phone profiles on page 142.
Phone Info	The model, MAC address, and firmware version of the phone for this extension.

To create or edit an IP extension

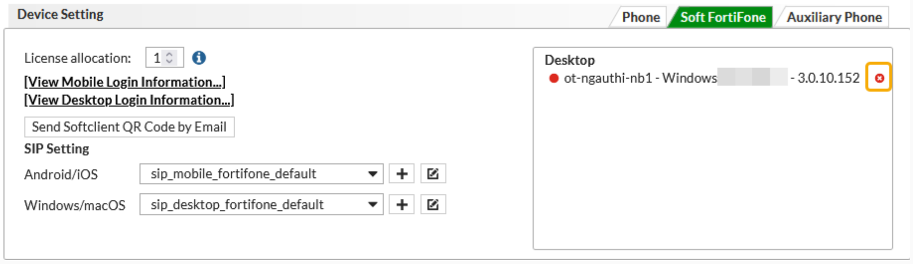
1. Go to *Extension > Extension > IP Extension*.
2. Click *New* or double-click an existing extension.
3. Configure the following:

GUI field	Description
Enabled	Select to activate the extension.
Number	Enter the extension number following the extension number pattern. See Configuring FortiVoice options on page 116. If you are editing the extension, you can click *Edit Preference* to configure the extension user preferences. See Setting extension user preferences on page 210.
User ID	This option is view only and appears when you edit an extension. This is the system-generated ID based on the user ID prefix you set (see User ID prefix on page 118) and the extension number.

GUI field	Description
Display name	⚠ Do not include quotation marks in an extension display name. The recommended character length is 20 characters or less. If you enter more than 20 characters, the name may not show properly on some phone models. The caller ID used for internal calls. Enter the name that the phone can display when it receives a call from this extension. This is usually the name of the extension user. Click +: • *External caller ID*: Enter the caller ID that displays on a called phone when you make an external call. Use the name<phone_number> format, such as John Doe<222134>. • *Emergency caller ID*: Enter the caller ID that displays on a called phone when you make an emergency call. Use the name<phone_number> format, such as John Doe<222134>. • *Voice DID Number*: This option is only available when you edit an extension. Click the *Edit* icon to modify the voice DID mapping for this extension. See Configuring direct inward dialing on page 251. • *Fax DID Number*: This option is only available when you edit an extension. Click the *Edit* icon to modify the fax DID mapping for this extension. See Configuring direct inward dialing on page 251.
Description	Enter any notes for the extension.
Upload/Delete (icons)	Click to add or remove a picture of the extension user. This option is only available when you edit an extension. By adding a picture of the extension user, the picture can be displayed on the callee phone screen whenever the user makes a phone call, if the phone model supports this feature.
Edit Preference	See Setting extension user preferences on page 210.
Device Setting	Extension SIP devices include desk phones, softclients, and auxiliary devices.
Phone	
Type	Select the desk phone type.
Device	This option is only available if you select FortiFone as *Type*. Select the specific phone model. To add a new device, click the *New* icon. See Configuring desk phones on page 159. To modify a selected device, click the *Edit* icon. To choose an existing device, click the *Select* icon. To unassign a device: **1.** Click the *Select* icon. **2.** Click the device that you want to unassign. **3.** Near the bottom right, click *Select None*.

GUI field	Description
Phone model	This option is only available if you select FortiFone as *Type*. The FortiFone model.
SIP settings	Select the SIP profile for the phone. Click the *New* icon to add a new profile. See Configuring SIP profiles on page 138. ⚠ The Zycoo X10 SIP Paging Gateway does not support secure RTP. Click the *Edit* icon to modify a selected profile.
Emergency zone type	Select how you want the assignment of an emergency zone to be made: • *Static*: Manually select the *Emergency zone* profile for the extension. • *Dynamic*: You allow the FortiVoice phone system to identify where the phone of the emergency caller is on the network. When a phone user calls an emergency number, the FortiVoice phone system checks where the calling phone is and assigns a matching emergency zone profile to the phone. This assignment is useful when phone users move their phones to different places on the network. • If you select *Dynamic*, enable and update the *Dynamic Network Match* in Configuring emergency zone profiles on page 156.
Emergency zone	If you selected *Static* for the *Emergency zone type*, select the emergency zone profile for the extension. Click the *New* icon to add a new profile. See Configuring emergency zone profiles on page 156. Click the *Edit* icon to modify a selected profile.
Programmable keys	This option is only available if you select the FortiFone as *Type* and is not available for all models. Select the keypad profile for the phone. Click the *New* icon to add a profile or *Edit* icon to modify a selected profile. See Configuring programmable key profiles on page 146.
Advanced	Configure the following and click *OK* when you finish. • *SIP password*: FortiVoice uses this password to register your SIP phone from the phone or the web. You need the phone IP to access it from the web. You can check the password strength. See Auditing the extension passwords on page 178. 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 118), 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.

GUI field	Description
	- *User programmable keys*: By clicking *Edit*, you can configure the phone programmable keys for the extension user if the programmable keys profile used for this extension gives users the permission to do so. - *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. - *Number*: Enter the phone number. This is the phone number that the FortiVoice unit automatically dials after the phone user lifts up the phone handset (or presses the headset or speaker button) to place a call. - *After*: If you want to delay the automatic dialing, enter a value in seconds. If the delay is set to 0, the extension is turned into a hotline meaning that the FortiVoice unit immediately dials the configured Direct call number after the extension is off-hook. - *Secondary account*: In addition to the main account, a secondary account can be added to an extension. The addition of a secondary account can be useful to an extension user that has more than one role in an organization and wants a different extension assigned to each one or needs to monitor and answer calls received on another extension. - FortiVoice assigns the selected secondary account to key 2 (line 2) on your phone automatically. - If the secondary account has an assigned device, both phones ring when receiving a call. - If the secondary account does not have a device assigned to it, extensions ring independently when receiving a call. For example, extension 100 sets extension 200 to be a secondary account. When a call comes in to extension 100, it's the only extension to ring and extension 200 is the only one to ring when a call is routed to it. - Prior to making the selection for the secondary account, make sure to enable the *Secondary account* option in *System > Advanced > Auto Provisioning, Other Setting*. For more information, see Secondary account (Enable secondary account for Desktop FortiFone) on page 100. - FortiVoice does not support the selection of an analog extension as a secondary account.
Soft FortiFone	This section is for the FortiFone softclient for mobile and desktop.
License allocation	Select the number of FortiFone softclient licenses for use on this extension.
View Mobile Login Information	Click *View Mobile Login Information* to view the login information of the mobile softclient. To log in to the mobile softclient, use the user name and password or scan the QR code using the mobile softclient.
View Desktop Login Information	Click *View Desktop Login Information* to view the login information file of the desktop softclient. To log in to the desktop softclient, use the user name and password.

GUI field	Description
Send Softclient QR code by Email	Prior to sending the QR code, make sure that the email address of the extension user is in the Notification Options on page 212. The extension owner can use the QR code to register the mobile softclient.
SIP Setting	• *Android/iOS*: If the softclient 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 138. • *Windows/macOS*: If the softclient 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 138.
Revoking a license	When licenses are allocated to an extension and the devices associated with the extension use the licenses, the devices appear.  Device Setting Phone | Soft FortiFone | Auxiliary Phone License allocation: 1 [View Mobile Login Information...] [View Desktop Login Information...] Send Softclient QR Code by Email SIP Setting Android/iOS: sip_mobile_fortifone_default Windows/macOS: sip_desktop_fortifone_default Desktop ● ot-ngauthi-nb1 - Windows [redacted] - 3.0.10.152 If you want to free up a license, you can revoke the license of a device that you no longer need and use it for another device in need. To do so, click the *Revoke License* (⊗) icon and confirm the action.
Auxiliary Phone	Click *New* to add SIP devices to the extension. When you add an auxiliary phone to your extension, you have two phones with the same extension number. The phones will ring at the same time but you can only use one phone to answer the call. This function is useful when you want to access the same extension from two different locations. For more information, see Configuring auxiliary phones on page 197. From *Extension > Extension > IP Extension*, 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 auto-provisioning for FortiFone phones and gateways on page 99. • Device type and MAC address is correctly configured. See To create or edit an IP extension on page 185. • Auto-provisioning is enabled for the extension associated with the device through the user privilege applied to it. See Configuring user privileges on page 151.
SLA	This tab is visible when the extension is part of a shared line appearance (SLA) group.

GUI field	Description
	For more details about the SLA function, see Appendix A: Shared line appearance on page 370.
User Setting	
Management	Configure the extension’s role in other settings.
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 about user privilege, see Configuring user privileges on page 151.
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 about extension department, see Creating extension departments on page 217.
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 173.
Voicemail	Configure the extension’s voicemail. In some cases, you may want other users or groups to share this voicemail. For example, a supervisor wants his/her co-workers to access his/her voicemail while he/she is away. *Main Voicemail:* Select the extension’s own voicemail (*Default*) or that of another extension as the voicemail of this extension. Typically, you use the default voicemail. If you select the voicemail of another extension, you can click *Edit* to modify that extension. *Send voicemail notification to - User(s) and Group(s)*: You can select user(s) and group(s) that will receive a notification when this extension receives a voicemail and have access to the voicemails by using the FortiVoice user portal, FortiFone phone or softclient. *User(s)* and *Group(s)*: To select users or groups, click + in the field and select the users/groups. Click *Close*. *View Monitored Voicemails*: This option is only available when you edit an extension. Click to view the list of voicemails that this extension is monitoring, if applicable. If you selected another extension than the default in *Main Voicemail*, then you can filter the list. 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 324) and enter the user’s own user PIN. For information about creating user groups, see Creating extension groups on page 217.
Web Access	Configure the authentication type to access to the user portal and FortiFone softclient (mobile and desktop) apps. If *Password policy is disabled* appears, see Setting password policies on page 177.

GUI field	Description
Authentication type	Select the extension authentication type: *Local* , *RADIUS*, or *LDAP* and configure the following settings.
If you selected *Local* as the *Authentication type*:	
User password	Enter the password for the access to the user portal and softclient access from mobile or desktop devices. This password can be much longer and stronger to mitigate the risk of password guess attack. To let the system create the user password, click *Generate*. To show the user password, click the eye icon. When you configure the phone system capacity, you can set the *Local authentication type* to one of the following: • User password only • User password or voicemail PIN For more information, see Configuring system capacity on page 120.
If you selected *RADIUS* for the *Authentication type*:	
RADIUS profile	Select or create a RADIUS profile to apply to this extension. For more information about RADIUS profiles, see Configuring RADIUS authentication profiles on page 150.
Authentication ID	Enter the username that is configured in the RADIUS Service of the FortiAuthenticator and to be associated with the extension.
If you selected *LDAP* for the *Authentication type*:	
LDAP profile	Select or create an LDAP profile to apply to this extension. For information about LDAP profiles, see Configuring LDAP profiles on page 130. You can click *New* to create a new profile or *Edit* to modify the selected one.
Authentication ID	During the configuration of the LDAP profile, you have two options for the user authentication: • If you select *Try common name with base DN as bind DN*, update the *Authentication ID* to match the common name attribute (example, uid) that you entered in the *Common name ID* of the profile, such as `jdoe`. • If you select *Search user and try bind DN*, leave the *Authentication ID* blank.
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 portal. Selection of using personal password or voicemail PIN to access user portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 120. You can check the PIN strength. See Auditing the extension passwords on page 178. 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 118), the password appears here. However, you can change it.

GUI field	Description
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.
Conferencing ID	Enter the conference organizer PIN for the extension conference call.
Call Center	This option appears if your FortiVoice unit has a call center license. Save your FortiVoice configuration before configuring call center. Select to configure the departments that a call center agent manages, queues that the agent belongs to, skill sets, and skill levels. Click *Call Center*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 280. • *Managed departments*: An agent manager may need to monitor call queues in certain departments. For information about setting up departments, see Creating extension departments on page 217. Click in the field and select the departments to be monitored and then click *Close*. • *Member of Queues*: Click to select the call queues to join. • *Queues*: Click in the field and select the queues of which you want the extension/agent to be a member. Click *Close*. • *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 281. 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. Click *OK*. • *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 278 and Creating agent skill levels on page 278. Click *OK*.

4. Click *Create* (for new extension) or *OK* (for editing extension).

Batch editing extensions

You can efficiently modify a group of extensions all at the same time.

To batch edit extensions

1. Go to *Extension* > *Extension* > *IP Extension.*
2. Under *Actions*, click *Batch Edit*.
3. Search or filter the extensions you want to edit, if required.
4. Click *Next*.
5. Select the options you want to modify and configure the following:

GUI field	Description
License	
License allocation	Select the number of licenses allocated to the extensions.
Android/iOS	Select the SIP profile for Android/iOS extension devices. You can add a new profile or edit a selected one. For more information, see Configuring SIP profiles on page 138.
Windows/macOS	Select the SIP profile for Windows/macOS extension devices. You can add a new profile or edit a selected one. For more information, see Configuring SIP profiles on page 138.
Agent profile	Enable or disable the agent profile. For more information about agent profiles, see Configuring agent profiles on page 280.
Call Center Agent	Select the agent profile for the call center agent. You can add a new profile or edit a selected one. For more information, see Configuring agent profiles on page 280.
Management	
Status	Enable or disable the extension’s role in other settings.
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 about user privilege, see Configuring user privileges on page 151.
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 about extension department, see Configuring agents on page 268.
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 173.
Caller ID	If you do not enter the caller IDs, your organization 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.
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 John Doe<222134>.
Emergency caller ID	Enter the caller ID that displays on a called phone when you make an emergency call. Use the name<phone_number> format, such as John Doe<222134>.
Authentication	
Authentication type	Select the extension authentication type: *Local* , *LDAP*, or *RADIUS*.
If you selected *LDAP* for *Authentication type*:	
LDAP profile	Select or create an LDAP profile to apply to the extensions. For information about LDAP profiles, see Configuring LDAP profiles on page 130. You can click *New* to create a new profile or *Edit* to modify the selected one.

GUI field	Description
If you selected *RADIUS* for *Authentication type*:	
RADIUS profile	Select or create a RADIUS profile to apply to the extensions. For more information about RADIUS profiles, see Configuring RADIUS authentication profiles on page 150.
If you selected *Local*, *LDAP*, or *RADIUS* for *Authentication type*:	
User password	If you selected *Local* as the *Authentication type*, enter the password for user portal access. This password can be much longer and stronger to mitigate the risk of password guess attack and preserve the voicemail PIN for phone access only. To let the system create the user password, click *Generate*. To show the user password, click the eye icon. Control of using user password or voicemail PIN to access user portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 120.
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.
Voicemail PIN	Enter the password for the extension user to access voicemail and the user portal. Selection of using personal password or voicemail PIN to access user portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 120. You can check the PIN strength. See Auditing the extension passwords on page 178. 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 118), the password appears here. However, you can change it.
Main Device	Main extension SIP devices include desk phones and soft phones.
SIP settings	Select the SIP profile for the phone. You can add a new profile or edit a selected one. For more information, see Configuring SIP profiles on page 138.
Emergency zone type	Select how you want the assignment of an emergency zone to be made: • *Static*: Manually select the *Emergency zone* profile for the extension. • *Dynamic*: You allow the FortiVoice phone system to identify where the phone of the emergency caller is on the network. When a phone user calls an emergency number, the FortiVoice phone system checks where the calling phone is and assigns a matching emergency zone profile to the phone. This assignment is useful when phone users move their phones to different places on the network. • If you select *Dynamic*, enable and update the *Dynamic Network Match* in Configuring emergency zone profiles on page 156.

GUI field	Description
Emergency zone	Select the emergency zone profile for the extension. You can add a new profile or edit a selected one. For more information, see Configuring emergency zone profiles on page 156.
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.
SIP password	Enter the password used for configuring your SIP phone from the phone or the web. You need the phone IP to access it from the web. You can check the password strength. See Auditing the extension passwords on page 178. Select *Auto generate* to let the system generate the password. Select *Default* if you have configured the default SIP user password (see Default SIP user password on page 118). In this case, the password appears here. However, you can change it. Select *Specific* to enter the password manually, or click *Generate* to generate a strong password automatically. Select the eye icon to display the password.
Type	Select the phone type: *FortiFone* or *Generic*.
Preference	
Phone language	Select the prompt language for the extension. The default is English.
Web language	Select the language for the FortiVoice user portal.
Time zone	Select the time zone for the FortiVoice user portal.
Ring duration	Enter the phone ringing duration in seconds before an incoming call goes to voicemail.
Notifications	
Missed call	Select *Enabled* if you want to receive an email notification when an incoming call is missed.
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 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.

6. Click *Next*, then *Apply*.

Auditing SIP extension password

You can verify the strength of SIP extension passwords. For information about setting SIP extension password, see Configuring IP extensions on page 183.

To audit a SIP extension password

1. Go to *Extension* > *Extension* > *IP Extension.*
2. Under *Actions*, click *Password Auditor*.
   The *Password Auditor* page opens.
3. If a password policy warning (yellow warning mark) appears, click the warning to view the password policy. To set the policy, see Setting password policies on page 177.
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, if any.
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 about extension numbers, see Configuring IP extensions on page 183.

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, if any.
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 header row containing the following column names. Otherwise, the import will fail.

- User ID
- Extension
- Phone type
- Mac address
- Phone profile
- Handset ID is required for FON-D71, FON-D72, FON-870, and Yealink W60B phone models.

The following table describes other columns that you can include in the CSV file and their associated values:

Column	Description
Email	Includes three emails or less. To separate the email addresses, use a space.
Authentication Type	For local, enter 1. For LDAP, enter 5.
Emergency Zone Type	For static, enter 1. For dynamic, enter 2. If you do not specify an emergency zone type, FortiVoice assigns the type 1 (static).

To import a list of extensions

1. Go to *Extension* > *Extension* > *IP Extension.*
2. Click *Actions* > *Import*.
3. Locate and select the CSV file.
4. Click *Open*.
   The file imports.
5. Review the list of extensions to import.
6. Verify the mapping and make changes, if required.
7. You have a few options:

Button or option	Description
Delete	To remove extensions from the list, select one or more extensions and click *Delete*. To confirm the deletion, click *Delete*.
Update existing extensions	If the FortiVoice system and CSV file include the same extension number, then the information in the CSV file replaces the information about the FortiVoice system for that extension.
Skip CSV first line	The FortiVoice system ignores the first line of the CSV file. For example, FortiVoice can ignore a header row.

8. Click *Apply Mapping*.
9. Click *Import*.
   FortiVoice displays the results of the import.
10. Click *Close*.

Configuring auxiliary phones

When you add an auxiliary phone to your extension, you have two phones with the same extension number. The phones will ring at the same time but you can only use one phone to answer the call. This function is useful when you want to access the same extension from two different locations.

When you add a device, it inherits your primary phone’s user privileges except hot desking and fax.

To add and configure an auxiliary phone

1. Go to *Extension* > *Extension* > *IP Extension*.
2. Double-click an extension, go to *Device Setting*, and click the *Auxiliary Phone* tab.
3. Click *New* and configure the following:

GUI field	Description
Type	
If you select *FortiFone* as the *Type*, configure the following settings:	
Device	Click the *Select* icon to choose a FortiFone desk phone and click *OK*. The phones are configured for SIP inventory. SeeConfiguring desk phones on page 159. You may also add a new phone or edit an existing one.
Phone model	This option appears after you select a device.
Setting	If you select *Custom*, configure the following options:
SIP settings	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 138.
Emergency zone type	Select how you want the assignment of an emergency zone to be made: • *Static*: Manually select the *Emergency zone* profile for the extension. • *Dynamic*: You allow the FortiVoice phone system to identify where the phone of the emergency caller is on the network. When a phone user calls an emergency number, the FortiVoice phone system checks where the calling phone is and assigns a matching emergency zone profile to the phone. This assignment is useful when phone users move their phones to different places on the network. • If you select *Dynamic*, enable and update the *Dynamic Network Match* in Configuring emergency zone profiles on page 156.
Emergency zone	If you selected *Static* for the *Emergency zone type*, select the emergency zone profile for the extension. If you want to add a new profile, click the *New* icon. See Configuring emergency zone profiles on page 156. To modify a selected profile, click the *Edit* icon.
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 account	
Account	If you enabled the option to add a secondary account for FortiFone desktop phones under *System* > *Advanced* > *Auto Provisioning*, do it here by selecting the FortiFone extension.
If you select *Generic* as the *Type*, configure the following settings:	

GUI field	Description
SIP settings	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 138.
Emergency zone type	Select how you want the assignment of an emergency zone to be made: • *Static*: Manually select the *Emergency zone* profile for the phone. • *Dynamic*: You allow the FortiVoice phone system to identify where the phone of the emergency caller is on the network. When a phone user calls an emergency number, the FortiVoice phone system checks where the calling phone is and assigns a matching emergency zone profile to the phone. This assignment is useful when phone users move their phones to different places on the network. • If you select *Dynamic*, enable and update the *Dynamic Network Match* in Configuring emergency zone profiles on page 156.
Emergency zone	If you selected *Static* for the *Emergency zone type*, select the emergency zone profile for the extension. If you want to add a new profile, click the *New* icon. See Configuring emergency zone profiles on page 156. To modify a selected profile, click the *Edit* icon.

4. Click *Create*.

Modifying managed extensions

The supported Fortinet FXS gateway models are the following:

- FVG-GS04 is a FXS gateway with 4 ports. When you add this gateway, the FortiVoice system creates 4 extensions.
- FVG-GS16 is a FXS gateway with 16 ports. When you add this gateway, the FortiVoice system creates 16 extensions.
- FVG-GS24 is a FXS gateway with 24 ports. When you add this gateway, the FortiVoice system creates 24 extensions.

For the local survivability branch, you can modify it paging numbers and change its password.

When your LSG deployment includes a FortiVoice FVE-20E2, FVE-50E6, or FVE-50G2 model configured as a survivability branch, you can access the FortiVoice system to modify the two managed extensions.

For details about adding the gateway, see the FortiVoice FXS Gateway Deployment Guide.

For details about configuring local survivability branches, see FortiVoice Local Survivable Gateway Deployment Guide.

To edit managed extensions

1. Go to *Extension* > *Extension* > *Managed Extension*.
2. In *Gateway device*, select:
   - the gateway or local survivability branch 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, enter the display name, and change the password. If you selected a gateway or LSG extension, configure the following:

GUI field	Description
Enabled	Select to activate the extension.
Number	Enter the extension number following the extension number pattern. See Configuring FortiVoice options on page 116.
Edit Preference	See Setting extension user preferences on page 210.
User ID	This is the system-generated ID based on the gateway and port. This option is view only and only appears when you edit an extension.
Display name	The caller ID for internal calls. Enter the name that the phone can display when it receives a call from this extension. To access and modify any of the following options, click the plus sign (+): • *External caller ID*: Enter the caller ID that displays on a called phone when you make an external call. Use the name<phone_number> format, such as John Doe<222134>. • *Emergency caller ID*: Enter the caller ID that displays on a called phone when you make an emergency call. Use the name<phone_number> format, such as John Doe<222134>. • *Voice DID Number*: Click the *Edit* icon to modify the voice DID mapping for this extension. For more details, see Configuring direct inward dialing on page 251. • *Fax DID Number*: Click the *Edit* icon to modify the fax DID mapping for this extension. For more details, see Configuring direct inward dialing on page 251.
Description	Enter any comments for the extension.
Device Setting	
Gateway device	This is the system-generated name of the gateway device. It is read only and only appears when you edit an extension.
Gateway fxs port	This is the gateway FXS port 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.
Emergency zone type	Select how you want the assignment of an emergency zone to be made: • *Static*: Manually select the *Emergency zone* profile for the extension. • *Dynamic*: You allow the FortiVoice phone system to identify where the phone of the emergency caller is on the network. When a phone user calls an emergency number, the FortiVoice phone system checks where the calling phone is and assigns a matching emergency zone profile to the phone. This assignment is useful when phone users move their phones to different places on the network. • If you select *Dynamic*, enable and update the *Dynamic Network Match* in Configuring emergency zone profiles on page 156.
Emergency zone	If you selected *Static* for the *Emergency zone type*, select the emergency zone profile for the extension. If you want to add a new profile, click the *New* icon. See Configuring emergency zone profiles on page 156. To modify a selected profile, click the *Edit* icon.

GUI field	Description
SIP settings	Select the SIP profile for the phone. You can add a new profile or edit a selected one. For more information, see Configuring SIP profiles on page 138.
User Setting	
Management	Configure the extension's role in other settings. *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 about user privilege, see Configuring user privileges on page 151. *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 about extension department, see Creating extension departments on page 217.
Web Access	Configure the access to the user portal and softclient for mobile and desktop apps. If *Password policy is disabled* appears, see Setting password policies on page 177.
Authentication type	Select the extension authentication type: *Local*, *RADIUS*, or *LDAP* and configure the following settings.
If you selected *Local* as the *Authentication type*:	
User password	Enter the password for the access to the user portal and softclient access from mobile or desktop devices. This password can be much longer and stronger to mitigate the risk of password guess attack. To let the system create the user password, click *Generate*. To show the user password, click the eye icon. When you configure the phone system capacity, you can set the *Local authentication type* to one of the following: • User password only • User password or voicemail PIN For more information, see Configuring system capacity on page 120.
If you selected *RADIUS* as the *Authentication type*:	
RADIUS profile	Select or create a RADIUS profile to apply to this extension. For more information about RADIUS profiles, see Configuring RADIUS authentication profiles on page 150.
Authentication ID	Enter the username that is configured in the RADIUS Service of the FortiAuthenticator and to be associated with the extension.
If you selected *LDAP* as the *Authentication type*:	
LDAP profile	Select an LDAP profile to apply to this extension. For information about LDAP profiles, see Configuring LDAP profiles on page 130. You can click *New* to create a new profile or *Edit* to modify the selected one.
Authentication ID	During the configuration of the LDAP profile, you have two options for the user authentication: • If you select *Try common name with base DN as bind DN*, update the *Authentication ID* to match the common name attribute (example, uid) that you

GUI field	Description
	entered in the *Common name ID* of the profile, such as `jdoe`. • If you select *Search user and try bind DN*, leave the *Authentication ID* blank.
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 portal. Selection of using personal password or voicemail PIN to access user portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 120. Click *Generate* to generate a strong password automatically. Select the eye icon to display the password. If you have configured the default user PIN (see Default Voicemail PIN on page 118), 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.

5. Click *OK*.

Modifying analog extensions

This section applies to the following models only:

- FVE-20E2
- FVE-50E6
- FVE-50G2

The FortiVoice FVE-20E2, FVE-50E6, and FVE-50G2 models have two analog ports used for analog phones and fax machines.

All three models support the following deployment modes:

- *PBX*: Select to assign the PBX function to your FortiVoice FVE-20E2, FVE-50E6, or FVE-50G2 model. The system creates two default analog extensions (7801 and 7802) visible in *Extension* > *Extension* > *Analog Extension*. You can edit the extensions’ default configuration.
- *Survivability Branch*: Select to assign the survivability branch function to your FortiVoice FVE-20E2, FVE-50E6, or FVE-50G2 model to provide resiliency in a centralized multi-site network deployment. The main office FortiVoice system manages the survivability branch and creates two extensions (*Extension* > *Extension* > *Managed Extension*). You need to apply this configuration to the survivability branch. For details about managed extensions, see Modifying managed extensions on page 199. For more details about survivability branches, see the FortiVoice Local Survivable Gateway Deployment Guide.

For details about setting the *Deployment mode*, see System Information widget on page 26.

To view the default analog extension

1. Go to *Extension* > *Extension* > *Analog Extension*.
2. You can view the following buttons and columns:

GUI	Description
Actions	
PSTN Setting	For details, see To edit PSTN settings for an analog extension on page 204.
Maintenance	Select an extension and click *Actions* > *Maintenance* to manage its voicemail (old), fax (inbox), and fax(sent). You can check the size of the box and empty the box. Click *Back* to return to the *Analog Extension* tab.
Enabled	Select to activate the extension.
Number	The analog extension number.
Display Name	The name displaying on the extension.

To edit a default analog extension

1. Go to *Extension* > *Extension* > *Analog Extension*.
2. Select a default extension and click *Edit*.
3. Configure the following:

GUI field	Description
Enabled	Select to activate the extension.
Number	Enter the extension number following the extension number pattern. See Configuring FortiVoice options on page 116. If required, click *Edit Preference* to modify the user preferences. See Setting extension user preferences on page 210.
User ID	This is the system-generated ID for the extension and is read-only.
Analog port	Select the analog port for the extension. By default, it is *fxs1*.
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>`. • For Voice DID Number and Fax DID Number details, see Configuring direct inward dialing on page 251. If you do not enter the caller IDs, your organization 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 190.

4. Click *OK*.

To edit PSTN settings for an analog extension

1. Go to *Extension* > *Extension* > *Analog Extension.*
2. Select an extension.
3. Click *Actions* > *PSTN Setting*.
4. Configure the following:

GUI field	Description
Name	The name of this configuration. This field is view-only.
Codec	Select the codec for the extension.
Caller ID signalling	Select the caller ID signalling standard per your phone company's request.
First digit Timeout Match digit Timeout	Enter the timeout in milliseconds. The following example explains both timeout settings using default values. The user picks up the phone handset and hears a dialtone. If the user does not enter a digit within the specified 16 seconds (first digit timeout), the dialtone restarts. After pressing the first digit, the user has 3 seconds (match digit timeout) to enter the next digit. After the user's finger is off the button, the timer resets and the user has another 3 seconds to enter the next digit and so on. When the 3-second timer expires, the phone number is identified as complete, and the call is attempted. The default *First digit timeout* is 16000. The default *Match digit timeout* is 3000.

5. Click *OK*.

Configuring 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 create or edit a remote extension

1. Go to *Extension* > *Extension* > *Remote Extension.*
2. Click *New* or double-click an existing extension.
3. Configure the following:

GUI field	Description
Enabled	Select to activate the remote extension.
Edit Preference	This option is only available when you edit an extension. Click to configure the extension user preferences. For details, see Setting extension user preferences on page 210.
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.
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 140. 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 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	
Management	
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 about user privilege, see Configuring user privileges on page 151.
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 about extension department, see Creating extension departments on page 217.
Voicemail	Configure the extension’s voicemail. In some cases, you may want other users or groups to share this voicemail. For example, a supervisor wants his/her co-workers to access his/her voicemail while he/she is away.

GUI field	Description
	Main Voicemail: Select the extension’s own voicemail (Default) or that of another extension as the voicemail of this extension. Typically, you use the default voicemail. If you select the voicemail of another extension, you can click *Edit* to modify that extension. *Send voicemail notification to - User(s) and Group(s)*: You can select user(s) and group(s) that will receive a notification when this extension receives a voicemail and have access to the voicemails by using the FortiVoice user portal, FortiFone phone or softclient. *User(s)* and *Group(s)*: To select users or groups, click + in the field and select the users/groups. Click *Close*. *View Monitored Voicemails*: This option is only available when you edit an extension. Click to view the list of voicemails that this extension is monitoring, if applicable. If you selected another extension than the default in *Main Voicemail*, then you can filter the list.
Web Access	Configure the access to the user portal and softclient (mobile and desktop) apps. If *Password policy is disabled* appears, see Setting password policies on page 177.
Authentication type	Select the extension authentication type: *Local*, *RADIUS*, or *LDAP* and configure the following settings. RADIUS authentication for desktop and mobile softclients is scheduled for a future release.
If you selected *Local* as the *Authentication type*:	
User password	Enter the password for the access to the user portal and softclient access from mobile or desktop devices. This password can be much longer and stronger to mitigate the risk of password guess attack. To let the system create the user password, click *Generate*. To show the user password, click the eye icon. When you configure the phone system capacity, you can set the *Local authentication type* to one of the following: • User password only • User password or voicemail PIN For more information, see Configuring system capacity on page 120.
If you selected *RADIUS* as the *Authentication type*:	
RADIUS profile	Select or create a RADIUS profile to apply to this extension. For more information about RADIUS profiles, see Configuring RADIUS authentication profiles on page 150.
Authentication ID	Enter the username that is configured in the RADIUS Service of the FortiAuthenticator and to be associated with the extension.

GUI field	Description
If you selected *LDAP* as the *Authentication type*:	
LDAP profile	Select an LDAP profile to apply to this extension. For information about LDAP profiles, see Configuring LDAP profiles on page 130. You can click *New* to create a new profile or *Edit* to modify the selected one.
Authentication ID	During the configuration of the LDAP profile, you have two options for the user authentication: • If you select *Try common name with base DN as bind DN*, update the *Authentication ID* to match the common name attribute (example, uid) that you entered in the *Common name ID* of the profile, such as `jdoe`. • If you select *Search user and try bind DN*, leave the *Authentication ID* blank.
Phone Access	
Voicemail PIN	Enter the password for the extension user to access voicemail. You can check the PIN strength. See Auditing the extension passwords on page 178. To let the system create the user password, click *Generate*. To show the user password, click the eye icon. If you have configured the default voicemail PIN (see Default Voicemail PIN on page 118), the password appears here. However, you can change it.

4. Click *Create* (for new extension) or *OK* (for editing extension).

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 about fax configuration, see Configuring fax on page 315.

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
Enabled	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 315.
Number	Enter the extension number following the extension number pattern. See Configuring FortiVoice options on page 116.
User ID	This is the system-generated ID based on the user ID prefix you set (see User ID prefix on page 118) and the extension number. This option is view only and appears when you edit an extension.
Display Name	Enter the name displaying on the extension.
Description	Enter any notes about the extension.
Device Setting	
SIP settings	Select the SIP profile for the phone. Click the *New* icon to add a new profile. See Configuring SIP profiles on page 138. Click the *Edit* icon to modify a selected profile.
Emergency zone type	Select how you want the assignment of an emergency zone to be made: • *Static*: Manually select the *Emergency zone* profile for the extension. • *Dynamic*: You allow the FortiVoice phone system to identify where the fax machine of the emergency caller is on the network. When a user calls an emergency number, the FortiVoice phone system checks where the fax machine is and assigns a matching emergency zone profile to this device. This assignment is useful when users move their fax machines to different places on the network. • If you select *Dynamic*, enable and update the *Dynamic Network Match* in Configuring emergency zone profiles on page 156.
Emergency zone	If you selected *Static* for the *Emergency zone type*, select the emergency zone profile for the extension. If you want to add a new profile, click the *New* icon. See Configuring emergency zone profiles on page 156. To modify a selected profile, click the *Edit* icon.
Advanced	Click to open the configuration page and click *OK* after completing the task.
SIP password	Enter the password used for configuring your SIP phone from the phone or the web. You need the phone IP to access it from the web. 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 118), the password appears here. However, you can change it.

GUI field	Description
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 settings.
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 about user privilege, see Configuring user privileges on page 151.
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 about extension department, see Configuring agents on page 268.
Web Access	Configure the access to the user portal and softclient (mobile and desktop) apps. If *Password policy is disabled* appears, see Setting password policies on page 177.
Authentication type	Select the extension authentication type: *Local*, *RADIUS*, or *LDAP* and configure the following settings.
If you selected *Local* as the *Authentication type*:	
User password	Enter the password for the access to the user portal and softclient access from mobile or desktop devices. This password can be much longer and stronger to mitigate the risk of password guess attack. To let the system create the user password, click *Generate*. To show the user password, click the eye icon. When you configure the phone system capacity, you can set the *Local authentication type* to one of the following: • User password only • User password or voicemail PIN For more information, see Configuring system capacity on page 120.
If you selected *RADIUS* as the *Authentication type*:	
RADIUS profile	Select or create a RADIUS profile to apply to this extension. For more information about RADIUS profiles, see Configuring RADIUS authentication profiles on page 150.
Authentication ID	Enter the username that is configured in the RADIUS Service of the FortiAuthenticator and to be associated with the extension.
If you selected *LDAP* as the *Authentication type*:	
LDAP profile	Select an LDAP profile to apply to this extension. For information about LDAP profiles, see Configuring LDAP profiles on page 130. You can click *New* to create a new profile or *Edit* to modify the selected one.
Authentication ID	During the configuration of the LDAP profile, you have two options for the user authentication:

GUI field	Description
	• If you select *Try common name with base DN as bind DN*, update the *Authentication ID* to match the common name attribute (example, uid) that you entered in the *Common name ID* of the profile, such as `jdoe`. • If you select *Search user and try bind DN*, leave the *Authentication ID* blank.
Phone Access	Configure voicemail access by phone or access to restricted phone calls.
Voicemail PIN	If you have configured the default user PIN (see Default Voicemail PIN on page 118), the password appears here. However, you can change it. Enter the password for the extension user to access voicemail and the user portal. Selection of using personal password or voicemail PIN to access user portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 120. Click *Generate* to generate a strong password automatically. Select the view PIN icon to display the password.
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 extension comes with its default user preferences, including voicemail setting and phone display preference. You can modify these settings.

Phone users can modify the preferences on the user portal.

To view the list of extensions, go to *Extension* > *Extension* > *Preference*.

GUI field	Description
Maintenance	Select an extension and click an option: *Reset*: To reset the extension preferences to the default values. *Reset Voice Messages*: To delete all voicemails for the selected extensions.
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 voicemails 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
Number	The extension number. This is read-only.
User ID	This is the system-generated ID based on the extension number. This is read-only.
Display name	The name displaying on the extension. This is usually the name of the extension user. 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 115) or the trunk phone number (see Phone Number on page 234). This ID is set when you configure the extension. 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.
Setting	
Ring duration	Enter the phone ringing duration in seconds before an incoming call goes to voicemail. The range is from 6 to 1800 seconds.
Programmable keys	This option is available when an extension is associated with a phone that supports programmable keys. Select the keypad profile for the phone. Click the *Edit* icon to modify a selected profile. See Configuring programmable key profiles on page 146.
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 151.
Call waiting	Select to enable call waiting. • If you enable this option, the following behavior applies: When a second incoming call comes in while the phone user is already on a call, the phone displays the new call information about the screen and plays a beep (if enabled, see *Call waiting tone* option in Configuring phone profiles on page 142). The phone user can answer the second incoming call by placing the in-progress call on hold. • If you disable this option, the following behavior applies: When a second incoming call comes in while the phone user is already on a call, the FortiVoice phone system connects the caller to the voicemail.
Do not disturb	Select to enable the Do not disturb (DND) function on the phone. This function works if the Do not disturb function is enabled in the extension's user privilege. See Configuring user privileges on page 151.

GUI field	Description
Voicemail handling (Caller presses 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 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. Click + to add more email addresses.
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 an audio file (including your name or extension number). The uploaded audio file must meet the following requirements: • WAVE file (WAV) in PCM format or an MP3 file • Maximum size of 10 MB • 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.

GUI field	Description
	• *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 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. The uploaded audio file must meet the following requirements: • WAVE file (WAV) in PCM format or MP3 file • Maximum size of 10 MB • 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. *Greeting File*: If you have uploaded a file by clicking *Audio File*, then select the greeting file. This option is only available when you select *Simple* for *Greeting*. For information about greeting files, see Managing phone audio settings on page 125. If you select *Scheduled* for *Greeting*, click *New* to add a system schedule or create a new one.
Display Preference	Configure the preference for screen display on the user portal.
Phone language	Select the prompt language for the extension. The default is English.
Web language	Select the language for the FortiVoice user portal.
Theme	Select the display theme for the FortiVoice user portal.
Time zone	Select the time zone for the FortiVoice user portal.
Idle timeout	Set the timeout for the FortiVoice user portal.
Account Management	
Change PIN Number	Click to change the password for accessing voicemails and the FortiVoice user portal.
Change User Password	Click to change the password for accessing the FortiVoice user portal.
View Sip Configurations	Click to display the SIP configuration information 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	If enabled, an agent must enter a user PIN to log into a queue or log out of a queue from the extension. For information about feature access codes, see Modifying feature access codes on page 324.

GUI field	Description
PIN required to pause/unpause from phone	If enabled, an agent must enter a user PIN to pause or unpause a queue from the extension. To pause a queue means the agent is not answering calls. For information about feature access codes, see Modifying feature access codes on page 324.
Auto-Pause after agent login queue	If enabled, FortiVoice automatically sets the agent in a pause (not ready) status after the agent logs into a queue. To answer calls, the agent can unpause queue calls. For information about feature access codes, see Modifying feature access codes on page 324.
Follow Me	See Configuring follow me settings on page 214.
Call Handling	*Retain original caller ID*: Select to maintain the original caller 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. *Normal Call Handling* and *Quick Call Handling*, see Handling calls on page 215.
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 151. • *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 215.

To configure follow me settings

1. Go to *Extension* > *Extension* > *Preference*.
2. Double-click a number and go to *Follow Me*.
3. Click *New*.
4. Enter a *Name* for this setting.
5. Under *Follow Me Numbers*, click *New.*
6. Enter a phone number to which the call to your extension can be transferred.
7. Enter the phone ringing duration, in seconds, before the call goes to voicemail or next number in the sequence.

8. Click *Create*.
9. Repeat steps 4 to 8 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.
10. Click *Create*.
11. Click *OK*.

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.*
2. Double-click a number and go to *Call Handling.*
3. Click *Normal Call Handling*.
4. Click one of the tabs for a call status.
   Each status can only be used for one call management configuration.
5. Keep *System default action* or select *User defined*.
   The *System default action* (action shows in brackets) changes depending on the status selection.
6. 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 about configuring schedules, see Scheduling the FortiVoice unit on page 158.
   - 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 about configuring follow me, see Follow Me on page 214.
       This option is available only if call forwarding is enabled in the extension’s user privilege. See Configuring user privileges on page 151.
     - If you select *Play announcement*, select a sound file. For information about configuring sound files, see Managing phone audio settings on page 125
     - If you select *Auto attendant*, select an auto attendant profile. For information about configuring auto attendant, see Configuring auto attendants on page 297.
     - 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 151.
   - Click *Create*.

7. Click *OK*.

To handle a quick call

1. Go to *Extension* > *Extension* > *Preference.*
2. Double-click a number.
3. Go to *Call Handling* .

GUI field	Description
Effective mode	Shows the mode that is active. For example: Effective mode: Away: (expiring at 2022-12-14 01:00:00) If Effective mode is blank, then none of the quick modes are enabled.
*720	To cancel the quick mode and revert the system to its regular schedule, users dial *720 on their phone.
*721	When the code is undefined, you can click the *Click to define* link. By default the mode is *Out of office* . You can set the option and time settings. To enable the *Out of office* schedule, users dials *721 on their phone.
*722	When the code is undefined, you can click the *Click to define* link. By default, the choice is the *Away* mode. You can set the option and time settings. To enable the *Away* schedule, users dials *722 on their phone.
*723	When the code is undefined, you can click the *Click to define* link. By default, the choice is the *Other*mode. You can set the option and time settings. To enable the *Other* schedule, users dials *722 on their phone.

4. If you want to add a new quick call handling process, click *Quick Call Handling*.
5. Select a call status.
   Each status can only be used for one call management configuration.
6. 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 about configuring schedules, see Scheduling the FortiVoice unit on page 158.
   - 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 about configuring follow me, see Follow Me on page 214.
       This option is available only if call forwarding is enabled in the extension’s user privilege. See Configuring user privileges on page 151.
     - If you select *Play announcement*, select a sound file. For information about configuring sound files, see Managing phone audio settings on page 125.
     - If you select *Auto attendant*, select an auto attendant profile. For information about configuring auto attendant, see Configuring auto attendants on page 297.
     - 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 151.
   - Click *Create*.
7. Click *OK*.

Creating extension groups

Extension > *Group* lets you configure extension groups including user groups, extension departments, ring groups, page groups, message groups, pickup groups, and business 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 voicemail, a general voicemail, a ring group, a page group, a message 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 about creating IP extension voicemail, see Configuring IP extensions on page 183.

For information about creating general voicemail, see Setting up a general voicemail on page 224.

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 about extension department, see Creating extension departments on page 217.
5. For *Members,* click in the field and select the available users or user groups that you want to include in the group and click *Close*.
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 about applying department profiles, see Setting up local extensions on page 183.

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 about call centers, see Setting up a call center on page 260.
   1. To set up a call center manager group, under *Manager,* click in the field and select the available users or user groups that you want to include in the group. Click *Close*.
   2. To set up a call center member group, under *Member,* click in the field and select the available users or user groups that you want to include in the group. Click *Close*.
   3. To set up a call center queue group, under *Queue,* click in the field and select the available users or user groups that you want to include in the group. Click *Close*.
6. Click *Create*.

Viewing members of extension departments

You can view which members (groups) are included in an extension department.

1. Go to *Extension* > *Group* > *Department.*
2. Double click a department.
3. Click *View Members*.
4. To get the latest information, click *Run Audit*.

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
Enabled	Select to activate the ring group.
Name	Enter the name for the ring group.
Number	Enter the ring group number following the extension number pattern. See Configuring FortiVoice options on page 116. 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”.
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

GUI field	Description
	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	Click in the field and select the available extensions or user groups that you want to include in the ring group. For information about creating extensions and user groups, see Setting up local extensions on page 183 and Creating extension groups on page 217.
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 219.
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 125. - *Caller ID option*: Select how you want the caller ID to display. - *Retain original caller ID*: Select to keep the original caller ID. - *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. - *Missed call notification*: Select to send a notification email when a call is missed. Enter the email address for the notification.

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 about the *Normal Call Handling* option, see Normal Call Handling on page 219.

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.

The *System default action* changes depending on the status selection.

3. 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 about configuring schedules, see Scheduling the FortiVoice unit on page 158.
   - 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 voicemail.
     - If you select *Play announcement*, select a sound file. For information about configuring sound files, see Managing phone audio settings on page 125.
     - If you select *Auto attendant*, select an auto attendant profile. For information about configuring auto attendant, see Configuring auto attendants on page 297.
     - 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 151.
   - Click *Create*.
4. Click *OK*.

Creating paging groups

A paging group is a group of extensions that can be paged using one number. Paging groups require telephones that support group paging.

A paging group can reach a group of extensions. For example, paging 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 paging group

1. Go to *Extension* > *Group* > *Paging Group.*
2. Click *New*.
3. Enter a name for the group.
4. Enter the paging group number following the extension number pattern. See Configuring FortiVoice options on page 116.
   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 about IVR, see Configuring IVR on page 269.

- *Prefix with Caller ID from IVR:* the caller ID will be prefixed by the IVR caller ID. For information about IVR, see Configuring IVR on page 269.

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*, click in the field and select the available extensions or extension groups that you want to include in the paging group.
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 about message groups, see Creating message groups on page 222.

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 FortiVoice options on page 116. 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.
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 in the field and select the available extensions or extension groups that you want to include in the multicast group.
Emergency call	You can configure whether to interrupt a group member's ongoing call when an emergency multicast page from this group comes in. • *Not an emergency page*: Ongoing calls are not affected by a multicast paging group call and operate according to the call handling actions you set. See Configuring call routing on page 248. • *Disconnect ongoing call*: Ongoing calls on FortiFone-x80 phones will be disconnected and replaced with an incoming emergency multicast page. • *Hold ongoing call*: Ongoing calls on FortiFone-x80 phones will be placed on hold and replaced with an incoming emergency multicast page.

GUI field	Description
Exempt ongoing numbers	This field is visible when you select either *Disconnect ongoing call* or *Hold ongoing call* for *Emergency call*. Enter the extension numbers that you want to exclude from the emergency call rules. Ongoing calls from the group member FortiFone-x80 extensions to the extensions you entered will not be interrupted when an emergency multicast page from this group comes in, even when the *Emergency call* setting is *Disconnect ongoing call* or *Hold ongoing call*. You can exempt up to 10 extension numbers. If you leave the field empty, this multicast paging group's extension number will be exempted by default.
Description	Select *Edit* to enter any notes you have for the group.

3. Click *Create*.

Creating message groups

A message group provides a mass notification service for delivering messages to the following endpoints:

- FortiFone IP desk phones can receive audio and text messages.
- FortiFone softclient for desktop app can receive text messages.

This solution supports standalone FortiVoice deployments and/or integration with third-party mass notification systems to provide emergency notifications.

For more information about multicast paging groups, see Creating multicast paging groups on page 221.

To create a message group

1. Go to *Extension* > *Group* > *Message Group.*
2. Click *New* and configure the following:

GUI field	Description
Enabled	Select to activate this group.
Name	Enter a unique name for the group.
Number	Enter the message group number following the extension number pattern. See Configuring FortiVoice options on page 116. 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”.
Message type	Select to send text or audio messages.
If you select to send a text message, click *Text* and configure the following:	
Title	Enter the message title.
Message	Use the variables to compose your message or enter your message directly.

GUI field	Description
Display time	Enter the time period (in seconds) that you want the message to display on the extension phones. The range is from 0 to 86400. If you want the message to display on the FortiFone phone screen permanently until the user takes action, enter 0.
Delay	Enter the time period (in seconds) that you want to delay sending the text. The range is from 0 to 120.
Alert tone	Select to activate notification alert on the extensions.
User group	Select the user groups for this message group. To add a user group, click + and fill in the fields. For information about user groups, see Creating user groups on page 217.
If you select to send an audio message, click *Audio* and configure the following:	
Sound file	Select an existing sound file or click *New* to create a new one for the audio message. For information about sound files, see Managing phone audio settings on page 125
Multicast group	Select the multicast paging group for this message group or click *New* to create a new one for the audio message. You can also click *Edit* to modify the selected one. For information about multicast groups, see Creating multicast paging groups on page 221.
Single number	Enter the external phone number to which you want to send this message and click *OK*. You can enter digits from 0 to 9.
Description	Select *Edit* to enter any notes you have for the group.

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 324.

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*, click in the field and select the extensions or user groups that you want to include in the pickup group.
7. Click *Close*.

   For information about creating extensions and user groups, see Setting up local extensions on page 183 and Creating extension groups on page 217.

8. For *Pickup by members*, click in the field and select the extensions or user groups that are allowed to answer incoming calls that ring on other extensions.
9. Click *Close*.
10. Click *Create*.

Creating business groups

Business groups introduce an abbreviated extension number dialing for phone users in the same logical group. As an example, lets use a company where employees are located in three different offices (locations 1, 2, and 3). Each location uses a different prefix code (11, 12, 13) but the same numbering pattern (XXX). Therefore, extensions in location 1 can be 11801, 11802, 11803, and so on. Extensions in location 2 can be 12801, 12802, 12803 and so on. Extensions in location 3 can be 13801, 13802, 13803, and so on.

When phone users in location 1 want to reach an extension in the same business group (location 1), they can dial the abbreviated extension (such as XXX) instead of the full extension number (11XXX).

When phone users in location 1 want to reach an extension in another business group (such as location 2), they dial the full extension number (such as 12XXX).

The business group option is available when you are using the following models and settings only:

- FVE-500F and larger models only
- Under *Phone System* > *Setting* > *Miscellaneous*, go to *Business Group* and select *Automatic*.

To create a business group

1. Go to *Extension* > *Group* > *Business Group.*
2. Click *New*.
3. Enter a *Name* for the group.
4. Enter the extension *Abbreviated prefix code* for the group. You can enter digits from 0 to 9. The allowed length is from 2 to 8 digits.
5. For *Abbreviated dialing pattern*, enter the pattern by following the pattern-matching syntax. For example, XXXX matches any four-digit number. For more details about the pattern-matching syntax, see Configuring FortiVoice options on page 116.
6. For *Description*, click *Edit* to enter any notes you have for the group.
7. Click *Create*.

Creating SLA groups

For details about shared line appearance (SLA) groups, see Appendix A: Shared line appearance on page 370.

Setting up a general voicemail

Some organizations, such as the sales team of a company, may have the need to share voicemails within multiple users or a user group for better service and efficiency. With a general voicemail, when there is a new voicemail, the entire group is copied or notified. Any member of the group can access the voicemail and once this is done, the notification is gone and others know that the voicemail has been taken care of.

To set up a general voicemail

1. Go to *Extension* > *General Voicemail* > *General Voicemail.*
2. Click *New*.
3. Configure the following:

GUI field	Description
Enabled	Select to activate the voicemail extension.
Number	Enter the voicemail extension number following the extension number pattern. See Configuring FortiVoice options on page 116.
User ID	This is the system-generated ID based on the voicemail extension number. This option is view only.
Display name	Enter the name of the voicemail extension.
Description	Enter any notes for the extension's voicemail.
User Setting	
Management	Configure the voicemail extension's role in other settings.
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 about user privilege, see Configuring user privileges on page 151.
Voicemail	Configure the users for sharing this extension's voicemail. *Mode*: Select the way to deliver the voicemail from this extension to the users sharing this voicemail. • *Centralized*: Select to copy or notify the entire group when a new voicemail comes in. Any member of the group can access the voicemail and once this is done, the notification is gone and others know that the voicemail has been taken care of. • *Notify message waiting light*: If you select this option, the FortiVoice unit turns on the message waiting light on a user's phone when a new voice message is left on this voicemail. • *List as mailbox*: Users can listen to a centralized voicemail by dialing *97 or the customized code (see Modifying feature access codes on page 324) from their own extensions and enter the personal voicemail PIN for this general voicemail. • *Broadcast*: If you select this option, the voicemail is sent to the voicemail of the users. Users can access the voicemail by dialing *98 or the customized code (see Modifying feature access codes on page 324) from any extensions and enter the personal voicemail PIN. • *User(s)/Group(s)*: Select the users or groups to notify when a voicemail is left in this voicemail extension. To select the users or groups to share this voicemail, click the + sign in the field and choose the users or groups. Click *OK*. For information about creating user groups, see Creating extension groups on page 217.

GUI field	Description
Web Access	Configure user portal and softclient access from mobile or desktop devices. If *Password policy is disabled* appears, see Setting password policies on page 177.
Authentication type	Select the extension's authentication type: *Local* or *LDAP*.
User password	If you selected *Local* as the *Authentication type*, enter the password for user portal access. This password can be much longer and stronger to mitigate the risk of password guess attack and preserve the voicemail PIN for phone access only. To let the system create the user password, click *Generate*. To show the user password, click the eye icon. Control of using user password or voicemail PIN to access user portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 120.
LDAP profile	If you select *LDAP* for *Authentication type*, select an LDAP profile to apply to this extension. For information about LDAP profile, see Configuring LDAP settings on page 130. You can click *New* to create a new profile or *Edit* to modify the selected one.
Authentication ID	This option is available if you selected *LDAP* or *RADIUS* for *Authentication type*. • For LDAP: During the configuration of the LDAP profile, you have two options for the user authentication: • If you select *Try common name with base DN as bind DN*, update the *Authentication ID* to match the common name attribute (example, uid) that you entered in the *Common name ID* of the profile, such as `jdoe`. • If you select *Search user and try bind DN*, leave the *Authentication ID* blank. • For RADIUS: Enter the username that is configured in the RADIUS Service of the FortiAuthenticator and to be associated with the extension.
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 portal. Selection of using personal password or voicemail PIN to access user portal is set when configuring phone system capacity. For more information, see Configuring system capacity on page 120. You can check the PIN strength. See Reviewing system configuration on page 168. 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 118), the password appears here. However, you can change it.

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 voicemail. 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
Enabled	Select to activate this virtual number.
Name	Enter a name for the virtual number.
Number	Enter the virtual number which is not assigned to any phone. The virtual number must be between 0 and 9.
Display name	Enter the name displaying on the extension. This is usually the name of the extension user.
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 227.

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 about the *Call Handling* option, see Call Handling on page 227.

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 about configuring schedules, see Scheduling the FortiVoice unit on page 158.
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 183 and Configuring call routing on page 248.

This topic includes:

- Configuring VoIP trunks on page 229
- Configuring PSTN/PRI trunks on page 235
- Configuring analog voice trunks on page 240
- Configuring office peers on page 242
- Setting up routing rules for FXO and PRI gateways on page 247

Configuring 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).

If you are accessing a FortiVoice FVE-20E2, FVE-50E6, or FVE-50G2 model that is a survivability branch managed by a main office FortiVoice system, *Trunk* > *VoIP* > *SIP* can show two SIP trunks mapped to two analog extensions associated with the FXS ports. For more details about survivability branches, see the FortiVoice Local Survivable Gateway Deployment Guide.

To view the list of VoIP service providers

1. Go to *Trunk* > *VoIP* > *SIP*.
2. You can view the following buttons and columns:

GUI field	Description
Test	Select to test if the trunk is created successfully. The duration of the test call is limited to 60 seconds. For more information, see Testing SIP trunks on page 234.
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 235.
Enabled	Select to activate this trunk.

GUI field	Description
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. • *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

Create a VoIP trunk for inbound and outbound calls.

1. Go to *Trunk > VoIP > SIP.*
2. Click *New*.
3. Configure the following:

GUI field	Description
Enabled	Select to activate the SIP trunk.
Name	Enter a name for this trunk such as the name of the VoIP service provider.
Display name	Enter your caller ID that will appear on the called phone, such as Example Company. For details about the caller ID hierarchy, see the Caller ID modification section in the FortiVoice Cookbook.
Main number	Enter the phone number provided by the VoIP service provider.
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 SRV 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 that 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 settings	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 + to add a new one. For more information, see Configuring SIP profiles on page 138.
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 142. 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. The value range is from 1 to 450.
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 about dialplans, see Configuring call routing on page 248. 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, if the max channel number is 10 and you want to reserve 4 channels for incoming calls, then you can enter 6 for *Max outgoing channel*. The value range is from 0 to 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.
Inband ringtone (Early media)	Select to enable the FortiVoice unit to send ring tone to the caller of an incoming call before the establishment of a call connection.
Caller ID Option	Configure how to display your caller ID to meet the different requirements and scenarios of the service providers. Caller ID information is contained in the From header and P-Asserted-Identity header of SIP packets sent to the called phone's PBX. *From header*: The From header field indicates the identity of the initiator of the call request from the point of view of the PBX server. • SIP user name: Select if you want the user name provided by the VoIP service provider for the FortiVoice unit to register with the SIP server to appear on the called phone. See User name on page 230. • Caller ID priority rule: Select if you want to configure your FortiVoice caller ID

GUI field	Description
	according to the FortiVoice caller ID priority hierarchy: • Emergency caller ID: See Setting extension user preferences in Setting up local extensions on page 183. • External caller ID: See Setting extension user preferences on page 210. • DID mapping caller number: See Configuring inbound dial plans on page 248. • Trunk caller ID: See Main number on page 230. • PBX caller ID (Main display name): See Configuring phone system settings on page 114. • Main number: Select if you want the trunk main number to appear on the called phone. See Main number on page 230. • Specified: Enter the ID you want to display on the called phone in the format of `display name <number>`. *P-Asserted-Identity header*: This header contains the caller ID information for the call on the INVITE SIP packet. • No PAI header: Select if you want to disable PAI header. • Caller ID priority rule: Select if you want to configure your FortiVoice caller ID according to the FortiVoice caller ID priority hierarchy: • Emergency caller ID: See Setting extension user preferences in Setting up local extensions on page 183. • External caller ID: See Setting extension user preferences in Setting up local extensions on page 183. • DID mapping caller number: See Configuring inbound dial plans on page 248. • Trunk caller ID: See Main number on page 230. • PBX caller ID (Main display number): See Configuring phone system settings on page 114. • Main number: Select if you want the trunk main number to appear on the called phone. See Main number on page 230. • Specified: Enter the ID you want to display on the called phone in the format of `display name <number>`. *Diversion Header Use*: Allows you to set the use of the diversion header for call twinning, call forwarding, or normal outbound calls. • On Redirect: Use the diversion header during call twinning and call forwarding. • No Diversion Header: Disable the use of the diversion header for all calls. • Always: Allow the diversion header to be applied to all calls. *Diversion Header Source*: • DID Mapping: Use the mapped DID if available, then use the caller ID (CID) of the main trunk. • Trunk Caller ID: Use the caller ID of the main trunk.
Registration	
Type	Enter the SIP registration information from the VoIP service provider by selecting a registration method in *Type*. You can receive calls after registering with the SIP server of the VoIP service provider.

GUI field	Description

	• *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. The string in Registration URI has the following format:
	`<user>@<host><:port>`
	where `<user>` is the user name.
	`<host>` is a hostname, domain name, FQDN, or IP address.
	`<:port>` is the port number. If you omit to specify a port, the default port (5060) is used.
	Examples:
	`support@mycompany.com`
	`support@mycompany.com:6000`
	`bob@168.176.248.255`
	• *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: • 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	
Automatic fax detection	⚠ Selecting this option may cause the following behaviors: • Delay the call response time on this trunk by automatically adding two ring tones to detect incoming fax signals. • Affect toll charges on incoming lines. Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically.

GUI field	Description
Forward to DID mapping extension	This option is available when you select *Automatic fax detection*. Select this option if a DID number is mapped directly to an extension to receive voice and fax calls (see details in To map a personal fax DID number on page 253). Faxes will be sent to the extension's personal fax account, accessible through the User Portal. In *Forward to eFax account* (next field), select an eFax account (as configured in Receiving faxes on page 316). Should a fax fail to be received by the DID mapping extension, the FortiVoice will use this eFax account as a fallback.
Forward to eFax account	This option is available when you select *Automatic fax detection*. Select or edit an eFax account to receive faxes. To add a new eFax account, click +. For details about the eFax account configuration, see Receiving faxes on page 316.
Phone Number	Adding a phone number in this field is optional and for information purposes only. The phone number supports digits from 0 to 9 and a maximum of 63 digits. Click *New* to add a phone number provided by your VoIP service provider. Click *Create* when done. You can add multiple phone 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 229.

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* if you want to run a system SIP trunk test without making a real phone call, or *Test Call* if you want to test the SIP trunk by making a real phone 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.
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.

GUI field	Description
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. Take note of 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 233.
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.

Configuring PSTN/PRI trunks

This section applies to the FVE 300E-T model only.

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 *Trunk* > *PRI* > *PRI.*
2. Click *New*.
3. Configure the following:

GUI field	Description
Trunk Setting	
Enabled	Select to activate the trunk.
Name	The name of this trunk.
Display name	Enter your caller ID, such as Example Company.
Number	Enter the phone number provided by the VoIP service provider.
Status	Shows the status of the PRI trunk.
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 *Span*, click in the field and select the span for the trunk from the popup window.
Edit span	Click Edit (✎) after selecting a span to configure the settings of the T1/E1 span to match the same settings of your PSTN service provider. Click *OK* after finishing the configuration. For more information, see Configuring the T1/E1 span on page 237.
Span	Click in the field and select the span for the trunk from the popup window.
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.

GUI field	Description
Automatic fax detection	Selecting this option may cause the following behaviors: • Delay the call response time on this trunk by automatically adding two ring tones to detect incoming fax signals. • Affect toll charges on incoming lines. Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically.
Forward to DID mapping extension	This option is available when you select *Automatic fax detection*. Select this option if a DID number is mapped directly to an extension to receive voice and fax calls (see details in To map a personal fax DID number on page 253). Faxes will be sent to the extension's personal fax account, accessible through the User Portal. In *Forward to eFax account* (next field), select an eFax account (as configured in Receiving faxes on page 316). Should a fax fail to be received by the DID mapping extension, the FortiVoice will use this eFax account as a fallback.
Forward to eFax account	This option is available when you select *Automatic fax detection*. Select or edit an eFax account to receive faxes. To add a new eFax account, click +. For details about the eFax account configuration, see Receiving faxes on page 316.
Phone Number	Adding a phone number in this field is optional and for information purposes only. The phone number supports digits from 0 to 9 and a maximum of 63 digits. Click *New* to add a phone number provided by your VoIP service provider. Click *Create* when done. You can add multiple phone numbers.

4. Click *OK*.

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.

To configure the T1/E1 span

1. On the *Trunk > PRI > PRI* page, select a PRI trunk and click *Edit*.
2. In *Hardware Property*, go to *Edit span*, select a span, and click Edit ✎.
3. 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.

GUI field	Description
Signaling	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 options	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.
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 237, 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 237, the typical channel settings 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.

GUI field	Description
Dialplan type (TON)	This option is active when you select *PRI signalling, CPE side* or *PRI signalling, network side* for Signaling on page 238. The service provider supplies the value for this option. Select the type of number (TON) which is the number format to use when placing a call from FortiVoice to the provider.
Local dialplan type (TON)	This option is active when you select *PRI signalling, CPE side* or *PRI signalling, network side* for Signaling on page 238. The service provider supplies the value for this option. Select the TON or number format to use for incoming calls from the provider to FortiVoice.
Connected party notification diaplan type (TON)	This option is active when you select *PRI signalling, CPE side* or *PRI signalling, network side* for Signaling on page 238. The service provider supplies the value for this option. Select the TON or number format to use in the caller ID and remote party ID (if supported by the provider).
PRI indication	This option is active when you select *PRI signalling, CPE side* or *PRI signalling, network side* for Signaling on page 238. The service provider typically supplies the value for this option. However, some providers allow this value to be set on the PBX. • *In-band*: Call failure tones (for example, busy signals and out of service messages) are played back as audio from the provider. • *Out-of-band*: FortiVoice generates call failure tones with the provider sending a code instead of a tone. Some automated dialing scenarios require this setting, but end users will often lose extra information that may be included in the recorded message.
PRI R2 Setting	This option is active when you select PRI R2 signalling for Signaling on page 238. Since there is no single signaling standard for R2, the FortiVoice unit addresses this challenge by supporting many localized implementations of R2 signaling.
Country	Select the country for the 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. The default is 20.
Max DNIS digits	A 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. Enter the number of digits of a dialed call to be sent by the telephone company. The default is 20.
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.

GUI field	Description
	- *DTMF answering*: Select to enable dual-tone multi-frequency signaling (DTMF) answering.
Allow collect calls	Select to allow collect calls.
MF timeout	To enable the multi-frequency (MF) timeout, enter a value in milliseconds. The default is -1, which disables the setting.
Metering pulse timeout	To enable the metering pulse timeout, enter a value in milliseconds. The default is -1, which disables the setting.

4. Click *OK*.

Configuring analog voice trunks

This section applies to the following models only:

- FVE-20E2
- FVE-50E6

To configure an analog voice trunk

1. Go to *Trunk > Analog > Analog*.
2. Click *New*.
3. Configure the following:

GUI field	Description
Trunk Setting	
Enabled	Select to activate the trunk.
Name	Enter a name for this trunk.
Display name	Enter your caller ID, such as Example Company.
Number	Enter the phone number provided by the VoIP service provider.
Hardware Property	
Port	Click + and select the FXO ports you want for this trunk. Click *Close*. 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	

GUI field	Description
Automatic fax detection	Selecting this option may cause the following behaviors: • Delay the call response time on this trunk by automatically adding two ring tones to detect incoming fax signals. • Affect toll charges on incoming lines. Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically.
Forward to DID mapping extension	This option is available when you select *Automatic fax detection*. Select this option if a DID number is mapped directly to an extension to receive voice and fax calls (see details in To map a personal fax DID number on page 253). Faxes will be sent to the extension's personal fax account, accessible through the User Portal. In Forward to eFax account (next field), select an eFax account (as configured in Receiving faxes on page 316). Should a fax fail to be received by the DID mapping extension, the FortiVoice will use this eFax account as a fallback.
Forward to eFax account	This option is available when you select *Automatic fax detection*. Select or edit an eFax account to receive faxes. To add a new eFax account, click +. For details about the eFax account configuration, see Receiving faxes on page 316.
Phone Number	Adding a phone number in this field is optional and for information purposes only. The phone number supports digits from 0 to 9 and a maximum of 63 digits. Click *New* to add a phone number provided by your VoIP service provider. Click *Create* when done. You can add multiple phone numbers.

4. Click *Create*.

To configure the PSTN settings of an analog voice trunk

This section applies to the following models only:

- FVE-20E2
- FVE-50E6

You can configure the PSTN settings of the analog voice trunk to match the same setting of your PSTN service provider.

1. Go to *Trunk > Analog > Analog*.
2. Select a trunk.
3. Click *PSTN Setting*.
4. Configure the following:

GUI field	Description
Name	The name of this configuration. This is view-only.

GUI field	Description
Codec	Select the Codec for the trunk.
Caller ID signalling	Select the caller ID signalling standard per your phone company's request.
First digit timeout Match digit timeout	Enter the timeout in milliseconds. The following example explains both timeout settings using default values. The user picks up the phone handset and hears a dialtone. If the user does not enter a digit within the specified 16 seconds (first digit timeout), the dialtone restarts. After pressing the first digit, the user has 3 seconds (match digit timeout) to enter the next digit. After the user's finger is off the button, the timer resets and the user has another 3 seconds to enter the next digit and so on. When the 3-second timer expires, the phone number is identified as complete, and the call is attempted. The default *First digit timeout* is 16000. The default *Match digit timeout* is 3000.

5. Click *OK*.

Configuring office peers

If you have 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.

You can set up three types of peer offices:

- Site to site: The office peer uses a FortiVoice unit and is in an equal position with your FortiVoice unit, rather than a primary/secondary relationship.
- Remote access: The office peer uses a FortiVoice unit and is in a primary/secondary relationship with your FortiVoice unit.
- Custom: The office peer uses a third-party PBX.

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 244) 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 43.
Enabled	Select to activate this trunk.
Name	The name of the office peer.
Display name	Enter the name displaying on the extension.

GUI field	Description
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. For more information, see Configuring FortiVoice options on page 116.
5. Review the basic *New office peer information*, click *Next*.
6. Configure the following:

GUI field	Description
Enabled	Select to activate the trunk.
Name	Enter a name for the trunk.
Display name	Enter the name displaying on the extension.
Peer Configuration	
Remote Host/IP	Enter the domain name or IP address of the office peer's FortiVoice unit.
Port	Enter the port number for VoIP network on the office peer's FortiVoice unit.
Authentication	Optionally, you may configure to authenticate the peer.
Disabled	If you do not need authentication for the office peer, select this option to disable it.
Symmetric	If you want to authenticate the FortiVoice units forming the office peer trunk, enter the *User name* and *Password*. These settings must be the same on both units. The FortiVoice unit on each end will use the settings 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 settings must be the same on both FortiVoice units forming the office peer trunk.

GUI field	Description
	The unit on each end will use the settings 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 same option is selected on the office peer's FortiVoice 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 43.
Share metric	Enter the hop count value for this FortiVoice unit to share the phone directory with an office peer. Example 1: You have configured the following deployment: • A and B are office peers. • A and C are office peers. If you want A, B, and C FortiVoice systems to share their phone directories, enter 2 on all three FortiVoice systems. Example 2: If your enter 1, the directory can only be shared with the first peer office site designated on the routing table of this FortiVoice unit.
SIP settings	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 138.
Max channel	Enter the maximum voice channels for the trunk. The value range is from 1 to 450.

7. Click *Create*.

To set up a remote access office peer

1. Go to *Trunk > Office Peer > Office Peer.*
2. Click *New*.
3. Under *Office peer type*, click *Remote Access*.
4. Select the role for the office peer: *Central* or *Satellite*.
5. If you want to change your local number pattern, click the *Edit* icon beside *Local/incoming digit pattern* to modify it. For more information, see Configuring FortiVoice options on page 116.
6. Review the basic *New office peer information*, click *Next*.
7. Configure the following and click *Create*.

GUI field	Description
Enabled	Select to activate the trunk.
Name	Enter a name for the trunk.
Display name	Enter the name displaying on the extension.
Peer Configuration	
Central Host/IP	This option is only available if you choose *Satellite* as the role of the office peer. Enter the domain name or IP address of the primary FortiVoice unit which is your local unit.
Port	This option is only available if you choose *Satellite* as the role of the office peer. Enter the port number for VoIP network on the primary FortiVoice unit.
User name	To authenticate the FortiVoice units forming the office peer trunk, enter the *User name* . This name must be the same on both units. The FortiVoice unit on each end will use this user name to authenticate each other.
Password	To authenticate the FortiVoice units forming the office peer trunk, enter the *Password*. This password must be the same on both units. The FortiVoice unit on each end will use this password to authenticate each other.
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 same option is selected on the office peer's FortiVoice 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 43.
Share metric	Enter the hop count value for this FortiVoice unit to share the phone directory with an office peer. Example 1: You have configured the following deployment: • A and B are office peers. • A and C are office peers. If you want A, B, and C FortiVoice systems to share their phone directories, enter 2 on all three FortiVoice systems. Example 2: If your enter 1, the directory can only be shared with the first peer office site designated on the routing table of this FortiVoice unit.
SIP settings	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 138.
Max channel	Enter the maximum voice channels for the trunk.

GUI field	Description
	The value range is from 1 to 450.
More	This option is only available if you choose satellite as the role of the office peer. This feature is used for remote access office peer connection through a proxy server, such as the case in a FortiVoice Cloud deployment.
DNS SRV record	The DNS service (SRV) record provides host and port information for specific services such as voice over IP (VoIP). SIP needs to connect to a specific port on a specific server. Enable this option to allow the FortiVoice unit to query the DNS SRV record for the IP address and port number of the central FortiVoice unit (office peer) to register.
Proxy	To connect to the central office peer through a proxy server, do the following: • If you have enabled *DNS SRV record*, enable *Proxy* and enter the unique hostname of the central office peer in the *(Host/IP)* field. The DNS SRV record will use the information to look for and provide the IP address and port number of the central office peer. • If you do not want to use the *DNS SRV record* service and therefore did not enable it, enable *Proxy* and enter the unique hostname of the central office peer in the *(Host/IP)* field. Also select the port number and communication protocol for the central office peer. The DNS server will use the information to look for and provide the IP address of the central office peer. • If you know the IP address of the central office peer, enter it in the *(Host/IP)* field. In this case, you do not need to enable *DNS SRV record*.
Registration interval	Select the time (in seconds) needed for your FortiVoice unit to register to the central office peer until it receives a response.

8. Click *Create*

To set up a custom office peer

1. Go to *Trunk* > *Office Peer* > *Office Peer.*
2. Click *New*.
3. Under *Office peer type*, click *Custom*.
4. Review the basic *New office peer information*, click *Next*.
5. Configure the following:

GUI field	Description
Enabled	Select to activate the trunk.
Name	Enter a name for the trunk.
Display name	Enter the name displaying on the extension.
Peer Configuration	
Connection (Site to Site)	
Host/IP	Enter the domain name or IP address of the office peer’s PBX.
Port	Enter the port number for VoIP network on the office peer’s PBX.

GUI field	Description
Authentication	Optionally, you may configure to authenticate the peer.
	Disabled: 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 settings must be the same on both PBXes. The PBX on each end will use the settings 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 settings must be the same on both PBXes forming the office peer trunk. The PBX on each end will use the settings to authenticate incoming and outgoing calls.
Connection (Remote Access Central)	
User name	To authenticate the PBXes forming the office peer trunk, enter the *User name* . This name must be the same on both PBXes. The PBX on each end will use this user name to authenticate each other.
Password	To authenticate the PBXes forming the office peer trunk, enter the *Password*. This password must be the same on both PBXes. The PBX on each end will use this password to authenticate each other.
Advanced	
Call routing	Create outgoing and incoming dial plans for the local and peer offices. For more information, see Configuring call routing on page 248.
SIP settings	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 138.
Max channel	Enter the maximum voice channels for the trunk. The value range is from 1 to 450.

6. Click *Create*.

Setting up routing rules for FXO and PRI gateways

After you create FXO or PRI gateways under *Managed System*, go to *Trunks* and refresh your browser. *Gateways* appears and lists all FXO or PRI gateways that you have 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 detailed instructions about deploying a FXO gateway, see the FortiVoice FXO Gateway Deployment Guide.

For detailed instructions about deploying a PRI gateway, see the FortiVoice PRI Gateway Deployment Guide.

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 248
- Configuring direct inward dialing on page 251
- Viewing office peers for inbound calls on page 254
- Configuring outbound dial plans on page 254
- Viewing office peers for outbound calls on page 259

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 settings 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 249.
Handling Description	The specific call handling actions.
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 249.
Match CID	The caller ID pattern for this dial plan. For details, see Caller ID Match on page 249.

To set up an inbound dial plan

1. Go to *Call Routing* > *Inbound* > *Inbound.*
2. Click *New*.

3. Configure the following:

GUI field	Description
Enabled	Select to activate this dial plan.
Name	Enter a name for this plan.
From Trunk	Select the trunks of the incoming calls that are subject to this dial plan. Click + and select the trunks. Click *Close*.
Dialed Number Match	If you configure *Dial Local Number on page 250*, FortiVoice ignores this *Dialed Number Match* setting. With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers. When a called number matches this pattern, FortiVoice follows the dial plan rule that you configure in *Call Handling on page 249* (*Endpoint Action* or *Call Routing*). Create the number match by following the Pattern-matching syntax on page 256 and Pattern-matching examples on page 257.
Caller ID Match	Click *New* to set the caller ID pattern following the Pattern-matching syntax on page 256 and Pattern-matching examples on page 257 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	Click + and select one or more caller ID modification configurations. Click *Close*. You can associate multiple caller ID modification configurations with a dial plan. For more information about caller ID modification, see Modifying caller IDs on page 140.
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.
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. To configure this action type: **1.** In *Action type*, select *Endpoint Action*. **2.** Click *New*. **3.** Select the *Schedule* for the action. For more information about FortiVoice schedule, see Scheduling the FortiVoice unit on page 158. **4.** 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*). **5.** Click *Create*. **6.** If you need more actions for this action type, repeat this procedure. To avoid schedule conflicts, do not use the same schedule for more than one

GUI field	Description
	action.
Dial Local Number	When you configure this *Dial Local Number* setting, FortiVoice ignores the *Dialed Number Match on page 249*. Select this action type 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. To configure this action type: **1.** In *Action type*, select *Dial Local Number*. **2.** Click *New*. **3.** Add a number pattern in *Match Pattern* following the Pattern-matching syntax on page 256 and Pattern-matching examples on page 257 for this dial plan. Repeat to add more patterns. **4.** 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. **5.** 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. **6.** 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 number. **7.** Click *Create*.
Call Routing	Select if you want to route incoming calls from the FortiVoice unit to an external phone system using an outbound dial plan. To configure this action type: **1.** In *Action type*, select *Call Routing*. **2.** You can choose to enable the *Retain original caller ID*. **3.** Click + to select the available outbound dial plans. This means that the FortiVoice unit will route incoming calls to an external phone system using the selected outbound dial plans. For details, see Configuring outbound dial plans on page 254.

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.

A DID number allows an inbound caller to bypass the auto attendant and directly reach a company employee or department.

A phone company can offer a DID service to provide a block of telephone numbers for calling into your company FortiVoice unit (PBX) 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 extension because each DID number can only be mapped to one extension. To address this issue, the FortiVoice unit offers the following two options:

- Only map the DID numbers to the extensions you want.
- Bundle caller number patterns to a DID number which can be mapped to any extension.

You cannot delete or move the two default DID mapping rules (system_voice and system_fax).

FortiVoice also gives you the option to provide a fax account to a user by mapping the user's extension to a DID number. Users can manage their personal fax account in the FortiVoice user portal.

This personal fax account is different from the eFax account which is used as a general fax for an organization. For information about eFax, see Configuring fax on page 315.

This section includes the following topics:

- To map a standard voice DID number on page 251
- To map an advanced voice DID number on page 252
- To map a personal fax DID number on page 253

To map a standard voice DID number

1. Go to *Call Routing* > *Inbound* > *DID Mapping.*
2. Click *New* and select *Voice - Standard.*

3. Configure the following:

GUI field	Description
Enabled	Select to activate this DID setting.
Rule name	Enter a name for this DID setting.
Condition	Select the trunk used for dialing the DIDs.
Additional Action	Select the fallback action to take should a call fail to be received by the DID mapping extension. For some actions, you need to enter the extension, such as *Dial voicemail*.
Number Mapping	Click *New* and update the following settings: • *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. The DID number can start with one or multiple optional plus signs followed by a maximum of 16 digits. • *Extension*: Enter the extension that you want to map to the DID number. The extension supports digits from 0 to 9 and a maximum of 16 digits. • *Description*: Enter any notes you have for the mapping.

4. Click *Create*.

To map an advanced voice DID number

1. Go to *Call Routing > Inbound > DID Mapping.*
2. Click *New* and select *Voice - Advanced.*
3. Configure the following:

GUI field	Description
Enabled	Select to activate this DID setting.
Rule name	Enter a name for this DID setting.
Condition	• *Trunk*: Select the trunk used for dialing the DIDs. • *Schedule*: Select a schedule to apply the rule. For information about creating schedules, see Scheduling the FortiVoice unit on page 158. • *Caller ID Match*: Click *New* to set the caller ID pattern following Pattern-matching syntax on page 256 and Pattern-matching examples on page 257 for this dial plan, and click *Create*.
Additional Action	• *Inbound caller ID modification*: Select the caller ID modification configuration. For more information about caller ID modification, see Modifying caller IDs on page 140. • *Inbound fallback action*: Select the fallback action to take should a call fail to be received by the DID mapping extension. For some actions, you need to enter the extension, such as *Dial voicemail*.
Number Mapping	Click *New* and update the following settings: • *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

GUI field	Description
	DID mapping configuration cannot be saved. The DID number can start with one or multiple optional plus signs followed by a maximum of 16 digits. • *Extension*: Enter the extension that you want to map to the DID number. The extension supports digits from 0 to 9 and a maximum of 16 digits. • *Description*: Enter any notes you have for the mapping. • *Option*: • To direct incoming calls to the extension through the mapped DID, select *Inbound*. If this option is not selected, incoming calls to this extension through the mapped DID will follow the inbound fallback action configured in Additional Action on page 252. By default, this option is selected. • 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, select *Outbound*. 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 115) or the trunk phone number (see Phone Number on page 234) associated with the extension. Alternatively, you can choose the caller ID to display on the called phone when configuring an extension. • *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. • The caller number pattern supports digits from 0 to 9, a maximum of 16 digits, and optionally starts with one or more + signs.

4. Click *Create*.

To map a personal fax DID number

1. Go to *Call Routing* > *Inbound* > *DID Mapping.*
2. Click *New* and select *Fax*.

3. Configure the following:

GUI field	Description
Enabled	Select to activate this DID setting.
Rule name	Enter a name for this DID setting.
Condition	*Trunk*: Select the trunk used for dialing the DIDs.
Additional Action	*Inbound fallback action*: Select the fallback action to take should a fax fail to be received by the DID mapping extension. For some actions, you need to enter the extension, such as *Dial voicemail*.
Number Mapping	• *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. The DID number can start with one or multiple optional plus signs followed by a maximum of 16 digits. • *Extension*: Enter the extension that you want to map to the DID number. The extension supports digits from 0 to 9 and a maximum of 16 digits. • *Description*: Enter any notes you have for the mapping.

4. 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 242.

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 256.
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 255.
Match CID	The caller ID pattern for this dial plan. For details, see Caller ID Match on page 255.
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 255.

To set up an outbound dial plan

1. Go to *Call Routing* > *Outbound* > *Outbound*.
2. Click *New*.
3. Configure the following:

GUI field	Description
Enabled	Select to activate this dial plan.
Name	Enter a name for this plan.
Emergency Call	Select to allow emergency call with this plan. By default, this is selected. For information about setting emergency number, see Setting FortiVoice location, contact, and emergency information on page 114.
Retain original caller ID	Select to keep the original caller ID.
Caller ID Match	Enter the caller ID pattern following Pattern-matching syntax on page 256 and Pattern-matching examples on page 257 for this dial plan. Click + if you need to enter more caller ID patterns. You can enter 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 about adding a dialed number match, see Creating dialed number match on page 256.
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 258.

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 255.

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. 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 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.

Syntax	Description
Z	Matches any single digit from 1 to 9.
N	Matches any single digit from 2 to 9.
[ ] (square brackets)	Matches any digits in the brackets. For a range of numbers, use a dash. Example: [15-7]. In this example, the pattern matches 1, 5, 6, and 7.
. (period)	Acts as a wildcard that matches any digit and allows for any number of digits to be dialed. Example of a pattern matching rule: XX. In this example, the system looks for a dialed number match that has three or more digits.
! (exclamation point)	Acts as a wildcard that matches any digit (including no digits) and allows for any number of digits to be dialed. Example of a pattern matching rule: XX! In this example, the system looks for a dialed number match that has two or more digits.

Pattern-matching examples

Pattern	Description
X.	Matches any dialed number.
NXXXXXX	Matches any seven-digit number, as long as the first digit is 2 or higher.
NXXNXXXXXX	Matches any dialed number that has 10 digits.
1NXXNXXXXXX	Matches any dialed number that matches this pattern: 1 + area code (between 200 and 999) + seven-digit number (first digit is 2 or higher).
011.	Matches any number that starts with 011 and has at least one more digit.
XX!	Matches any two or more digits.

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 256 and Pattern-matching examples on page 257 for this dial plan. 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 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 about PBX schedule, see Scheduling the FortiVoice unit on page 158.
Action	Select the call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern. If you choose *Authorize*, select the *Account code*. For more information, see Configuring account codes on page 179.

GUI field	Description
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 about trunks, see Configuring trunks on page 229.
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 about caller ID modification, see Modifying caller IDs on page 140.
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 about sound files, see Managing phone audio settings on page 125.
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 242.

Setting up a call center

Access to the complete call center setup is available when you purchase a call center license and upload that license to the FortiVoice unit.

If the FortiVoice unit does not include a call center license but you want to create a call queue, go to *Call Feature > Call Queue*. For more details, go to Creating call queues and queue groups on page 310.

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 then operate the center using the user portal.

This topic includes:

- Creating call queues and queue groups on page 260
- Configuring agents on page 268
- Configuring IVR on page 269
- Configuring surveys on page 275
- Setting up monitor view on page 276
- Configuring other agent information on page 277
- Configuring agent profiles on page 280
- Working with call queue statistics on page 281
- Configuring call report profiles and generating reports on page 337

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 310
  - Configuring scheduled business hour queue call handling actions on page 313
  - Configuring non scheduled business hour queue call handling actions on page 314
  - Configuring exit key press queue call handling actions on page 314
- Creating queue groups on page 314

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 248.

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
Enabled	Select to activate this call queue.
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 FortiVoice options on page 116. 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.
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 about creating departments, see Creating extension departments on page 217.
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 *OverflowCall Handling* action you set in Queue Overflow on page 267. The maximum is 100.
Maximum queuing time	Enter the maximum call queue waiting time in minutes or seconds, or both. 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 267. The maximum is 720 minutes.

GUI field	Description
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 from 5 to 120 seconds.
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 125.
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 278. • 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 278.
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. • *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

GUI field	Description
	change the priority of a call on the agent console of the user portal. See Setting caller priorities on page 280.
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 125. *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 261 is added before the caller ID on the agent's phone. If you select *Replace*, the queue Display name on page 261 replaces the caller ID on the agent's phone. *Ring pattern*: Select a queue extension ring pattern.
Business schedule	Click in the field and select an operation schedule for the queue. For example, "business_hour" schedule means agents are only available to answer the calls for this queue during business hours. For information about scheduling, see Scheduling the FortiVoice unit on page 158.
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*. For example, if you select *Abbreviated* andenter 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 settings. If you select *Periodic* or *Random*, enter the announcement frequency in seconds in *Announcement interval*. Also, click in the field and select a greeting sound file for the announcement. For more information, see Managing phone audio settings on page 125. • *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 125.
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

GUI field	Description
	action triggered by the threshold being reached is configured in Call Handling on page 266. • *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 *QueueOverflow* call handling action you set in Service Level Low on page 267 when the call queue is full.
Alert	
Events	Select the event that triggers an action which is configured in Call Handling on page 266.
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 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 280. • *Alert interval:* Enter a value in minutes during which 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 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.
Prompt	Select a audio file to provide callers with callback information. If no file is selected, the default file is applied. You can also add a new audio file or edit an existing one. For more information, see Managing phone audio settings on page 125.
Interval	After selecting a audio file, set the time interval for playing the audio file.
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 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 call a caller back when he/she is within the next 3 calls in the queue. This happens when a caller does not wish to wait and leaves his/her number following the prompt. If the caller calls back before the FortiVoice callback occurs, the call will be treated as a new call in the queue which may result in a longer

GUI field	Description
	waiting time.
Prompt to caller to leave the call back number	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 about IVR, see Configuring IVR on page 269.
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 125.
Trunk and callback prefix table	FortiVoice can automatically add a prefix to the beginning of the callback number before placing an outside line call. To configure the callback prefix, complete the following steps: **1.** Click *New*. **2.** In *Trunk*, select, create, or edit a trunk to associate with the *Callback Prefix* setting. **3.** In *Callback Prefix*, enter a prefix that FortiVoice will add to the beginning of the callback number to allow the outside line call to be completed. **4.** Click *Create*.
Survey settings	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 about surveys, see Configuring surveys on page 275.
Call classifications	Enter custom call label names, such as external, or company A, to classify calls and enable call center agents to easily generate reports against those classifications. When an agent finishes a call, they receive a pop-up window where they can choose and apply the classification.
Agent	
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* as the agent 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* agent 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.

GUI field	Description
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 265 field.
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 210). 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	This option is only active when you edit a call queue. • Click *Agent Members* for enrolling agents into the queue. • Click in the field and select the agents for this queue. • Click *Close*, then *OK*. You can type an agent's extension or name in the *Search* field and press Enter to search for the agent. Note that a mobile softclient cannot be assigned to the call queue as an agent.
Call Handling	
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 266.
Non Scheduled Business Hour Call Handling	This option is only available when you edit a call queue. For details, see Configuring non scheduled business hour queue call handling actions on page 267.
Exit Key Press Call Handling	This option is only available when you edit a call queue. For details, see Configuring exit key press queue call handling actions on page 268.

3. Click *Create*.

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 261. 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 261. 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.
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 266.
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 266.
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 about schedules, see Scheduling the FortiVoice unit on page 158.
   - 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 about schedules, see Scheduling the FortiVoice unit on page 158.
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*.

Configuring exit key press queue call handling actions

Configure the call handling action for the queue to provide more options for callers to leave the voice queue. This action applies to all calls once they enter into the 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 *Exit Key PressCall Handling*.
4. On the *Call Processing* page, select a key number and click *New* to configure call handling action.
5. For *Schedule*, select the FortiVoice operation schedule to implement this call handling action. For more information about schedules, see Scheduling the FortiVoice unit on page 158.
6. For *Action*, select the call handling action. Depending on the action selected, further configuration may be needed. For example, if you select *Dialextension* 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 queue group

1. Go to *Call Center > Call Queue > Queue Group.*
2. Click *New*.
3. Enter a name for the group.
4. Click + and select the available call queues that you want to include in the group.
5. Click *Close*, then *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 be 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 183.)
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 280.
4. For *Managed departments*, click in the field and select the departments to be managed by this agent if required.
5. Click *Close*.
6. Click *Member of Queues* to select the call queues to join.
   - *Queues*: Click in the field and select the queues of which you want the extension/agent to be a member. Click *Close*.
   - *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 281. 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.
   - Click *OK*.
7. Add skill sets for the agent by clicking *New* under *Skill Sets*.
8. 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 278 and Creating agent skill levels on page 278.
9. 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 217.

Configuring IVR

The interactive voice response (IVR) function is available when you purchase a call center license and upload that license to the FortiVoice system.

With the FortiVoice interactive voice response (IVR) function, callers listen to audio instructions and make menu selections by pressing numbers on their phone keypad to reach agents or get the information they need.

Based on the information collected from callers and by interacting with the backend database, the FortiVoice IVR function can prioritize calls using call queues and present callers' information to agents.

FortiVoice IVR interfaces with the 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 269
- Configuring RESTful service on page 274

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 systems based on information gathered by digit and RESTful collectors (see To configure a SIP header collector on page 270).
- Digits collector to collect digit inputs from callers (see To configure a digit collector on page 271).
- RESTful collector to gather caller information from database (see To configure a RESTful collector on page 271).
- Call handling to route calls based on information gathered by digit and RESTful collectors (To configure IVR handling on page 273).
- Error handling to deal with unknown errors and RESTful service errors (To configure error handling on page 274).

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 system 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. • *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. • *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 about surveys, see Configuring surveys on page 275. 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, on the IVR configuration page, 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 125.
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 about surveys, see Configuring surveys on page 275.
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 from 1 to 30.
Max digits	Enter the maximum digits the digits collector allows. The range is from 1 to 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 from 0 to 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 from 0 to 60 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 from 0 to 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 afterward.

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, on the IVR configuration page, 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 274.
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 272, its URL displays here.
HTTP Headers	This option is only available if you select *Get* for *Method*. 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.
Posting HTTP Headers	This option is only available if you select *Post* for *Method*. 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.
Posting Message Body	This option is only available if you select *Post* for *Method*. 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.
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 from 0 to 10 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 from 0 to 10.
Description	Enter any notes you have for the RESTful collector.
Fields	Click *New* 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

GUI field	Description
	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 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 about surveys, see Configuring surveys on page 275.

2. Click *Create*, 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, on the IVR configuration page, 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, on the IVR configuration page, click *Add IVR Exception 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*, then *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 system 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.*
2. 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 about FortiVoice and Salesforce integration, see Integrating FortiVoice with Salesforce on page 355. • *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*.

GUI field	Description
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.

3. 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. Under *Questionnaire*, click *New*.
5. 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 125.
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 from 1 to 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 from 0 to 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 from 0 to 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 from 0 to 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.

6. Click *Create*.
   The survey is listed under *Questionnaire*. You may click *New* to add more.

7. If you want callers to comment on the survey, select *Caller Comment*.
8. 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 125.
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 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 when logging into the user 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 277.
Start time	Enter the time for the monitor view to start.
Queue	Click in the field and select the queues to be included. Click *Close,* then *Create.*
Logo	Select *Customized logo* to add text or logo for agents with privileges to view on the user portal. In the text editor window, you can type the text or copy and paste a logo image here. You can paste an image that is 32.7 KB or less.

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.
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*.

To change column order and hide or show columns for a monitor view

1. Go to *Call Center* > *Monitor View* > *Monitor*.
2. Under the *View* column of a monitor view record, click *Open*.
3. Click any of the column headings and do the following:
   a. Change the column order by dragging the column headings to the places you want.
   b. Click a heading, then *OK* to hide it. Click it again, then *OK* to show it. Click *Reset* to restore the default setting.

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.

This topic includes:

- Adding agent skill sets on page 278
- Creating agent skill levels on page 278
- Modifying agent reason code descriptions on page 278
- Configuring the data service on page 278
- Setting caller priorities on page 280

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 a *Name*.
4. Enter a *Code* number. The code number can be from 1 to 5 digits.
5. Enter a *Description*.
6. Click *Create*.

Configuring the 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.

Using a daily schedule as an example, the data service includes the following files:

- daily_<yyyy-mm-dd>_<24hourtime>_agent_information.csv
- daily_<yyyy-mm-dd>_<24hourtime>_cdr.csv
- daily_<yyyy-mm-dd>_<24hourtime>_fields_desc.csv

- daily_<yyyy-mm-dd>_<24hourtime>_queue.csv
- daily_<yyyy-mm-dd>_<24hourtime>_queue_activity.csv

The data service files are available in the following ways:

- By email: The data service sends the CSV files to your specified email address.
- Locally: With the *Local* setting enabled, you can download a .tar package.
- Remotely: With the *Remote* setting enabled and configured, you can find the CSV files in the following directory: <remote directory specified in the GUI>/<serial number of FortiVoice unit>/daily_<yyyy-mm-dd>_<24hourtime>_/

To edit the settings in *Call Center* > *Configuration* > *Data Service*, you require an account with an admin profile (*System* > *Administrator* > *Admin Profile*) that has the *Call center settings* with the read/write permission.

To configure the data service and back up the data on a schedule

1. Go to *Call Center* > *Configuration* > *Data Service*.
2. Select *Enabled* to activate the service.
3. To generate the data backup according to a schedule, configure the following settings:
   a. In *Schedule*, click *Daily*.
   b. In *Schedule hour*, select the hour(s) to start the data backup. Hours use the 24-hour time format.
   c. Click *Weekdays*.
   d. In *Schedule weekday*, select one or multiple days on which to generate the data backup.
4. In *Email*, enter the email address for sending the call center reports or statistics.
5. Configure the *Max backup number*. When the maximum number is reached, the oldest version will be overwritten.
6. If you want to back up the data locally, enable *Local*.
7. If you want to back up the data remotely, enable *Remote* and configure the following FTP/SFTP server options:

GUI field	Description
Remote host	Enter the domain name or IP address of the remote server.
Remote username	Enter the username associated with the account used to access the remote server.
Remote password	Enter the password associated with the account used to access the remote server.
Remote directory	Enter the directory where the files are saved on the remote server.
Remote protocol	Select *SFTP* or *FTP* as the protocol used to transfer files to the remote server.
Remote port	Enter the port used to transfer files to the remote server.
Retry Interval	Specifies the interval (in minutes) before FortiVoice attempts to reconnect and transfer files to the remote server after it has failed to either connect or successfully transfer files to the remote server.
Retry Attempts	Specifies the maximum number of times FortiVoice attempts to connect and transfer files to the remote server after it has failed to either connect or successfully transfer files to the remote server.
Test (button)	Click to test the connection and login to the remote server.

8. Click *Field Description* to view the FortiVoice data value number and description.
9. Click *Apply*.

To back up the data service on demand

1. Go to *Call Center* > *Configuration* > *Data Service*.
2. Select *Enabled* to activate the service.
3. Click the *Generate* button.
4. Select today's date or a past date.
5. Click *Generate*.
   FortiVoice displays a *Generation Successful* message.
6. Click *OK*.

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 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 about extensions, see Configuring IP extensions on page 183.

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.

GUI field	Description
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 call center console of the user portal. If you select *Caller prioritization*, the *Priority* button appears on the call center console of the user portal. If you select *Transfer call to another queue*, the *Transfer* button appears on the call center console of the user portal. For *Paused agent ring option*, if you want to ring agents in pause status, select *Ring Targeted*.
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 portal.
Manager Privilege	If the agent is a manager, select the privileges to manage the agents using the agent console of the user portal. The privileges include coaching, listening, and logging in and logging out agents, or pausing and resuming agents.
Monitoring Console Privilege	Select to enable monitoring console on the user 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.

GUI field	Description
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 dependent on your queue management configuration inCreating call queues and queue groups on page 260.
Out. Talk Time	The total time of outgoing calls made by the agent. This option is dependent on your queue management configuration in Creating call queues and queue groups on page 260.
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 261.
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 dependent on your queue management configuration in Creating call queues and queue groups on page 260.
Out. Talk Time	The total time of outgoing calls made by the agents in the queue. This option is dependent on your queue management configuration in Creating call queues and queue groups on page 260.

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 about scheduling the generation of reports, Configuring the report schedule on page 285.

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 Configuring report email notifications on page 339.
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 39.
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 about departments, see Creating extension departments on page 217.
5. Collapse each option and configure the following as needed:
   - Configuring the report query selection on page 283
   - Configuring the report time period on page 284
   - Configuring report email notifications on page 284
   - Configuring the report schedule on page 285
   - Generating a report manually on page 285
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*. If you select an option with an unspecified “N” value, enter the number of hours, days or weeks in the *Value* field, as applicable.

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 Configuring call report profiles and generating reports on page 337.

To configure an email notification

1. Go to *Call Center* > *Report* > *Report*.
2. Expand *Email*.
3. Enter the email address of the person who will receive the report notification in the *Recipients* field. Click + to enter more email addresses if necessary, or click x to remove an address.
4. In the *File format* field, select the format of the generated attachment, either *HTML, PDF, CSV ZIP,*or *CSV*.

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 285.

To configure the report schedule

1. Go to *Call Center* > *Report* > *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 285. • *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*.

Generating a report manually

You can always generate a report on demand whether the report profile includes a schedule or not.

To manually generate a report

1. Go to *Call Center* > *Report* > *Report*.
2. Click to select the report profile whose settings 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 39.

Working with a property management system

Businesses such as hotels use a 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 hotel management license and uploaded that license to the FortiVoice phone system.

This topic includes:

- Configuring hotel management settings on page 286
- Configuring hotel room status on page 291

Configuring hotel management settings

Hotel Management > *Setting* lets you configure the FortiVoice phone system to interoperate with your PMS, set the room condition codes, and configure guest check-in and check-out actions.

Complete the configuration of your PMS and then configure the hotel management settings on the FortiVoice phone system.

This section covers the PMS protocols, data synchronization, check-in and check-out options, and minibar codes:

- Configuring hotel management settings for the FortiVoice protocol on page 286
- Configuring hotel management settings for the Micros protocol on page 287
- Configuring hotel management settings for the Comtrol protocol on page 288
- Configuring hotel management settings for the Opera Cloud protocol on page 288
- Performing a manual data synchronization with the PMS on page 289
- Configuring check-in and check-out actions on page 290
- Configuring minibar codes for room maids to order room items on page 291

Configuring hotel management settings for the FortiVoice protocol

1. Go to *Hotel Management* > *Setting* > *PMS*.
2. Configure the following:

GUI field	Description
Enabled	Select to activate the communication with the PMS.

GUI field	Description
Protocol	Select *FortiVoice*. The FortiVoice phone system will use this protocol to communicate with the PMS.
Port	Enter the port number that connects to the PMS. Note that you need to use an adapter for the FortiVoice-PMS connection. From the port you configured, connect the PMS serial cable to the adapter and then connect the RJ45 cable from the FortiVoice phone system to the adapter.
Network Setting	Enter the IP address and netmask of the PMS. If the PMS uses serial connection to an adapter, enter the IP address and netmask of the adapter. If you have multiple PMSes, you may enter multiple trusted hosts.

3. Click *Apply*.

Configuring hotel management settings for the Micros protocol

1. Go to *Hotel Management* > *Setting* > *PMS*.
2. Configure the following:

GUI field	Description
Enabled	Select to activate the communication with the PMS.
Protocol	Select *Micros*. The FortiVoice phone system will use this protocol to communicate with the PMS.
Serial connection	Select to connect to the PMS using a serial cable.
LRC	Select to perform longitudinal redundancy check (LRC).
Mode	Choose to use the FortiVoice phone system as *Server* or *Client* when connecting to the PMS. If it is used as client, enter the server IP address in the *Server* field.
Port	Enter the port number that connects to the PMS. Note that you need to use an adapter for the FortiVoice-PMS connection. From the port you configured, connect the PMS serial cable to the adapter and then connect the RJ45 cable from the FortiVoice phone system to the adapter.
Call billing	Select to activate call billing.
Enable link establishment	If your PMS device needs the link establishment to exchange data with the FortiVoice phone system, select to activate this function.
Network Setting	Enter the IP address and netmask of the PMS. If the PMS uses serial connection to an adapter, enter the IP address and netmask of the adapter. If you have multiple PMSes, you may enter multiple trusted hosts.

3. Click *Apply*.
4. For details about *Data Sync*, see Performing a manual data synchronization with the PMS on page 289.

Configuring hotel management settings for the Comtrol protocol

1. Go to *Hotel Management* > *Setting* > *PMS*.
2. Configure the following:

GUI field	Description
Enabled	Select to activate the communication with the PMS.
Protocol	Select *Comtrol*. The FortiVoice phone system will use this protocol to communicate with the PMS.
Mode	Choose to use the FortiVoice phone system as *Server* or *Client* when connecting to the PMS. If it is used as client, enter the server IP address in the *Server* field.
Port	Enter the port number that connects to the PMS. Note that you need to use an adapter for the FortiVoice-PMS connection. From the port you configured, connect the PMS serial cable to the adapter and then connect the RJ45 cable from the FortiVoice phone system to the adapter.
Call billing	This option is only available for *Micros* and *Comtrol* protocols. Select to activate call billing.
Network Setting	Enter the IP address and netmask of the PMS. If the PMS uses serial connection to an adapter, enter the IP address and netmask of the adapter. If you have multiple PMSes, you may enter multiple trusted hosts.

3. Click *Apply*.
4. For details about *Data Sync*, see Performing a manual data synchronization with the PMS on page 289.

Configuring hotel management settings for the Opera Cloud protocol

The Oracle Hospitality Integration Platform (OHIP) uses the Opera Cloud protocol.

Prerequisites

Register an application in Opera Cloud using the Oracle Developer Portal and add an environment. This application acts as middleware to allow FortiVoice and the Opera Cloud server to communicate with each other. For more information about completing the following configurations, see the Oracle Hospitality Integration Platform User Guide:

- Register and manage an application
- Add an environment

To configure hotel management settings for the Opera Cloud protocol

1. Go to *Hotel Management* > *Setting* > *PMS*.
2. Configure the following:

GUI field	Description
Enabled	Select to activate the communication with the PMS.

GUI field	Description
Protocol	Select *Opera Cloud*.The FortiVoice phone system will use this protocol to communicate with the PMS.
URL	Enter the URL of the API gateway for the user acceptance testing (UAT) or production (PROD).
Client ID	Enter the client ID that you copied from the Opera Cloud Developer Portal for the UAT or PROD.
Client secret	Enter the client secret that you copied from the Opera Cloud Developer Portal for the UAT or PROD.
Interface ID	Enter the integration username that you copied from the UAT or PROD.
Interface key	Enter the integration password that you copied from the UAT or PROD.
Hotel ID	Enter the hotel ID on which you want to perform actions. For example, obtaining reservation data.
App key	Enter the application key that you copied from the Opera Cloud Developer Portal for the UAT or PROD.
Data Monitoring	
Periodic sync status	Select to activate the periodic data synchronization with the Opera Cloud PMS.
Data sync interval	Set a time interval in minutes to synchronize the data with the Opera Cloud PMS.

3. Click *Apply*.
4. For details about *Data Sync*, see Performing a manual data synchronization with the PMS on page 289.

Performing a manual data synchronization with the PMS

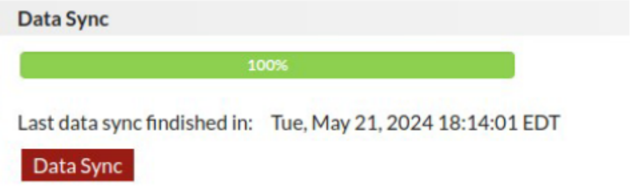
This function is available when the *Protocol* setting is Comtrol, Micros, or Opera Cloud.

1. Go to *Hotel Management* > *Setting* > *PMS*.
2. Review the following:

If you need to perform a manual data synchronization, Fortinet recommends that you perform this action at off-hours because all related operations, such as check-ins and check-outs, are suspended during a data synchronization.

Data Sync	To perform an on-demand data synchronization, click this button.

3. When the synchronization is complete, the section shows completion details, such as in the following example:



Data Sync

100%

Last data sync findished in: Tue, May 21, 2024 18:14:01 EDT

Configuring 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 about setting user privileges, see Configuring user privileges on page 151. • *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.
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 about setting user privileges, see Configuring user privileges on page 151. • *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 about the item code, see Configuring minibar codes for room maids to order room items on page 291.

3. Click *Apply*.

Configuring minibar codes 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 290.

Configuring hotel room status

Hotel Management > *Room Status* lets you set hotel room status.

When 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. Click *Close*.
3. 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 291.
4. 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 183.
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*.

GUI field	Description
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. To add a new room condition or edit a current one: **1.** Click + to add a new code. If the existing room conditions have reached the code range limit, click 🗑 to delete one first. If you want to modify an existing code, click ✎. **2.** In *Code*, enter a number for this room condition. **3.** In *Description*, enter a code description.

The following table summarizes the code range and default room conditions for each protocol:

Protocol	FortiVoice	Micros	Comtrol	Opera Cloud
Code range	1 to 9	1 to 99	1 to 10	1 to 6
Room condition	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	1: Dirty/Vacant 2: Dirty/Occupied 3: Clean/Vacant 4: Clean/Occupied 5: Inspected/Vacant 6: Inspected/Occupied	1: Room Cleaned 2: Cleaning Requested 3: Cleaning In-Progress 4: Inspection Requested 5: Maintenance Requested 6: Out of Order 7: Pick Up 8: Passed Inspection 9: Failed Inspection 10: Cleaning Skipped	1: Clean 2: Dirty 3: Pickup 4: Inspected 5: Out of Order 6: Out of Service

GUI field	Description
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 about setting user privileges, see Configuring user privileges on page 151. 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 the phone auto dialer

With the auto dialer function, the FortiVoice unit can be configured to automatically dial telephone numbers. After the call is answered, the FortiVoice unit plays a recorded message.

This topic includes:

- Setting up an auto dialer campaign on page 293
- Creating a recorded broadcast message on page 294
- Adding contacts and contact groups on page 294
- Configuring auto dialer settings on page 296
- Viewing auto dialer reports on page 296

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 294.
Retry	Enter the number of times you want to retry calling.
Description	Enter any notes you have for this campaign.
External Numbers	Prior to selecting external numbers, add these numbers by going to *Auto Dialer > Contact > Contact/Contact Group.* See Adding contacts and contact groups on page 294. Click in the field and select the external phone numbers you want to autodial. You can select up to 600 external numbers. Click *Close*.
Internal Numbers	Click in the field and select the internal phone numbers you want to autodial. Click *Close*. 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 *Create*.

Creating a recorded broadcast message

Auto Dialer > *Campaign* > *Audio* allows you to create a sound file for the auto dialer to broadcast.

Before you begin

If you want to upload a sound file, make sure that the file meets the following requirements:

- WAVE file (.wav) in PCM format or an MP3 file
- Maximum size of 10 MB

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.
   - *Record*: Click to enter a phone number and click *Send*. When the phone rings, pick up the receiver, and record your message.
   - *Play*: After a file is uploaded or recorded, click to play it.
   - *Download*: After a file is uploaded or recorded, click to download it.
5. Click *Create*.

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 import multiple auto dialer contacts using a CSV file or vCard, the Auto Dialer Read+Write permission must be enabled in your admin profile. For more information, see Configuring administrator profiles on page 58.

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. Click in the field and select the contacts for the group.
   Members are created by adding contacts.
5. Click *Close*.
6. Click *Create*.

Importing auto dialer contacts

The import feature provides a simple way to add a list of new auto dialer contacts in one operation using a CSV or vCard file.

To import multiple auto dialer contacts using a CSV file or vCard, the Auto Dialer Read+Write permission must be enabled in your admin profile. For more information, see Configuring administrator profiles on page 58.

1. Go to *Auto Dialer* > *Contact* > *Contact*.
2. Click *Import* > *CSV* or *vCard*.
3. Locate and select the file.
4. Click *Open*.

   The file imports.
5. Review the following options:

GUI option	Description
First line of CSV file contains contact	Enable this option if the file includes a contact in the first line instead another information type such as a header. If this option is disabled, FortiVoice ignores the first line of the CSV file.
Mapping content	Map each *Contact Field* used by FortiVoice to a *CSV Attribute* which is the content in your CSV file. Click + to add a row.

6. Click *OK*.

   FortiVoice displays the results of the import.

Configuring auto dialer settings

Auto Dialer > *Setting* allows you to set the maximum of 64 call channels for campaigns. The default is 10. 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 settings for many call features such as conference call, auto attendant, faxing, and much more.

This topic includes:

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 attendant limits on FVE models

Model	Number of auto attendants supported
FVE-100F and FVE-VM-100	10
FVE-200F8 and FVE-VM-200	20
FVE-300E-T	30
FVE-500F and FVE-VM-500	50
FVE-VM-1000	100
FVE-2000F, and FVE-VM-2000	200
FVE-VM-3000	300
FVE-5000F and FVE-VM-5000	500
FVE-VM-10000	1000
FVE-VM-50000	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 FortiVoice location, contact, and emergency information on page 114. You can also select other languages. The language files are created in Managing phone audio settings on page 125.
Greeting mode	If you select *Simple*, select a greeting message (sound file) for the auto attendant. See Greeting on page 298. 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 158. • 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 125. • 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 125. 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. • *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 183. • *Go to Voicemail*: The call is transferred to a voicemail box. Select the voicemail extension.

GUI field	Description
	• *Ring Group*: The call is transferred to a ring group. Select the ring group. For more information, see Creating ring groups on page 218. • *Call Queue*: The call is transferred to a call queue. Select the queue. For more information, see Creating call queues on page 261. • *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 300.
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 324.
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 120.
All recording of prompt sound file	Select to enable an external caller to dial into the FortiVoice unit and record a 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 about DISA code, see Modifying feature access codes on page 324. For more information about an account code, see Configuring account codes on page 179.
Outbound dialplans allowed for access	Click in the field and select the outbound dial plan for users to call the FortiVoice unit and use it to make outbound calls. Click *Close*. For details, see Configuring outbound dial plans on page 254.
Business group	This option is available on FVE-500F and larger models only. 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 224.
Department	This option is unavailable on the FVE-20E2 and FVE-50E6 models.

GUI field	Description
	Select or add a department to allow a caller to access the phone directory categorized by department. Make sure to also enable the *Include subdirectory* setting in Configuring system capacity on page 120.
Survival branch	This option is available on FVE-300E-T, FVE-VM-500, and larger models. Select or add a survival branch to allow a caller to access phone directory entries that belong to a FortiVoice survivability branch. Make sure to also enable the *Include subdirectory* setting in Configuring system capacity on page 120.

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 299.

To configure a key action

1. While configuring an auto attendant, click *New* under *Dial Pad Key Action*.
2. For *Key*, 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 that includes details such as directions, business hours. • 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 about sound files, see Managing phone audio settings on page 125. • 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.
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 183.
Go to Voicemail	The call is transferred to voicemail, allowing the caller to leave a message. Select an extension. 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 183.
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.

GUI field	Description
	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 217.
Dial Number	The call is transferred to a specified remote extension number. Enter the remote extension number. For more information, see Configuring remote extensions on page 204.
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 260.
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. Select the *Directory*. For details about the directory and subdirectory selection, see the Directory section in Configuring system capacity on page 120.
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 FortiVoice location, contact, and emergency information on page 114. You can also select other languages. The language files are created in Managing phone audio settings on page 125.
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 about creating auto attendants, see Configuring auto attendants on page 297.
Start Over	The auto attendant will repeat the announcement.
Hang Up	The call is terminated.
IVR	The IVR action is visible when you purchase a call center license and upload that license to the FortiVoice unit. Route the call to the FortiVoice IVR system. For more information, see Configuring IVR on page 269.

5. For *Music on hold*, select the voice prompt to be used for this key action. See Managing phone audio settings on page 125.
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 302.
5. For *Mapped Number*, enter the phone number to map to the speed dial code.
   You can enter digits 0 to 9, space, dash, comma, # and *.

   The speed dial pattern accepts # as the lead digit (for example, #XX or #613XXX).

   If you want to enter an auto attendant number followed by an extension, you can use a comma (,) or semicolon (;) to pause the automatic dialing.
   A comma pauses the dialing for two seconds, for example, 1-123-222-1234, 5678#. In this case, after pressing the speed dial code you set, the auto attendant 1-123-1234 is reached, and after two seconds, extension 5678 is automatically dialed.
   A semicolon pauses the dialing for one second, for example, 1-123-222-1234; 5678#. In this case, after pressing the speed dial code you set, the 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 about setting speed dial number pattern, see Configuring FortiVoice options on page 116.
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 settings.

FortiVoice allows two types of conferencing:

- **User conferencing**: You can configure and enable a user conference call privilege for extension users to hold their own conference calls on the user portal. For details about adding a conference call event, see the FortiVoice User Portal Guide.
- **Admin conferencing**: The administrator can set up static or dynamic conference calls for the users using the FortiVoice GUI. Static conference calls are configured directly on the GUI whereas dynamic conference calls are configured using the calendar.

Conference call options

Conference call organizers and attendees can access features such as mute and volume controls.

To access the conference call menu, organizers and attendees press the asterisk (*) and then an available menu option:

Menu option	Organizer	Attendee	Action
0	Yes	No	Mute all members except yourself.
1	Yes	Yes	Mute or unmute yourself.
2	Yes	No	Lock or unlock the conference.
3	Yes	No	Reject the last user.
4	Yes	Yes	Decrease your outbound volume.
6	Yes	Yes	Increase your outbound volume.
7	Yes	Yes	Decrease your inbound volume.
8	Yes	Yes	Exit the menu.
9	Yes	Yes	Increase your inbound volume.

This section includes the following topics:

- To configure user conferencing on page 303
- To set up a static conference call on page 304
- To configure a dynamic conference call on page 305

To configure user conferencing

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	Click the *Edit* icon and 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 about creating music on hold file, see Managing phone audio settings on page 125.
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 (from 3 to 10 digits) that users need to organize

GUI field	Description
	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
Enabled	Select to activate this conference call.
Mode	Select *Static*.
Name	Enter a conference call name.
Number	Enter a number that callers can dial to join a conference call.
Setting	
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 about creating music on hold file, see Managing phone audio settings on page 125.
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 about setting up a schedule, see Scheduling the FortiVoice unit on page 158.
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*.

GUI field	Description
	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
Enabled	Select to activate this conference call.
Mode	Select *Dynamic*.
Name	Enter a conference call name.
Number	Enter the number that callers can dial 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 about creating music on hold file, see Managing phone audio settings on page 125.
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. Click *View Scheduled Conferences* and 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 306
- Archiving recorded calls on page 308

- Setting the file format for recorded calls on page 309
- Configuring the recorder warning tone on page 309

For more information, see the Call recording section in the FortiVoice Cookbook.

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. For details, see Playing and downloading recorded calls on page 44.
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
Enabled	Select to activate this configuration.
Name	Enter a name for 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 FortiVoice options on page 116. 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 FortiVoice options on page 116. 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 217.
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 217.
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 229.
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 260.
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 percentage of calls that you want to record. This value is a rolling percentage. In the following example scenario, FortiVoice records 50% of calls: **1.** Set the record ratio to 50. **2.** With a system that has no recorded calls, you are at 0% of recorded calls. The system records the first call. With the first call recorded, the record ratio is now at 100%. **3.** To reach the 50% record ratio, the system will not record the second call. **4.** With the record ratio at 50%, the system does not record the third call and the record ratio drops below 50%. **5.** With the record ratio below 50%, the system records the fourth call to achieve the 50% ratio again. **6.** To summarize this example scenario, the system has received four calls and recorded two calls to achieve the recorded ratio of 50%. The following settings can have an effect on the recorded call storage: • Retention duration on page 307 • Archiving recorded calls on page 308 • Setting the file format for recorded calls on page 309
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 in *Monitor > Storage*. See Playing recorded calls and viewing fax storage on page 44.

3. Click *Create*.

Archiving recorded calls

Configure the settings to archive the recorded calls.

To configure the recording archive settings

1. Go to *Call Feature* > *Call Recording* > *Archive.*
2. Configure the following:

GUI field	Description
Rotation Setting	
Recording rotation size Recording rotation 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 in Rotation Setting on page 308. To view logs for the deletion of local call recordings, go to *Monitor* > *Log* > *System* (see Viewing log messages on page 40).
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`.

GUI field	Description
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. 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 308.
Schedule	Select a schedule for the archiving. Click *Edit* to modify the selected schedule or click *New* to configure a new one.

3. Click *Apply*.

Setting the file format for recorded calls

Select the file format for recorded calls. FortiVoice has the following two levels of recording quality and associated kilobit per minute (kbit/m) of recorded call:

- Standard, pulse code modulation (PCM) which equals to 950 kbit/m of a recorded call.
- Low rate, global system for mobile communications (GSM), which equals to 95 kbit/m of a recorded call.

To set the file format for recorded calls

1. Go to *Call Feature* > *Call Recording* > *Setting*.

> To play a call recording that is using the low rate (GSM) setting, you must download that recording first and then play it. You cannot play that recording in the web browser directly. For information about playing a recorded call, see Viewing call detail records on page 38.

2. Under *Recording Bitrate Setting*, select: *Standard, PCM, 128Kbps* or *Low Rate, GSM, 6.10, 13Kbps*.
3. Click *Apply*.

Configuring the recorder warning tone

FortiVoice can transmit a recorder warning tone to indicate to the called party that the calling party is recording the phone conversation.

The recorder warning tone is disabled by default.

To configure the recorder warning tone

1. Go to *Call Feature* > *Call Recording* > *Setting*.
2. Under *Start Warning Tone*, select *Periodic Monitor Enabled*.
3. In *Periodic Monitor Interval*, enter a new interval (in seconds) or keep the default. For example, if you set the interval to 20, FortiVoice will send a warning tone every 20 seconds. FortiVoice records the conversation and the warning tone.
4. Click *Apply*.

Creating call queues and queue groups

This option is only available if you have *not* purchased and installed the call center license.

If you have purchased and installed the call center license, then the call queue related menus are visible under *Call Center* > *Call Queue* instead. For more details, see Setting up a call center on page 260.

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 310
- Creating queue groups on page 314

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 248.

Call queues consist of:

- Incoming calls waiting in the queue
- Agents who answer the calls in the queue
- 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 Feature* > *Call Queue* > *Call Queue.*
2. Click *New* and configure the following:

GUI field	Description
Enabled	Select to activate this call queue.
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 FortiVoice options on page 116.

GUI field	Description
	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.
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 about creating departments, see Creating extension departments on page 217.
Queue Setting	
Distribution policy	• *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. • *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 portal. See Setting caller priorities on page 280.
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 *OverflowCall Handling* action you set in Queue Overflow on page 313. The maximum is 100.
Maximum queuing time	Enter the maximum call queue waiting time in minutes or seconds, or both. 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 313. 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 from 5 to 120 seconds.
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 125.
Additional Setting	

GUI field	Description
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 125. *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 311 is added before the caller ID on the agent's phone. If you select *Replace*, the queue Display name on page 311 replaces the caller ID on the agent's phone. *Ring pattern*: Select a queue extension ring pattern.
Business Schedule	Click in the field and select an operation schedule for the queue. For example, "business_hour" schedule means agents are only available to answer the calls for this queue during business hours. For information about scheduling, see Scheduling the FortiVoice unit on page 158.
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*. 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 settings. If you select *Periodic* or *Random*, enter the announcement frequency in seconds in *Announcement interval*. Also, click in the field and select a greeting sound file for the announcement. For more information, see Managing phone audio settings on page 125. • *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 125.
Agent	
Agent Members	This option is only active when you edit a call queue. • Click *Agent Members* for enrolling agents into the queue. • Click in the field and select the agents for this queue. • Click *Close*, then *OK*.

GUI field	Description
	You can type an agent's extension or name in the *Search* field and press Enter to search for the agent. Note that a mobile softclient cannot be assigned to the call queue as an agent.
Call Handling	
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 313.
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 313.
Exit Key Press Call Handling	This option is only available when you edit a call queue. For details, see Configuring exit key press queue call handling actions on page 314.

3. Click *Create*.

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 Feature* > *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 queuing time on page 261. 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 261. A popup notification appears when this barometer is triggered.

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 about schedules, see Scheduling the FortiVoice unit on page 158.
   - Select the call handling action. Depending on the action selected, further configuration may be needed. For example, if you select *Dialextension* 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 for non scheduled business hour

1. Go to *Call Feature* > *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 *NonScheduled 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 about schedules, see Scheduling the FortiVoice unit on page 158.
6. For *Action*, select the call handling action. Depending on the action selected, further configuration may be needed. For example, if you select *Dialextension* for *Action*, enter the extension to which a call is transferred.
7. Click *Create*, then *OK*.

Configuring exit key press queue call handling actions

Configure the call handling action for the queue to provide more options for callers to leave the voice queue. This action applies to all calls once they enter into the queue.

To configure the call handling action for exit key press

1. Go to *Call Feature* > *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 *Exit Key PressCall Handling*.
4. On the *Call Processing* page, select a key number and click *New* to configure call handling action.
5. For *Schedule*, select the FortiVoice operation schedule to implement this call handling action. For more information about schedules, see Scheduling the FortiVoice unit on page 158.
6. For *Action*, select the call handling action. Depending on the action selected, further configuration may be needed. For example, if you select *Dialextension* 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 Feature* > *Call Queue* > *Queue Group.*
2. Click *New*.
3. Enter a name for the group.
4. Click in the field and select the available call queues that you want to include in the group.
5. Click *Close*, then *Create*.

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 to 320.

To view the parked calls, see Viewing parked calls on page 31.

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 which has the same effect as the call park feature code *40. See Mid-Call/DTMF codes on page 330.
   For example, when a user receives a call and wants to park it, the user may:
   - Press 300.
     The FortiVoice unit selects the first available park orbit (301 to 320). The user hears a confirmation indicating the caller has been parked successfully and into which park orbit.
   - Provide the park orbit to the person with the parked call through paging or other means. For example, “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 timeout*, 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 about music on hold, see Managing phone audio settings on page 125.
7. Click *Apply*.

Configuring fax

The FortiVoice unit supports fax in the following ways:

- Replace your organization's physical fax machine by using 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 portal or a user’s email. End users can log into their FortiVoice user portal to view the faxes and upload PDF or JPEG files to send faxes. For configuration information, see Receiving faxes on page 316 and Sending faxes on page 317.
- 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 (see Configuring fax extensions on page 207). You then need to configure the FortiVoice unit to receive and relay faxes to the fax machine (see Receiving faxes on page 316 and Sending faxes on page 317).

This topic includes:

- Receiving faxes on page 316
- Sending faxes on page 317

- Archiving faxes on page 321
- Configuring other fax settings on page 322

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

1. Go to *Call Feature* > *Fax* > *eFax Account*.
2. Click *New.*
3. Configure the following:

GUI field	Description
Incoming Fax Setting	
Enabled	Select to activate this fax.
Name	Enter a name for the receiving fax configuration.
Number	Enter an extension for this fax. This is where the incoming faxes go to.
Display name	Enter the name displaying on the extension.
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 reach the extension. To map the DID numbers: **1.** Click *New*. **2.** Select *Enabled* to activate this DID mapping. **3.** Select the *Incoming trunk* used for dialing the DIDs. **4.** Enter the *DID number* that you want to map to the extension of the fax. **5.** Click *Create*.
Select Fax Monitors	Click in the field and select the users that can monitor the faxes received on this fax extension in their FortiVoice user portal and can choose to view, delete, resend, forward, or download the faxes. Click *Close*. 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 210. 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 119.
Relay to Fax Machine	Click in the field and select the fax machines connected to the FortiVoice unit via T.38 adapters. Faxes will be relayed to the selected machines.

GUI field	Description
	Click *Close*.
Archive	Select *Fax archive* to activate fax archiving and enter the file name to archive following the formats in the dropdown list. To view faxes sent and received through the FortiVoice unit, see Viewing archived faxes on page 45.

4. 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 about dial plans, see Configuring call routing on page 248.

You send faxes in the user 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 210.

In addition, senders can always view the status of the fax sent in their FortiVoice user portal. For more information, see the online help of the 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 318.
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 318.
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 318.

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
Enabled	Select to activate this dial plan.
Name	Enter a name for 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 about adding a dialed number match, see Creating dialed number match on page 319.
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 320.

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 317.

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.

GUI field	Description
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.
[ ] (square brackets)	Matches any digits in the brackets. For a range of numbers, use a dash. Example: [15-7]. In this example, the pattern matches 1, 5, 6, and 7.
. (period)	Acts as a wildcard that matches any digit and allows for any number of digits to be dialed. Example of a pattern matching rule: XX. In this example, the system looks for a dialed number match that has three or more digits.
! (exclamation point)	Acts as a wildcard that matches any digit (including no digits) and allows for any number of digits to be dialed. Example of a pattern matching rule: XX! In this example, the system looks for a dialed number match that has two or more digits.

Pattern-matching examples

Pattern	Description
X.	Matches any dialed number.
NXXXXXX	Matches any seven-digit number, as long as the first digit is 2 or higher.
NXXNXXXXXX	Matches any dialed number that has 10 digits.
1NXXNXXXXXX	Matches any dialed number that matches this pattern: 1 + area code (between 200 and 999) + seven-digit number (first digit is 2 or higher).
011.	Matches any number that starts with 011 and has at least one more digit.
XX!	Matches any two or more digits.

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 319 and Pattern-matching examples on page 319). 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 about PBX schedule, see Scheduling the FortiVoice unit on page 158.
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 about trunks, see Configuring trunks on page 229.
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 about caller ID modification, see Modifying caller IDs on page 140.
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 about sound files, see Managing phone audio settings on page 125.
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 Fax rotation 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.
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. Click *Edit* to modify the selected schedule or click *New* to configure a new one.
Destination Setting	
Destination	Select an archiving destination:

GUI field	Description
	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 308.
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.
Maximum Transmission Rate	Select the fastest fax transfer speed.
Minimum Transmission Rate	Select the slowest fax transfer speed.
Enable T.30 ECM (error correction mode)	Enable to monitor the entire fax process from the initial dialing to disconnecting.

GUI field	Description
	By enabling this option, if any issues occur in the process, the receiving fax system will request the sending fax system to resend part or all of the fax information. This may make the transmission time longer. If it cannot fix the issue detected, it will fail the fax.
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 reminders

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*.
2. Click *New*.
3. Enable the reminder and add notes if required.
4. Enter a *Name* for the reminder.
5. In *Description*, add notes, if required.
6. Click *Create*.
7. In the reminder list, select the reminder record you just created.
8. Click *Edit in calendar mode*.
9. Click a date that you want to apply to the reminder.
10. 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. The start time uses the time zone setting available in *System* > *Configuration* > *Time*.
Recurrence	If you want the reminder event to be on a repeating schedule, click *None*, update the settings, and click *OK*.
Description	Enter any notes as required.
Guest	To add internal phone numbers, click +, select extensions, and click *Close*. To add an external phone number, enter a phone number in *External*, and click ⇥. The number is added to the Guest list.
Reminder audio	To send a reminder audio to the selected guest phones, select one of the following options: • *Default*: Select to send a beep sound as the reminder audio. To hear the beep sound, click *Play*, and save the GSM file. • *Customized*: Select to customize the reminder audio. **a.** Click *Create New*. **b.** You have two options to create a customized message: • To record a message, select an extension and click *Call me*. You can then follow the prompts to create a new message. • To upload a message that you have already recorded: • Make sure that the file is a WAVE file (WAV) in PCM format or MP3 file and with a maximum size of 10 MB. • Click *Upload*. • Select the file and click *Open*. **c.** Click *Close*.

11. Click *Create*, then *Close*.

Modifying feature access codes

By default, the FortiVoice system 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.

FortiVoice supports the following feature access codes:

- Vertical service codes: Are a sequence of digits, star (*), and number sign (#) that a user dials on a telephone keypad to enable or disable certain telephony service features. See Vertical service codes on page 325.
- Mid-Call/DTMF codes: Allow a user to hold, transfer, and conference calls by using DTMF digit codes entered on the phone. See Mid-Call/DTMF codes on page 330.
- Floating codes: Allow you to limit international, long distance, or local calls. See Floating code format on page 331.

Vertical service codes

To access the list of codes, go to *Call Feature* > *Feature Code* > *Vertical Service Code*.

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 'not assigned' 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 system and enter the phone configuration PIN. For information about setting the phone configuration PIN, see Configuring auto-provisioning for FortiFone phones and gateways on page 99.
Reset the phone to be 'not assigned' 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 system and enter the phone configuration PIN. For information about setting the phone configuration PIN, see Configuring auto-provisioning for FortiFone phones and gateways on page 99.
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 system and enter the phone configuration PIN. You can then enter an existing extension to set it as the extension of this phone. For information about setting the phone configuration PIN, see Configuring auto-provisioning for FortiFone phones and gateways on page 99.

GUI field	Description
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 system 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.
Listen/Barge on a call	To join an active phone call for listening and providing assistance, complete the following steps: **1.** Dial *50 or the code you set. **2.** Enter your voicemail PIN and press #. **3.** Enter the extension number that you want to join and monitor, and press #. For details about configuring a user privilege that allows call barging, see Monitor/Recording on page 154.
Agent login to all queues	Dial *61 or the code you set to log into the queues, which your extension is a member.
Agent logout from all queues	Dial *62 or the code you set to log out of the queues, 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.
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.
Login all queue members	Dial *65 or the code you set to login all members of a queue, which your extension is a member. The administrator can perform this action.
Logout all queue members	Dial *66 or the code you set to logout all members of a queue, which your extension is a member. The administrator can perform this action.
Pause agent in all queues	Dial *67 or the code you set and the reason code to pause all queues, which this extension is a member. For information about reason codes, see Modifying agent reason code descriptions on page 278.
Unpause agent from all queues	Dial *68 or the code you set and the reason code to unpause all queues, which this extension is a member. For information about reason codes, see Modifying agent reason code descriptions on page 278.
Pause agent in one queue	To pause an agent from a queue, which this extension is a member, complete the following steps: **1.** Dial *69 or the code you set. **2.** Enter the reason code.

GUI field	Description
	3. Enter the queue number. For information about reason codes, see Modifying agent reason code descriptions on page 278.
Unpause agent in one queue	To unpause an agent from a queue, which this extension is a member, dial *70 or the code you set and enter the queue number. For information about reason codes, see Modifying agent reason code descriptions on page 278.
Set call forward	To set call forward, complete the following steps: **1.** Dial *71. **2.** If you are prompted, enter your voicemail PIN and press #. **3.** Enter the number that you want your calls to be forwarded to. To deactivate the call forward, complete the following steps: **1.** Dial *710. **2.** If you are prompted, enter your voicemail PIN and press #. To change the call forwarding number, complete the following steps: **1.** Dial *719. **2.** If you are prompted, enter your voicemail PIN and press #. **3.** Enter the new number to forward your calls to.
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 about twinning, see Configuring IP extensions on page 183.
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 331.
Hotel room condition	Dial *75 or the code you set and enter a maid code to show the room condition. For information about maid codes, see Configuring hotel management settings on page 286.
The default maid codes vary depending on the PMS protocol selected:	

<table>
<tr><th>GUI field</th><th>Description</th></tr>
<tr><td colspan="2">
<table>
<tr><td><b>Protocol</b></td><td>FortiVoice</td><td>Micros</td><td>Comtrol</td><td>Opera Cloud</td></tr>
<tr><td><b>Code range</b></td><td>1 to 9</td><td>1 to 99</td><td>1 to 10</td><td>1 to 6</td></tr>
<tr><td><b>Room condition</b></td><td>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</td><td>1: Dirty/Vacant
2: Dirty/Occupied
3: Clean/Vacant
4: Clean/Occupied
5: Inspected/Vacant
6: Inspected/Occupied</td><td>1: Room Cleaned
2: Cleaning Requested
3: Cleaning In-Progress
4: Inspection Requested
5: Maintenance Requested
6: Out of Order
7: Pick Up
8: Passed Inspection
9: Failed Inspection
10: Cleaning Skipped</td><td>1: Clean
2: Dirty
3: Pickup
4: Inspected
5: Out of Order
5: Out of Order</td></tr>
</table>
</td></tr>
<tr><td>Minibar notification</td><td>Dial *76 or the code you set and enter a minibar code to order room items.
For information about minibar codes, see Configuring hotel management settings on page 286.</td></tr>
<tr><td>Wake-up call</td><td>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.</td></tr>
<tr><td>DND on</td><td>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.</td></tr>
<tr><td>DND off</td><td>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.</td></tr>
<tr><td>Pickup any ringing extension in pickup group</td><td>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 about pickup groups, see Creating pickup groups on page 223.</td></tr>
<tr><td>Pickup group extension</td><td>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 about pickup groups, see Creating pickup groups on page 223.</td></tr>
</table>

GUI field	Description
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 level phone schedule profile with one of the three default ones. Dial *820 to go back to the original schedule. The phone system schedule profiles are used when configuring dial plans, virtual numbers, or auto attendant. For information about the phone system schedule profile, see Scheduling the FortiVoice unit on page 158.
Intercom	Dial *92 or the code you set and enter an extension to intercom that extension.
Prompt sound file recording	You can record a prompt sound file. Complete the following steps. Take note of the File ID: **1.** If you have an existing sound file entry in *Phone System* > *Audio* > *Prompt*, access it and take note of the File ID. **2.** If you need to create a new sound file entry: **a.** Go to *Phone System* > *Audio* > *Prompt*. **b.** Click *New*. **c.** Enter a *File name*. **d.** Make sure to assign a *File ID*. **e.** Take note of this *File ID*. You will need the information when you record the prompt sound file. **f.** Complete the configuration. For more information, see Uploading or recording sound files on page 125. **g.** Click *Create*. Record a prompt sound file: **1.** Dial the following: *93<File ID>*<language code> where: • *93 is the feature code or the one you set. • <File ID> identifies the prompt sound file. • * is the command to enter a language code.

<table>
<tr><th>GUI field</th><th>Description</th></tr>
<tr><td></td><td>

- <language code> is the code associated with the language to record the prompt. The available language codes are:

<table>
<tr><td>Code</td><td>Language</td></tr>
<tr><td>1</td><td>English</td></tr>
<tr><td>2</td><td>French</td></tr>
<tr><td>3</td><td>Spanish</td></tr>
<tr><td>4</td><td>Polish</td></tr>
<tr><td>5</td><td>Chinese</td></tr>
<tr><td>6</td><td>Italian</td></tr>
<tr><td>7</td><td>Portuguese (Brazil)</td></tr>
<tr><td>8</td><td>Portuguese (Portugal)</td></tr>
</table>

Here is an example for creating a new French prompt for the sound file 4185:

*934185*2

2. When FortiVoice prompts you for a PIN, enter 326326 or the code that you have set in *Phone System > Setting > Miscellaneous, Administrator PIN*.
3. Follow the prompts to complete your recording.
FortiVoice allows you to download or play your recording in *Phone System > Audio > Prompt*.

</td></tr>
<tr><td>Voicemail direct</td><td>Dial *97 (or the code you set) from your own phone and then enter your voicemail password to directly access your voicemail.
If the voicemail password option is disabled (see Configuring user privileges on page 151), users can access their voicemail without a password.</td></tr>
<tr><td>Voicemail prompt</td><td>Dial *98 (or the code you set) from any extension and then enter your extension number and voicemail password to access your voicemail.
If the voicemail password option is disabled (see Configuring user privileges on page 151), users can access their voicemail without a password.</td></tr>
<tr><td>Operator</td><td>Dial 0 or the code you set to access the operator.</td></tr>
</table>

Mid-Call/DTMF codes

To access the list of codes, go to *Call Feature > Feature Code > Mid-Call/DTMF Code*.

GUI field	Description
Blind transfer	Blind transfer serves two 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 315.
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 FortiVoice user portal. For more information, see the Call recording section in the FortiVoice Cookbook. Before recording a phone call, the user must have the agreement of the person on the call or check the local laws regarding phone recording.
Cancel personal recording	Dial *31 or the code you set to cancel personal call 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 FortiVoice GUI. For more information, see the Call recording section in the FortiVoice Cookbook. Before recording a phone call, the user must have the agreement of the person on the call or check the 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
Allowed	*74 + extension number + * + voicemail PIN (*Phone System* > *Setting* > *Option* > *Default Setting* > *Default Voicemail PIN*) **or** 74* + extension number + * + extension personal code (*Extension* > *IP Extension* > *User Setting* > *Phone Access* > *Personal Code*)
Allow with personal code	*74 + extension number + * + voicemail PIN (*Phone System* > *Setting* > *Option* > *Default Setting* > *Default Voicemail PIN*)
Allow with account code	*74 + extension number + * + user privilege account code (*Security* > *User Privilege* > *Account Code*)
Allow with account and personal code	*74 + extension number + * + user privilege account code *Security* > *User Privilege* > *Account Code*) **or** *74 + extension number + * + voicemail PIN (*Phone System* > *Setting* > *Option* > *Default Setting* > *Default Voicemail PIN*)

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 on page 332
- Configuring logging on page 334
- Configuring call report profiles and generating reports on page 337
- Submitting CDRs to a database on page 340
- Configuring SMDR on page 342
- Configuring alert email on page 344

About FortiVoice logging

FortiVoice units can log multiple events. See FortiVoice log types on page 332.

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 333.

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 334. 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 282.

This topic includes:

- FortiVoice log types on page 332
- Log message severity levels on page 333

FortiVoice log types

FortiVoice units can record the following types of log messages. The Event log also contains several subtypes. You can view these logs from *Monitor > Log*.

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 system 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 about severity levels, see Log message severity levels on page 333.

For information about viewing locally stored log messages, see Viewing log messages on page 40.

This section includes the following topics:

- Configuring logging to the hard disk on page 334
- Choosing which events to log on page 335
- Configuring logging to a Syslog server or FortiAnalyzer unit on page 336

Configuring logging to the hard disk

You can store log messages locally on the hard disk of the FortiVoice system.

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 system. (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 40.

For logging accuracy, you should also verify that the FortiVoice system time is accurate. For details, see Configuring the time and date on page 81.

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 system 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 system 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*, enable the types of logs that you want to record to this storage location. For details, see Choosing which events to log on page 335.
9. *SIP Registration Log* tracks the registration status of extensions. You can configure the following settings:
   a. *SIP Registration Log Status*: Enable or disable this log function.
   b. *Incoming SIP register retention*: Enter the number of days that you want FortiVoice to retain the logs.
10. Click *Apply*.
11. To display the SIP registration logs, go to *Monitor* > *Log* > *SIP Registration Log*.

Choosing which events to log

Both the local and remote server configuration recognize the following events. Enable the events that you want to log.

Events logging options

Option	Description
System	Enable and select specific system logs. No system types are logged unless you enable this option. • *Configuration change*: Log configuration changes. • *Admin activity*: Log all administrative events, such as logins, resets, and configuration updates. • *System activity*: Log all system-related events, such as rebooting the FortiVoice system. • *HA*: Log all high availability (HA) activity. • *DHCP*: Log DHCP server events. • *Monitor*: Log call recording, call barging, and traffic capture events. • *Voicemail*: Log voicemail events. • *DNS*: Log DNS events.
Generic	Enable and select specific events. No event types are logged unless you enable this option. • *SMTP:* Log SMTP relay or proxy events. • *Activity*: Log voice user login and logout events.

Option	Description
Voice	Logs phone call events.
Fax	Logs fax events.
DTMF (Enhanced CDR)	Logs Dual Tone Multi-Frequency events. This option is for the local log setting only.
Hotel	Logs hotel management events, such as guest check-in and check-out. This option is for the local log setting only.
Call Center	Logs call center events, such as IVR and agent events. This option is for the 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 GUI of the FortiVoice system. If you require the ability to view logs from the GUI, also enable local storage. For details, see Configuring logging to the hard disk on page 334.

Before you can log to a remote location, you must first enable logging. For details, see Choosing which events to log on page 335. For logging accuracy, you should also verify that the FortiVoice system time is accurate. For details, see Configuring the time and date on page 81.

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
Enabled	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 system 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 333.
Facility	Select the facility identifier that the FortiVoice system will use to identify itself when sending log messages.

GUI field	Description
	To easily identify log messages from the FortiVoice system 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	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 335.

3. Click *Create*.
4. If the remote host is a FortiAnalyzer unit, confirm with the FortiAnalyzer administrator that the FortiVoice system 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 system, 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 GUI or download a backup copy of the FortiVoice system's configuration file in order to trigger an event log message.

   If the remote host does not receive the log messages, verify the FortiVoice system's network interfaces (see Configuring the network interfaces on page 48 and About the management IP on page 47) and static routes (see Configuring static routes on page 51), 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 call report profiles and generating reports

Log & Report > *Call Report* > *Call Report* displays a list of call report profiles.

A report profile is a group of settings that contains the report name, its subject matter, its schedule, and other aspects that the FortiVoice unit considers when generating reports from call 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 about scheduling the generation of reports, see Configuring report email notifications on page 339.

To view call 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 340.
View Report	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 39.
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.

To configure call report profiles

1. Go to *Log & Report* > *Call Report* > *Call Report*.
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, backslashes, single quotes, double quotes, commas, tabs or new lines.
4. Enter the *Time period* for the report.
5. For *Department*, select an option:

   The *Department* section is *not* visible on FVE-20E2 and FVE-50E6 models.

   - *All*: With this option, the call report will include calls from/to all departments.
   - *Single*: With this option, the call report will include all calls made from/to the specified department.
   - *Multiple*: With this option, the call report will include all calls for the specified *From* and *To* departments. To explain the *Multiple* option, let's use Engineering (From) and Marketing (To) as examples. The call report will include all calls from the Engineering department to the Marketing department.
6. Expand each option and configure the following as needed:
   - Configuring the report query selection on page 338
   - Configuring report email notifications on page 339
   - Configuring the report schedule on page 339
   - Generating a report manually on page 340
7. 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* and double-click on a report.
2. Expand *Query List* and click *New*.

3. Configure the following:

GUI field	Description
Department	Displays a single department or multiple departments, as specified in the call report profile. This field is read-only.
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.

4. 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 119.

To configure an email notification

1. Go to *Log & Report* > *Call Report* > *Call Report* and double-click on a report.
2. Expand *Email*.
3. In the *Format* field, select the format of the generated attachment, either *HTML*, *PDF, CSV ZIP*, 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.
5. Click *OK*.

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 340.

To configure the report schedule

1. Go to *Log & Report* > *Call Report* > *Call Report* and double-click on a 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 340. • *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*. • *These Dates*: Select to generate the report on specific date of each month, then enter those date numbers in *These days*. Also configure *Hour*.

4. Click *Close*.

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. Select the report profile that you want to use when generating the report.
3. Click *Generate*.
   The FortiVoice unit immediately begins to generate a report.
4. To view the resulting report, see Viewing generated reports on page 39.

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 the CDR submission, make sure to select *Add to Remote CDR - Field name*. For more information, see Setting up an IVR on page 269.

This section includes the following topics:

- Configuring CDR submission on page 340
- Modifying CDR templates on page 342
- Creating CDR filters on page 342

Configuring CDR submission

The *Log & Report* > *CDR* > *Submit CDR* submenu lets you configure the CDR submission to a database. The configuration values should match those of the database server.

To configure a CDR submission

1. Go to *Log & Report > CDR > Submit CDR.*
2. Click *New* . If *New* is grayed out, you have reached the maximum number of CDR entries.
3. Configure the following:

GUI field	Description
Name	Enter a name for the configuration.
Status	Select to enable the configuration.
Description	Click to enter any notes you have for the configuration.
Remote RESTful Server	Configure the database to which CDRs are submitted. For more information, see Configuring RESTful service on page 274.
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 from 1 to 60 minutes.
Authentication	*None*: Select to log onto the restful server without entering the user name and password. • *URL*: Enter the URL of the server hosting restful service. • *SSL verification*: Select if required. *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 about FortiVoice and Salesforce integration, see *Integrating FortiVoice with Salesforce on page 355*. • *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	Description
	For more information, see Modifying CDR templates on page 342.
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 342.
Custom value	Click *New* to add a custom value (a token, for example) that is required by the database server for information exchange. Click *Create*.

4. 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 *Create*.

Configuring SMDR

The FortiVoice station messaging detail record (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, CDR submission requires the FortiVoice SMDR to be enabled and Property Management System (PMS) uses the FortiVoice SMDR to manage hotel guest call charges.

This section contains the following topics:

- Configuring SMDR settings on page 343
- Setting SMDR formats on page 343

Configuring SMDR settings

Configure SMDR Setting to enable the FortiVoice communications with third-party devices.

To configure SMDR settings

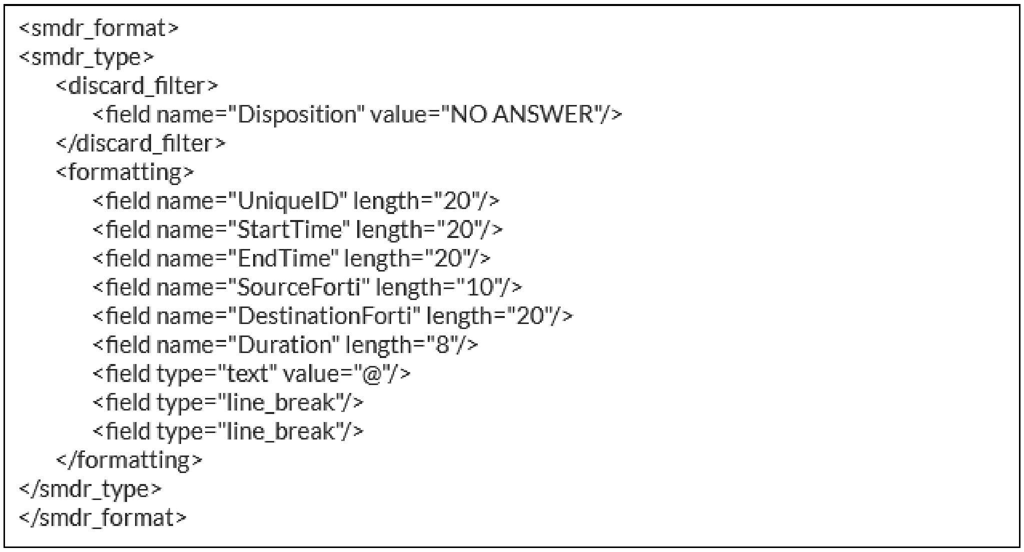
Configuring FortiVoice SMDR requires advanced SMDR knowledge and should be performed by advanced administrative users and field engineers.

1. Go to *Log & Report* > *SMDR* > *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 about format, see Setting SMDR formats on page 343.
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 from 1 to 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 SMDR XML format files. You can modify the files to meet your needs. The following image shows an example SMDR XML format file:



```
<smdr_format>
<smdr_type>
    <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="20"/>
        <field name="Duration" length="8"/>
        <field type="text" value="@"/>
        <field type="line_break"/>
        <field type="line_break"/>
    </formatting>
</smdr_type>
</smdr_format>
```

An SMDR format is composed of parts as shown in the above example:

- *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 > SMDR Format*.
2. Click *New*.
3. To display the complete list of FortiVoice SMDR field names, click *FortiVoice SMDR Fields*.
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 344) and which event categories will trigger an alert email message (see Configuring alert categories on page 345).

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 about DNS, see Configuring DNS on page 52.

You can customize the alert email. For more information, see Customizing call report and notification email templates on page 119.

This section contains the following topics:

- Configuring alert recipients on page 344
- Configuring alert categories on page 345

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. To add the email address of a recipient, click *New*.
   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 344).

To select events that will trigger an alert email message

1. Go to *Log & Report* > *Alert* > *Category*.
2. Enable one or more of the following event categories:

GUI field	Description
Critical events	Send an alert email when the FortiVoice unit detects a system error that may affect its operation.
Disk is full	Send an alert email when the hard disk of the FortiVoice unit is full.
HA events	Send an alert email when any high availability (HA) event occurs.
Archive quota is exceeded	Send an alert email 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 308.
Deferred emails # over	Send an alert email 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 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.
Generate daily call summary at hour	Send an alert email with a daily call summary including the number of total calls, long distance calls, and international calls. 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 09:00, the summary will be for the period from 9 am of the previous day to 9 am 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.

GUI field	Description
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 Configuring VoIP trunks on page 229.
Massive SIP authentication failure	Send an alert email when big scale SIP authentication sessions fail.
Daily Security Audit report	Send an alert email with a daily security audit.
Entitlement changed	Send an alert email when an entitlement has expired. If your FortiVoice phone system uses entitlements, you can view them in the License Information widget on page 26.
SIP trunk/office peer connectivity alert	Set the time interval (hours) for sending an alert email. Click + and select the trunks of which an alert email is sent when a trunk has an issue.

3. Click *Apply*.

Integrating FortiVoice with third-party solutions

This topic includes:

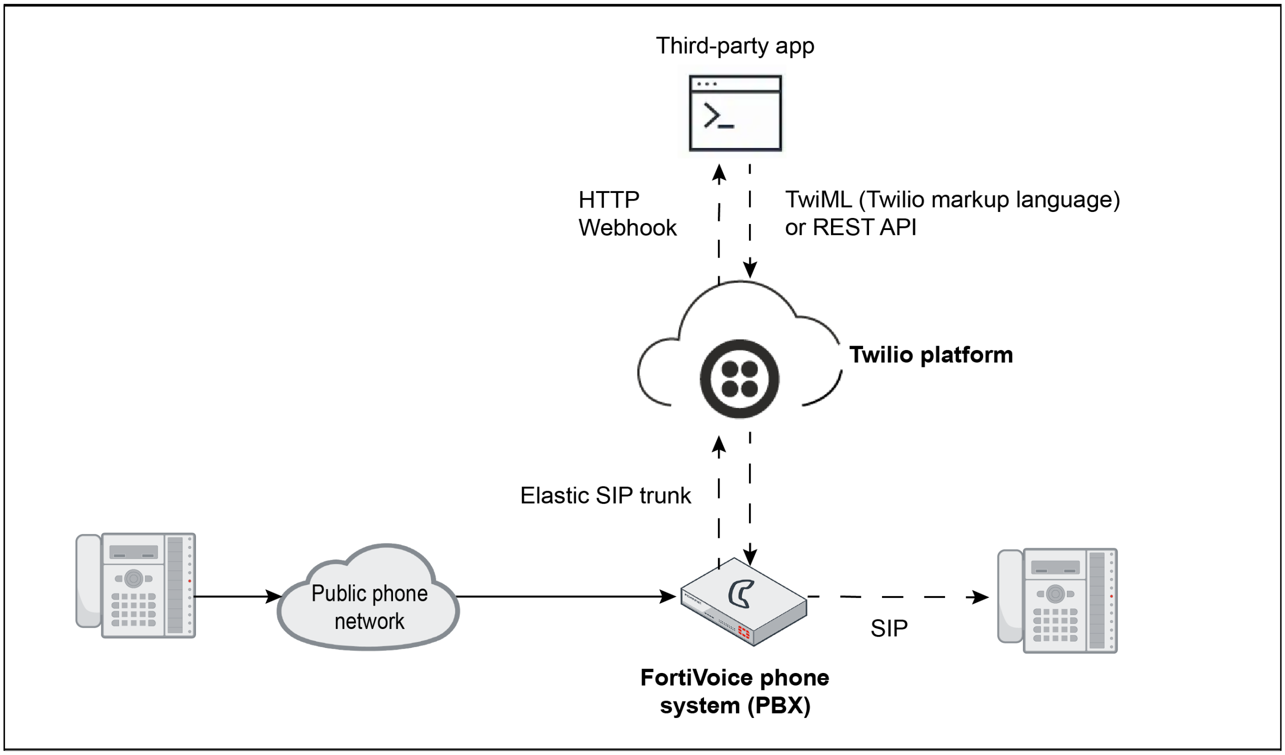
- Integrating FortiVoice with Twilio on page 347
- Integrating FortiVoice with Singlewire InformaCast on page 350
- Integrating FortiVoice with Salesforce on page 355

Integrating FortiVoice with Twilio

This section describes how to configure the FortiVoice phone system to provide a telephony service with Twilio's elastic SIP trunking. The integration enables incoming calls to the FortiVoice phone system to be routed to Twilio for additional services such as interactive voice response (IVR) or speech recognition. After completing the user data collection and responses, the call control can be subsequently transferred to a telephone extension or an agent served by the FortiVoice phone system.

The FortiVoice dial plan provides digit translation and call routing for the system. Use the dial plan to customize the routing of calls to and from the Twilio platform. If Twilio uses a SIP REFER to implement a call back to FortiVoice, you do not have to configure an inbound dial plan.

The following diagram illustrates an example network topology of FortiVoice with Twilio.



Considerations about accessing and using Twilio:

- A Twilio demo account does not allow you to call from and to numbers that you did not add to the FortiVoice phone system. Therefore, it is a good idea to upgrade your Twilio account to perform your testing.
- Twilio treats a SIP trunk (in and out) as two separate items.
- Twilio uses a specific number format (+1xxxyyyyyyy) where xxx is the area code and yyyyyyy is the phone number.

To complete the configuration tasks on Twilio

1. Sign up for a Twilio paid account. The demo account has too many restrictions.
2. Create and configure a Twilio elastic SIP trunk. After you complete this task, you will receive a uniform resource identifier (URI). Twilio's elastic SIP trunking uses an fully qualified domain name (FQDN) as a termination URI that is used by the FortiVoice phone system to direct SIP traffic towards Twilio.
3. Take note of this URI because you will need this URI when you set the SIP server during the configuration of the FortiVoice SIP trunk.

To create a FortiVoice SIP trunk

1. In the FortiVoice GUI, go to *Trunk* > *VoIP* > *SIP*.
2. Click *New*.
3. Configure the following parameters:

GUI field	Description
SIP	
Name	Enter the trunk name. For example, Twilio.
Enable	Select to activate this SIP trunk.
Display name	Enter the caller ID that will appear on the called phone, such as Example Company.
Main number	Enter the number that will appear on the called phone.
SIP setting	
SIP server	Enter the SIP URI that you have received from Twilio. For example, yourname.pstn.twilio.com.
SIP port	Keep the default value (5060).
Using SRV record	Keep this setting disabled.
User name	Enter the name that you have used during the creation of the Twilio elastic SIP trunk.
Password	Enter the password that you have used during the creation of the Twilio elastic SIP trunk.
Auth. user name	Enter the same user name that you have used during the creation of the Twilio elastic SIP trunk. The user name and auth. user name are the same.
Realm/Domain	Enter the same URL that you have entered in the *SIP server* field.
SIP settings	Keep the default setting (sip_trunk_default).
Max channel	Each trunk contains multiple channels. The number of channels you have in a trunk is controlled by your VoIP provider.

GUI field	Description
Max outgoing channel	With the known number of max channels, if you need to reserve incoming channels, you can enter the number of outgoing channels allowed and the remaining channels are for incoming calls.
User=Phone in SIP URI	Keep this setting disabled.
Inband ringtone (Early media)	Keep this setting disabled.
Caller ID Option	Keep the default settings.
Registration	Select *Standard*.
Outbound Proxy	Keep this setting disabled.

4. Click *Create*.

To create a FortiVoice dial plan for inbound calls

1. In the FortiVoice GUI, go to *Call Routing* > *Inbound*.
2. Click *New*.
3. Configure the following parameters:

GUI field	Description
Name	Enter a name for this plan.
Enable	Select to activate this dial plan.
From Trunk	Click **+**. From the list available entries, select the Twilio SIP trunk.
Call Handling	From the Action type list, select *Dial Local Number* to process incoming calls. To route calls to a local extension number, create a match pattern.

4. Click *Create*.

To create a FortiVoice dial plan for outbound calls

1. In the FortiVoice GUI, go to *Call Routing* > *Outbound*.
2. Click *New*.

3. Configure the following parameters:

GUI field	Description
Name	Enter a name for this plan.
Enable	Select to activate this dial plan.
Dialed Number Match	Create a number pattern to match a number or a range of numbers for how the call handling will be applied to the respective calls.
Call Handling	The actions to process the incoming calls with matched dialed numbers and/or caller IDs. **1.** Click *New*. **2.** In *Action*, select *Allow*. **3.** In *Outgoing trunk*, select the Twilio SIP trunk.

4. Click *Create*.

Integrating FortiVoice with Singlewire InformaCast

This section describes how to configure the FortiVoice phone system to work with the InformaCast message notification solution for delivering real-time text and audio message notifications to Fortinet FortiFone IP desk phones (FON-x70, FON-x75 and FON-x80). This integration provides a powerful notification solution that extends device coverage across both data and voice networks.

For information about InformaCast configuration, see its product guides.

The FortiVoice - InformaCast message notification solution is implemented using the following features and applications on each platform:

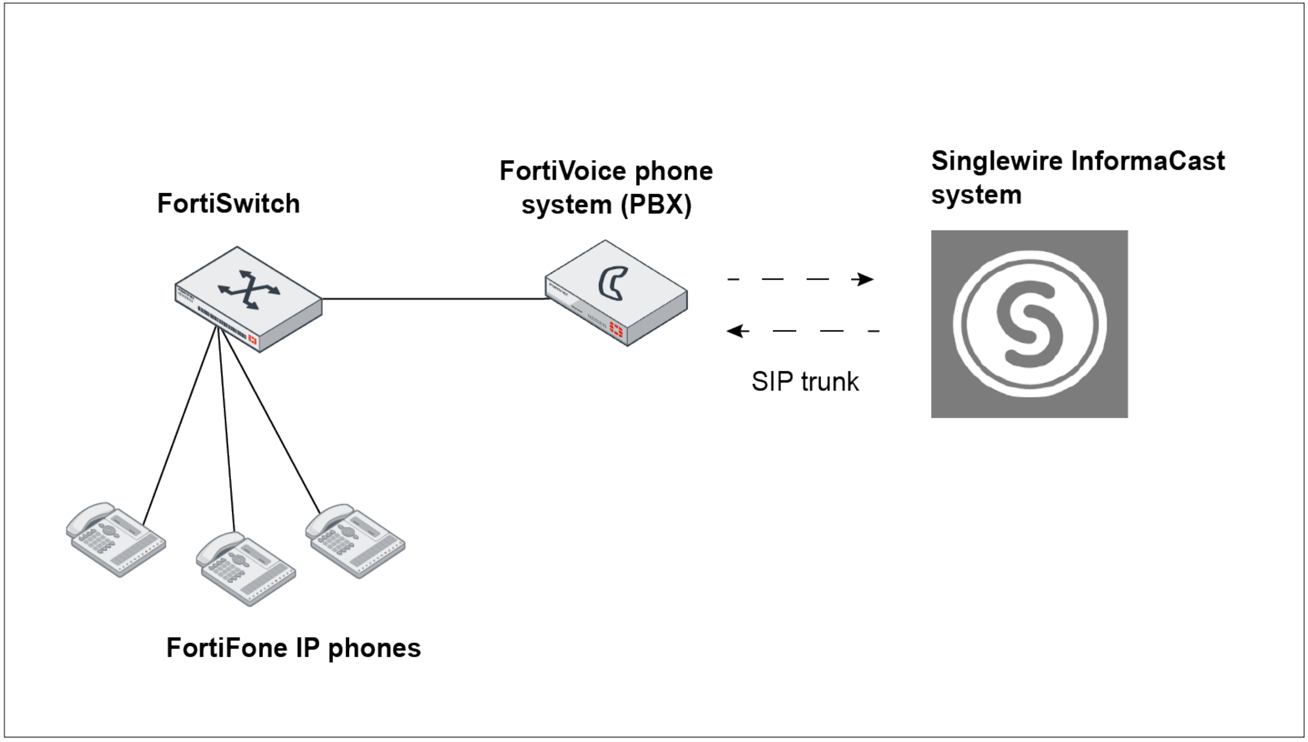
Feature or application	Platform	
	FortiVoice	InformaCast
Transport	IP SIP Trunk	Legacy Paging Interface (LPI)
Call Routing	Dial Plan	DialCast
Message Group	Page/Message Group	Recipient Group
Message(s)	Audio and/or text	Audio and/or text
Recipient	Extensions	IP Speaker

- **Transport**: A SIP trunking interface on the FortiVoice platform is configured to connect with InformaCast's Legacy Paging Interface (LPI) using a standard SIP protocol. A SIP trunk and server group is defined on both platforms to provide a logical voice-over-IP connection for the delivery and reception of calls and notifications.
- **Call Routing**: A dial plan on the FortiVoice platform is configured to route calls to and from the InformaCast platform. Similarly, InformaCast uses a DialCast feature to configure a dialed pattern match to trigger a message broadcast.
- **Message Group**: A group of endpoints configured to receive, display, and play message(s).
- **Message(s)**: Custom text and audio (pre-recorded or live) message types for broadcasting. FortiVoice can

broadcast text messages to FortiFone IP phones.

- **Recipient**:An endpoint configured to receive, display, and play message(s).

The following diagram illustrates the high-level network topology of FortiVoice and InformaCast integration:



Configuring the FortiVoice

Using the FortiVoice GUI, configure the FortiVoice phone system to work with the InformaCast message notification solution for delivering real-time text and audio message notifications to FortiFone IP phones.

To create a FortiVoice SIP trunk

1. Go to *Trunk* > *VoIP* > *SIP*.
2. Click *New*.
3. Configure the following:

GUI field	Description
SIP	
Name	Enter the trunk name. For example, InformaCast.
Enable	Select to activate this SIP trunk.
Display name	Enter the caller ID that will appear on the called phone, such as Example Company.
Main number	Enter the number that will appear on the called phone.

GUI field	Description
SIP setting	
SIP server	Enter the URL that you have received from InformaCast. For example, yourname.pstn.informacast.com.
SIP port	Keep the default value (5060).
Using SRV record	Keep this setting disabled.
User name	Enter the name that you have used during the creation of the InformaCast SIP trunk.
Password	Enter the password that you have used during the creation of the InformaCast SIP trunk.
Auth. user name	Enter the same user name that you have used during the creation of the InformaCast SIP trunk. The user name and auth. user name are the same.
Realm/Domain	Enter the same URL that you have entered in the *SIP server* field.
SIP settings	Keep the default setting (sip_trunk_default).
Max channel	Each trunk contains multiple channels. The number of channels you have in a trunk is controlled by your VoIP provider.
Max outgoing channel	With the known number of max channels, if you need to reserve incoming channels, you can enter the number of outgoing channels allowed and the remaining channels are for incoming calls.
User=Phone in SIP URI	Keep this setting disabled.
Inband ringtone (Early media)	Keep this setting disabled.
Caller ID Option	Keep the default settings.
Registration	Select *Standard*.
Outbound Proxy	Keep this setting disabled.

4. Click *Create*.

To create a dial plan for inbound calls

1. Go to *Call Routing* > *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	Click **+**. From the list available entries, select the InformaCast SIP trunk.
Call Handling	From the *Action type* list, select *Dial Local Number* to process incoming calls. To route calls to a local extension number, create a match pattern.

4. Click ***Create***.

To create a dial plan for outbound calls

1. Go to *Call Routing* > *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 about setting emergency number, see Setting FortiVoice location, contact, and emergency information on page 114.
Dialed Number Match	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 about adding a dialed number match, see Creating dialed number match on page 256.
Call Handling	The actions to process the outgoing calls with matched dialed numbers and/or caller IDs. **1.** Click *New*. **2.** In *Action*, select *Allow*. **3.** In *Outgoing trunk*, select the InformaCast SIP trunk.

4. Click *Create*.

To create a message group for sending and relaying text and audio messages

1. Go to *Extension* > *Group* > *Message Group.*
2. Click *New*.
3. Configure the following:

GUI field	Description
Name	Enter a unique name for the group.

GUI field	Description
Number	Enter the message group number following the local number pattern defined when configuring your inbound dial plan handling action. This is the number that, once dialed, will send text or audio messages to all the extensions included in the group. For example, an authorized InformaCast user can dial this number to send text and audio messages to FortiFone IP phones.
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 messages.
If you select to send text messages, select *Text* and configure the following:	
Title	Enter the notification message title.
Message	If this message group is for relaying text messages from InformaCast to FortiFone IP phones, do not do anything. If you want to send a text message to the FortiFone IP phones through InformaCast, 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.
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	Select the user groups for this message group. The text messages received from InformaCast or composed on FortiVoice will be sent to the FortiFone extensions of these user groups. For more information, see Creating extension groups on page 217.
If you select to send audio messages, select *Audio* and configure the following:	
Sound file	If this message group is for relaying audio messages from InformaCast to FortiFone IP phones, do not do anything. If you want to send an audio message to the FortiFone IP phones through InformaCast, select an existing sound file or click *New* to create a new one for the audio message. For information about sound files, see Managing phone audio settings on page 125.
Multicast group	Select the multicast paging group for this message group or click *New* to create a new one for the audio message. You can also click *Edit* to modify the selected one. The audio messages received from InformaCast or recorded on FortiVoice will be sent to the FortiFone extensions of these multicast groups. For more information, see Creating extension groups on page 217.
Single number	Enter the external phone number to which you want to send audio messages and click *OK*.

4. Click *Create*.

Integrating FortiVoice with Salesforce

This section describes how to configure the FortiVoice phone system to work with Salesforce for calling and call detail record (CDR) logging.

Prerequisites

- The FortiVoice phone system must use the firmware version 5.3.10 or later.
- The Salesforce summer release must be version 17 or later.
- The FortiVoice IP address is added in the Network Access of Salesforce.
- The Salesforce Ant Migration tool is available.
- The FortiVoice public domain name with signed certificate by a trusted CA is available.
- The FortiVoice SMDR is enabled.
- The FortiVoice HTTPS port mapping is complete.

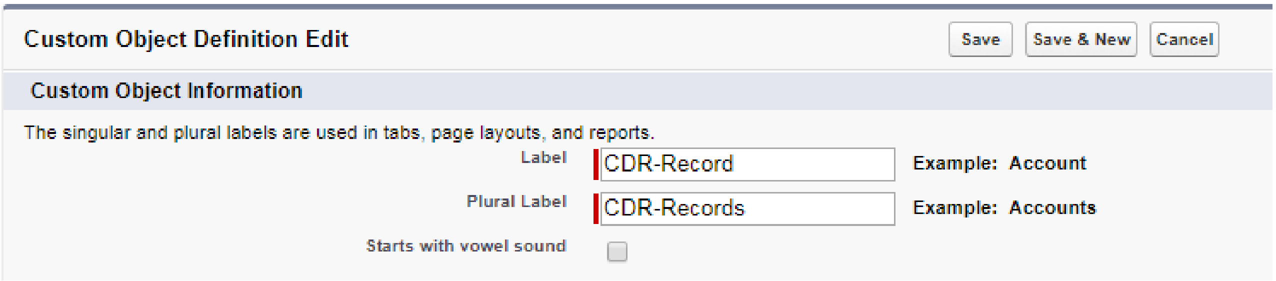
Workflow

To configure the Salesforce and FortiVoice integration, perform the following tasks:

1. Setting up a connected application on Salesforce on page 355
2. Creating a custom object on Salesforce on page 356
3. Configuring the FortiVoice phone system on page 358

Setting up a connected application on Salesforce

1. Log in to Salesforce as an administrator.
2. Click the Setup icon, then *Setup*.
3. Select *Objects and Fields* > *Object Manager*.
4. Click *Create* > *Custom Object*.
5. Enter the *Label* and the *Plural Label* for this object.
6. Click *Save*.



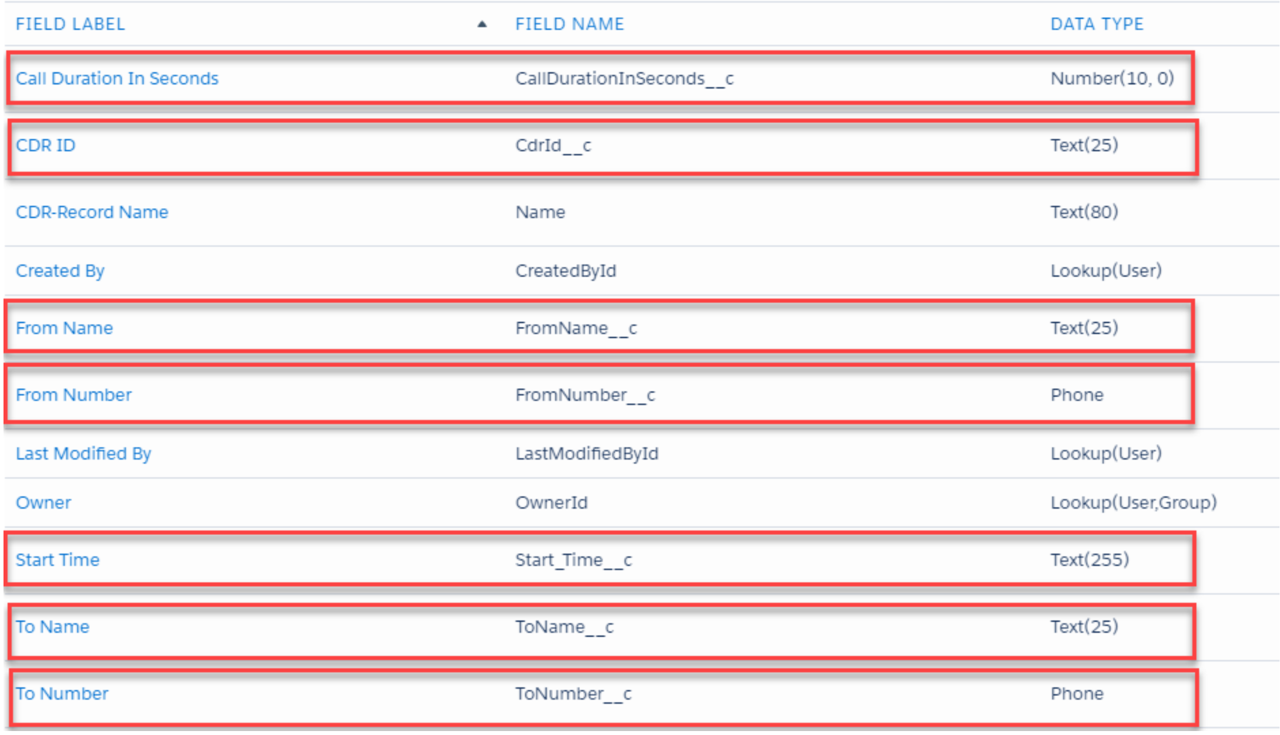
Custom Object Definition Edit

Custom Object Information

The singular and plural labels are used in tabs, page layouts, and reports.

Label	CDR-Record	Example: Account
Plural Label	CDR-Records	Example: Accounts
Starts with vowel sound	☐	

7. Go to *Field and Relationships* > *New* and select the following field names and data types for *FIELD LABEL:*



FIELD LABEL ▲	FIELD NAME	DATA TYPE
Call Duration In Seconds	CallDurationInSeconds__c	Number(10, 0)
CDR ID	CdrId__c	Text(25)
CDR-Record Name	Name	Text(80)
Created By	CreatedById	Lookup(User)
From Name	FromName__c	Text(25)
From Number	FromNumber__c	Phone
Last Modified By	LastModifiedById	Lookup(User)
Owner	OwnerId	Lookup(User,Group)
Start Time	Start_Time__c	Text(255)
To Name	ToName__c	Text(25)
To Number	ToNumber__c	Phone

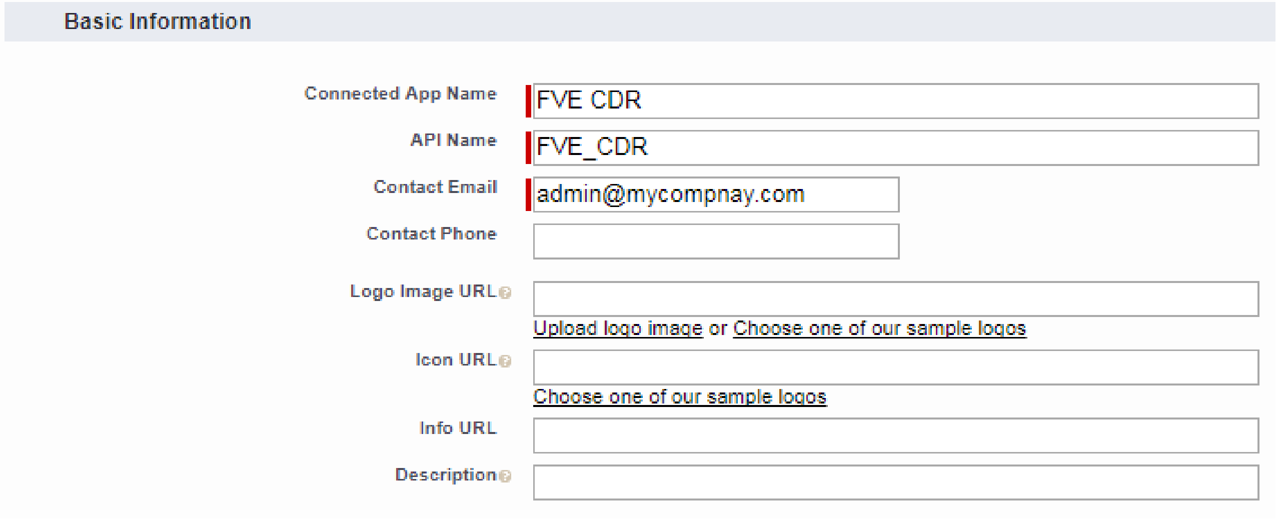
8. To display the call duration in a readable format, click *New* and choose *Formula* for the type.
9. For *Name*, enter Call duration.
10. In *Formula Return Type*, select *Text*.
11. Enter the following into the text field:

```
IF ((MOD(CallDurationInSeconds__c,3600)/60)>10,
TEXT(FLOOR(CallDurationInSeconds__c/3600))+ ":",
TEXT(FLOOR(CallDurationInSeconds__c/3600))+ ":0")
+ IF ((MOD(MOD(CallDurationInSeconds__c,3600),60))>10,
TEXT(FLOOR(MOD(CallDurationInSeconds__c,3600/60)/60)) + ":",
TEXT(FLOOR(MOD(CallDurationInSeconds__c,3600/60)/60)) + ":0")
+ TEXT(MOD(MOD(CallDurationInSeconds__c,3600),60))
```

12. To ensure that there are no errors, click *Check Syntax*.
13. Click Save.

Creating a custom object on Salesforce

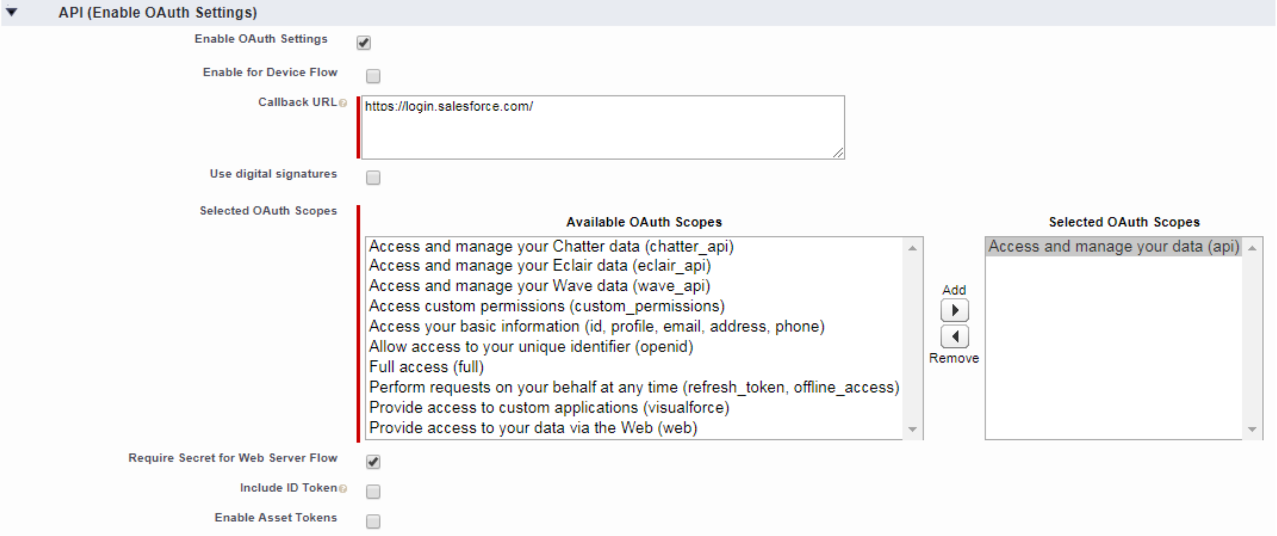
1. Log in to Salesforce as an administrator.
2. Click the Setup icon, then *Setup*.
3. Select *App* > *App Manager*, and click the *New Connected App* button.
4. Under *Basic Information*, enter the names for the application and API and email address for the administrator.



Basic Information

Connected App Name	FVE CDR
API Name	FVE_CDR
Contact Email	admin@mycompnay.com
Contact Phone	
Logo Image URL	Upload logo image or Choose one of our sample logos
Icon URL	Choose one of our sample logos
Info URL	
Description	

5. For *API (Enable OAuth Settings)*, configure the following fields and then click *Save:*
   - In *Callback URL*, enter https://login.salesforce.com/
   - In *Selected OAuth Scopes*, select *Access and manage your data (api)* and click *Add*.



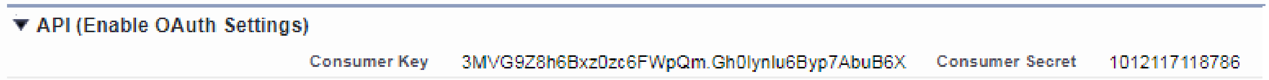
API (Enable OAuth Settings)

Enable OAuth Settings	☑
Enable for Device Flow	□
Callback URL	https://login.salesforce.com/
Use digital signatures	□
Selected OAuth Scopes	

Available OAuth Scopes	Selected OAuth Scopes
Access and manage your Chatter data (chatter_api)	Access and manage your data (api)
Access and manage your Eclair data (eclair_api)	
Access and manage your Wave data (wave_api)	
Access custom permissions (custom_permissions)	
Access your basic information (id, profile, email, address, phone)	
Allow access to your unique identifier (openid)	
Full access (full)	
Perform requests on your behalf at any time (refresh_token, offline_access)	
Provide access to custom applications (visualforce)	
Provide access to your data via the Web (web)	

Require Secret for Web Server Flow	☑
Include ID Token	□
Enable Asset Tokens	□

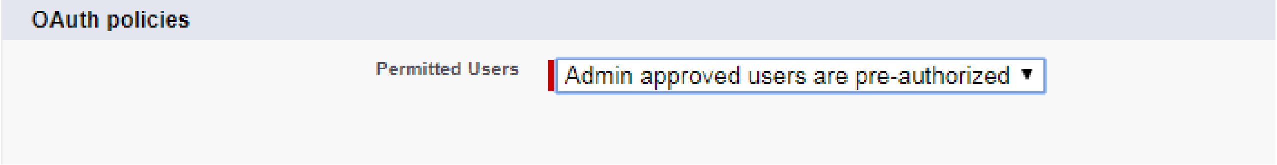
6. Copy the *Consumer Key* and the *Consumer Secret*. You will need this information during the FortiVoice configuration.



API (Enable OAuth Settings)

Consumer Key 3MVG9Z8h6Bxz0zc6FWpQm.Gh0lynlu6Byp7AbuB6X Consumer Secret 1012117118786

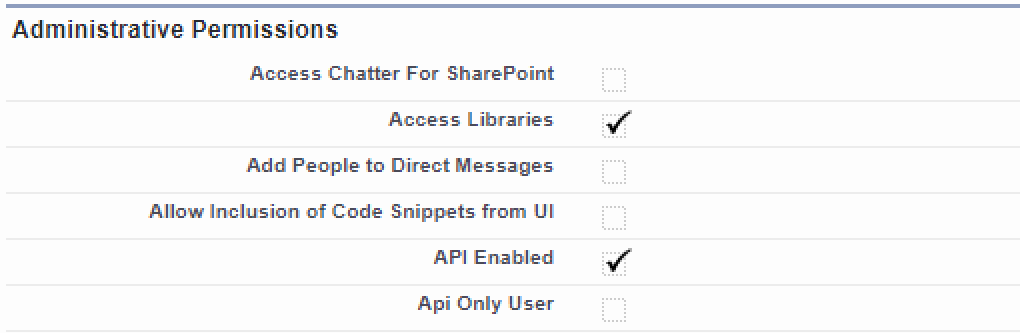
7. Click *Manage* > *Edit Policies*.
8. In *Permitted Users*, select *Admin approved users are pre-authorized* and click *Save*.



OAuth policies

Permitted Users: Admin approved users are pre-authorized ▼

9. Click *Manage Profile* > *System Administrator*.
10. Make sure *Access Libraries* and *API Enabled* are checked, and click *Save*.



Administrative Permissions

Access Chatter For SharePoint	☐
Access Libraries	✓
Add People to Direct Messages	☐
Allow Inclusion of Code Snippets from UI	☐
API Enabled	✓
Api Only User	☐

Configuring the FortiVoice phone system

A new database interface must be configured for FortiVoice to send out CDR.

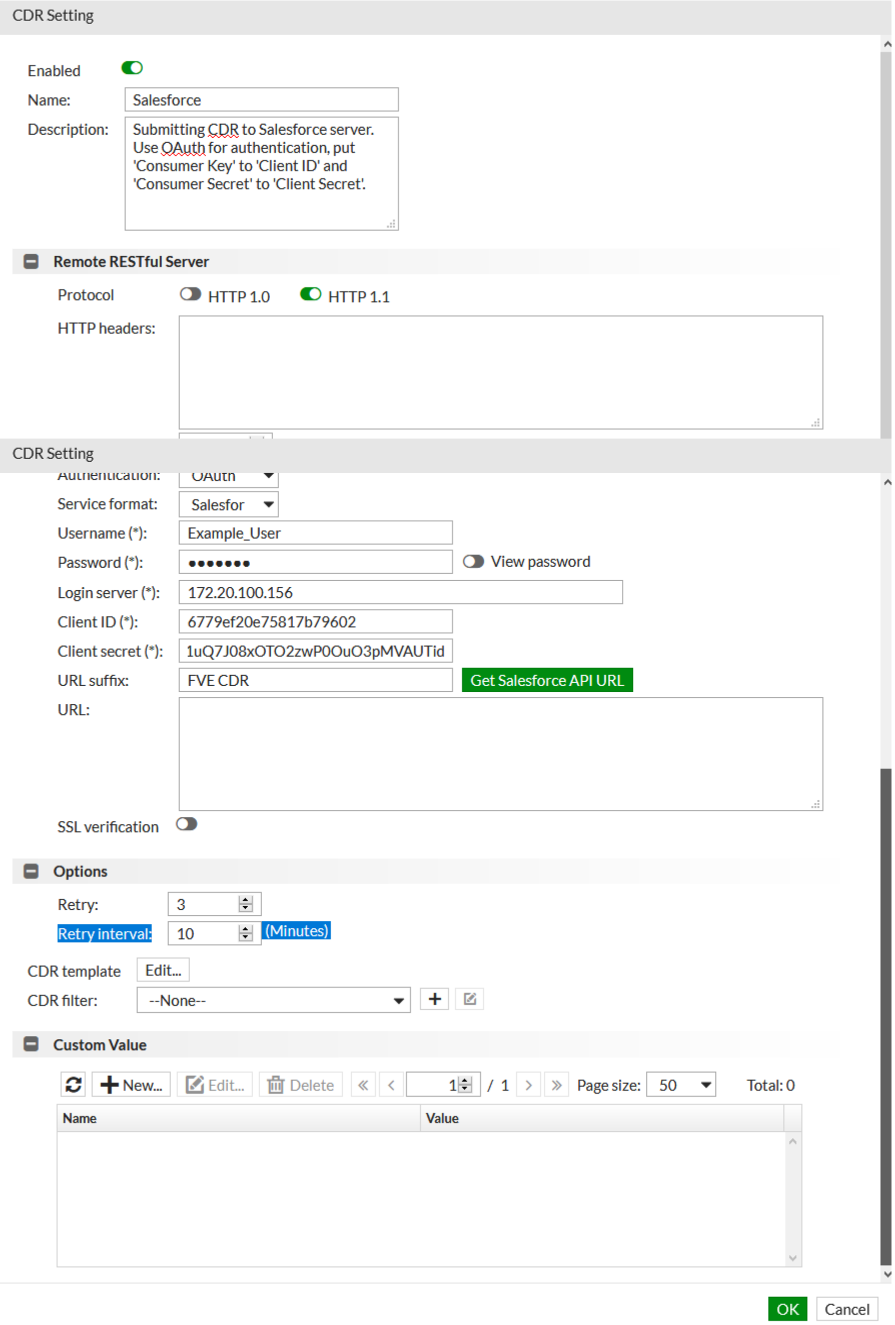
1. Log in to FortiVoice as an administrator.
2. Go to *Log & Report > CDR > Submit CDR*.
3. Click *New*.
4. Configure the following:

GUI field	Description
Name	Enter a name for the CDR submission.
Remote RESTful Server	*Protocol*: Select *HTTP 1.1*.
Authentication	Select *OAuth*.
Service format	Select *Salesforce*.
Username	Enter the login user name registered on the Salesforce server.
Password	Enter the login password registered on the Salesforce server.
Login server	Enter the Salesforce server IP address.
Client ID	Enter the Consumer Key recorded in step 6 of Creating a custom object on Salesforce on page 356.
Client secret	Enter the Consumer Secret recorded in step 6 of Creating a custom object on Salesforce on page 356.
URL suffix	Enter the Connected App Name that was created in step 4 of Creating a custom object on Salesforce on page 356. Click *Get Salesforce API URL* to display the created URL.

Options	*CDR template*:
	• Click *Edit*.
	• On the *CDR Template* page, go to *Content > HTML*.
	• Replace the field content with the following:
	`<FV_CDR__c>`
	`        <CdrId__c>%%CDR_UNIQUE_ID%%</CdrId__c>`
	`        <ToName__c>%%CDR_CALLEE_ID%%</To_Name__c>`
	`        <ToNumber__c>%%CDR_DST_UID%%</To_Number__c>`

GUI field	Description
	<FromName__c>%%CDR_CALLER_ID%%</From_Name__c> <FromNumber__c>%%CDR_SRC_UID%%</From_Number__c> <StartTime__c>%%CDR_ANSWER_TIME%%</Start_Time__c> <CallDurationInSeconds__c>%%CDR_TALK_TIME%%</CallDurationInSeconds__c> </FV_CDR__c>

5. Click *OK*.
6. Click *Create*.



CDR Setting

Enabled ●
Name: Salesforce
Description: Submitting CDR to Salesforce server. Use OAuth for authentication, put 'Consumer Key' to 'Client ID' and 'Consumer Secret' to 'Client Secret'.

Remote RESTful Server

Protocol ○ HTTP 1.0 ● HTTP 1.1
HTTP headers:

CDR Setting

Authentication: OAuth
Service format: Salesfor
Username (*): Example_User
Password (*): •••••••• ○ View password
Login server (*): 172.20.100.156
Client ID (*): 6779ef20e75817b79602
Client secret (*): 1uQ7J08xOTO2zwP0OuO3pMVAUTid
URL suffix: FVE CDR
URL:
SSL verification ○

Options

Retry: 3
Retry interval: 10 (Minutes)

CDR template Edit...
CDR filter: --None--

Custom Value

Managing the firmware

Fortinet periodically releases FortiVoice firmware updates to include enhancements and address issues. New firmware can also introduce new features which you must configure for the first time. Fortinet recommends that you download and install patch releases as soon as they are available.

For information about new and changed features, supported upgrade paths, and resolved issues included in a FortiVoice firmware version, see the Release Notes.

This section includes the following topics:

- Downloading the firmware image file on page 360
- Testing a firmware image on page 360
- Upgrading the firmware on page 362
- Downgrading the firmware on page 364
- Performing a clean firmware installation on page 367

Downloading the firmware image file

Access the Fortinet Support website and download the firmware image file for the version that you want to upgrade to.

1. Go to the Fortinet Support website.
2. Log in to your existing account or register for an account.
3. Select *Support* > *Firmware Download*.
4. In *Select Product*, select *FortiVoice*.
5. Select the *Download* tab and navigate to the folder for the firmware version that you are upgrading to.
6. To download the firmware image file to your management computer, go to the end of the row and click *HTTPS*.
7. Save the file on your management computer.
8. Take note of the location where you save the file.

Testing a firmware image

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.
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 Upgrading the firmware on page 362.
    - If the new firmware image does **not** operate successfully, reboot the FortiVoice unit to discard the temporary firmware and resume operations using the existing firmware.

Upgrading the firmware

⚠ Before upgrading the firmware of the FortiVoice unit, review the Release Notes for the new firmware version. The Release Notes document includes the most current upgrade information such as the supported upgrade path and may contain details that were unavailable at the time this guide was created.

Older 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.

You can use either the GUI or the CLI to upgrade 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.

To determine if you are upgrading your firmware image, examine the firmware version number. For example, if your current firmware version is `v64,build0446` and you are changing to `v64,build0469`, then the later build number indicates that you are upgrading your firmware image.

To upgrade the firmware using the GUI

1. Download the firmware image files from the Fortinet Support website. For details, see Downloading the firmware image file on page 360.
2. Back up the configuration and call data. For details, see Backing up the configuration on page 109.
3. Log in to the GUI as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
4. To upload the firmware for an upgrade:
   a. Go to *Dashboard* > *Status*.
   b. In the *System Information* widget, go to Firmware version and click Update.
   c. Locate and select the file, and then click *Open*.
   d. To confirm the upload, click *Yes*.
   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.
5. Clear the cache of your web browser and restart it to ensure that it reloads the GUI and correctly displays all changes.
6. To verify that the firmware was successfully installed, log in to the GUI and go to *Dashboard* > *Status* and in the *System Information* area. Text appearing in the *Firmware version* row indicates the currently installed firmware version. [

To install firmware using the CLI

1. Download the firmware image files from the Fortinet Support website. For details, see Downloading the firmware image file on page 360.
2. Back up the configuration and call data. For details, see Backing up the configuration on page 109.
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 GUI, clear the cache of your web browser and restart it to ensure that it reloads the GUI 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. Go to Verifying the configuration after an upgrade on page 363.

Verifying the configuration after an upgrade

After upgrading to a new firmware image, 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 the 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 GUI.
2. Log in to the GUI 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.

Downgrading the firmware

Downgrading the firmware is not recommended.

The downgrade process may cause the FortiVoice system to remove parts of the configuration that are invalid for that earlier version.

After downgrading the firmware, you may be unable to restore your previous configuration from the backup configuration file.

In some cases, you may lose all call data and configurations.

You can use either the GUI or the CLI to 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.

To determine if you are downgrading your firmware image, examine the firmware version number. For example, if your current firmware version is `v64,build0469` and you are changing to `v64,build0446`, then the earlier build number indicates that you are downgrading your firmware image.

To downgrade to an earlier firmware version using the GUI

1. Download the firmware image files from the Fortinet Support website. For details, see Downloading the firmware image file on page 360.
2. Back up the configuration and call data. For details, see Backing up the configuration on page 109.
3. Log in to the GUI as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
4. To upload the firmware for an upgrade:
   a. Go to *Dashboard* > *Status*.
   b. In the *System Information* widget, go to Firmware version and click Update.
   c. Locate and select the file, and then click *Open*.
   d. To confirm the upload, click *Yes*.
   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.
   The FortiVoice unit reverts the configuration to default values for that version of the firmware.
5. Clear the cache of your web browser and restart it to ensure that it reloads the GUI and correctly displays all changes.
6. Reconnect to the FortiVoice unit to either reconfigure the FortiVoice unit or restore the configuration file. For details, see
7. To verify that the firmware was successfully installed, log in to the GUI and go to *Dashboard* > *Status* and in the *System Information* area. Text appearing in the *Firmware version* row indicates the currently installed firmware version.

To downgrade to an earlier firmware version using the CLI

1. Download the firmware image files from the Fortinet Support website. For details, see Downloading the firmware image file on page 360.
2. Back up the configuration and call data. For details, see Backing up the configuration on page 109.

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 GUI, clear the cache of your web browser and restart it to ensure that it reloads the GUI 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. 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 365 and Restoring the configuration on page 366.

Reconnecting to the FortiVoice unit

After a firmware downgrade, the FortiVoice unit reverts to default settings for the installed firmware version, including the IP addresses of network interfaces through which you connect to the FortiVoice GUI and/or CLI.

If your FortiVoice unit has not been reset to its default configuration, but you cannot connect to the GUI 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 367.

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 a terminal emulation software such as PuTTY.
3. Configure the software to connect directly to the communications (COM) port on your computer and click *OK*.
4. Use the following serial connection settings:

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

5. Start a serial connection 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 IP address and netmask are saved.
9. You can now reconnect to either the GUI or CLI through that network interface. For information about restoring the configuration, see Restoring the configuration on page 366.

Restoring the configuration

After a firmware downgrade or clean firmware installation, you may be able to restore a backup copy of the configuration file from your local computer using either the GUI or CLI. For information about configuration backup, see Backing up the configuration on page 109.

To restore the configuration file using the GUI

1. Clear your browser's cache. If your browser is currently displaying the GUI, also refresh the page.
2. Log in to the GUI.
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 settings have been successfully loaded.

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 settings have been successfully loaded.

Performing a clean firmware installation

Performing a clean firmware installation can be useful if:

- You are unable to connect to the FortiVoice unit using the GUI or the CLI.
- You want to install firmware **without** preserving any existing configuration.
- A firmware version that you want to install requires that you format the boot device (see the Release Notes accompanying the firmware).

Unlike a firmware upgrade or downgrade, a clean firmware installation re-images the boot device. Also, a clean firmware installation 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 about backups, see Backing up the configuration on page 109. For information about reconnecting to a FortiVoice unit whose network interface configuration has been reset, see Reconnecting to the FortiVoice unit on page 365.

If you are downgrading to an earlier FortiVoice version, you may not be able to restore your previous configuration from the backup configuration file.

To perform a clean firmware installation

1. Download the firmware image file from the Fortinet Support website. For details, see Downloading the firmware image file on page 360.
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 GUI 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 366.

Appendix A: Shared line appearance

Configure the shared line appearance (SLA) feature to allow any group member to monitor and answer calls received on a shared line.

Supported phone models

The SLA functionality is available on FortiFone FON-x80/x80B phones.

Supported accounts

The following table lists the phone models, account totals, and lines per account:

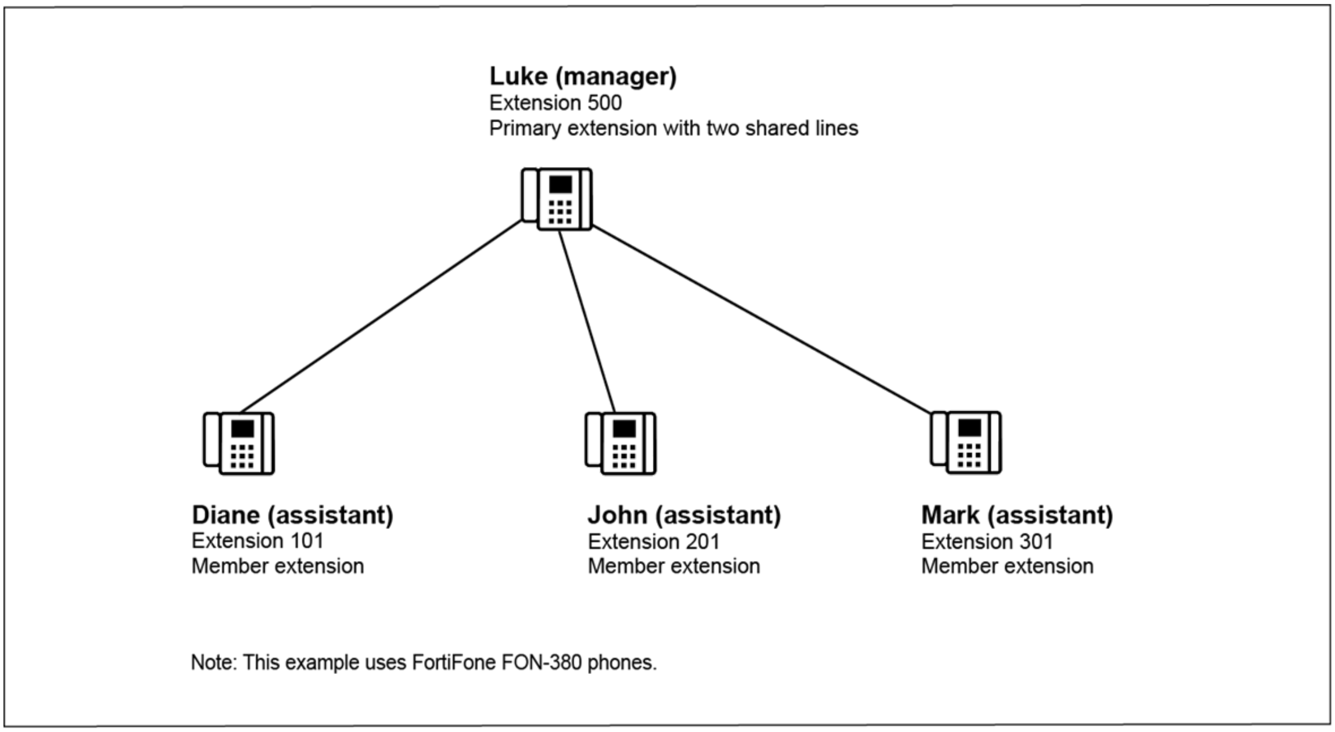
Phone model	Account total	Lines per account
FON-280B	2	10
FON-380 and FON-380B	4	10
FON-480 and FON-480B	8	10
FON-580 and FON-580B	16	10
Note 1: The account total equals how many extensions a phone can monitor minus one account which is the phone's own extension. Note 2: The information in this table applies to FON-x80/x80B phones using version 3.0.19 or later.		

Example scenario with one manager and three assistants

This section describes the following scenario for the SLA feature:

- Diane, John, and Mark are assistants and use extensions 101, 201, and 301 respectively. Luke is their manager and uses extension 500.
- All assistants can monitor their manager's lines. Those are the shared lines. In our example scenario, Luke has two shared lines.
- When there is an incoming call on one of the shared lines, all assistant phones will ring. Any assistant can answer the call. If no one answers the call after a specified time period, the manager's phone will ring.

The following diagram illustrates the example SLA scenario:



Prerequisites

- You have created and configured the assistant and manager extensions in *Extension* > *Extension* > *IP Extension*. For details, see Configuring IP extensions on page 183.
- You have added the FortiFone-380 phones to FortiVoice and assigned them to the extensions. For details, see Configuring desk phones on page 159.

To configure SLA, complete the following sections:

1. Configuring an SLA group on page 371
2. Configuring the programmable key profile for a primary extension on page 372
3. Configuring the programmable key profile for a member extension on page 372
4. Updating the phone configurations on page 373
5. Viewing SLA configuration details for an extension on page 373

Configuring an SLA group

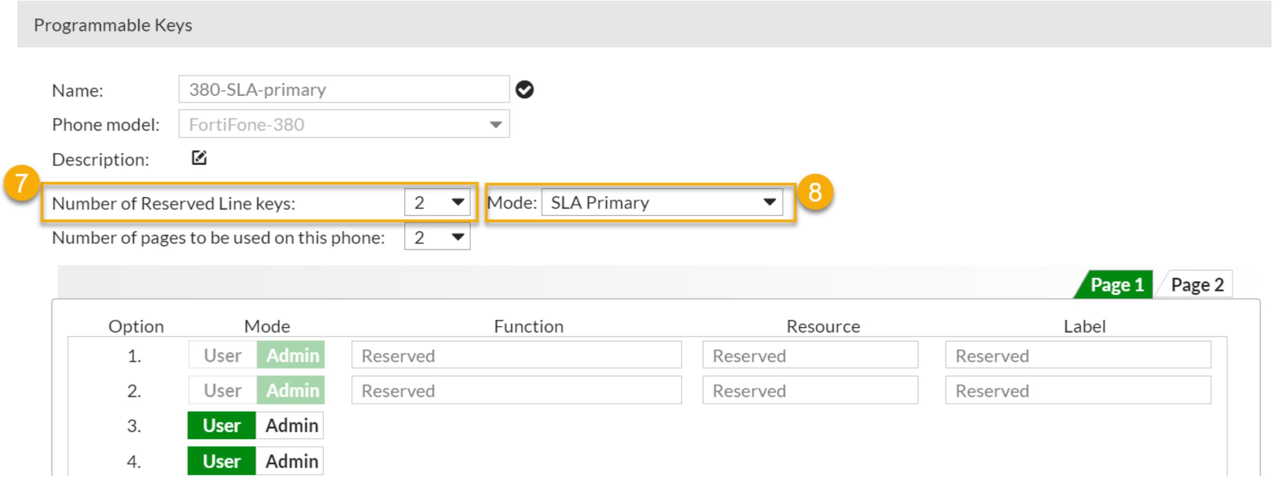
Configure an SLA group to organize the primary and member extensions.

1. Go to *Extension* > *Group* > *SLA Group*.
2. Click *New*.
3. In *Primary*, select 500 (500) Luke.
4. In *Members*, click + and select 101 (101) Diane, 201 (201) John, and 301 (301) Mark.
5. In *Member's Ring Pattern*, select the ring tone that you want to use.
6. In *Ring Mode*, select *Members first then primary*.
7. In *Ring Delay*, select how many seconds you want the assistant phones to ring before an unanswered call starts to ring Luke's phone.
8. Click *Create*.

Configuring the programmable key profile for a primary extension

Configure a programmable key profile for a primary extension and assign an SLA function to one or more programmable phone keys.

1. Go to *Phone System* > *Profile* > *Programmable Keys*.
2. Click *New*.
3. In *Name*, enter a name for this programmable key profile. For example, 380-SLA-primary.
4. Make sure that the *Phone model* shows the correct model. For our example, its FortiFone-380.
5. Click *Create*.
6. Select the profile that you just created and click *Edit*.
7. In *Number of Reserved Line keys*, select the number of lines that you want to have with the SLA function. The maximum is 4. For our example, select 2.
8. In *Mode*, select *SLA Primary*.



Programmable Keys

Name: 380-SLA-primary

Phone model: FortiFone-380

Description:

Number of Reserved Line keys: 2

Mode: SLA Primary

Number of pages to be used on this phone: 2

Page 1 Page 2

Option	Mode	Function	Resource	Label
1.	User Admin	Reserved	Reserved	Reserved
2.	User Admin	Reserved	Reserved	Reserved
3.	User Admin			
4.	User Admin			

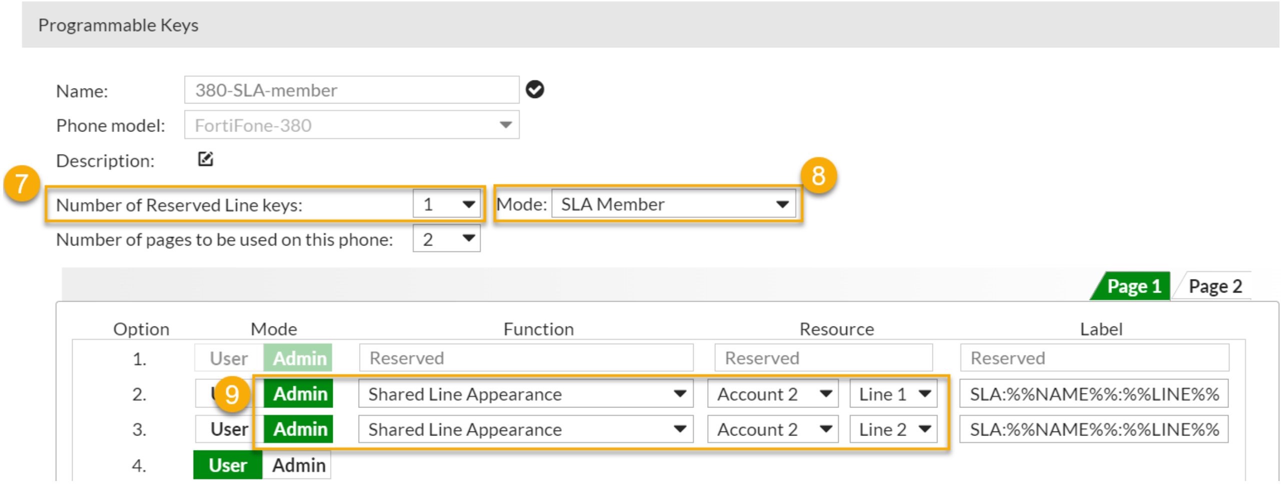
9. Click *OK*.
   FortiVoice has automatically configured the two programmable keys with the SLA feature.
10. To assign the programmable key profile to a primary extension:
    a. Go to *Extension* > *Extension* > *IP Extension*.
    b. Double-click on the primary extension. For example, 500 (Luke).
    c. Go to *Device Setting* > *Programmable keys* and select the profile. For example, 380-SLA-primary.
    d. Click *OK*.
11. To update the phone configuration, wait until you have configured the programmable key profile for the member extensions.

Configuring the programmable key profile for a member extension

Configure a programmable key profile for a member extension and assign an SLA function to one or more of the phone keys.

1. Go to *Phone System* > *Profile* > *Programmable Keys*.
2. Click *New*.
3. In *Name*, enter a name for this programmable key profile. For example, 380-SLA-member.
4. Make sure that the *Phone model* shows the correct model.
5. Click *Create*.

6. Select the profile that you just created and click *Edit*.
7. In *Number of Reserved Line keys*, select 1. This is the member's line.
8. In *Mode*, select *SLA Member*.
9. In the table, add the following two Shared Line Appearance entries (Account 2, Lines 1 and 2):



Programmable Keys

Name: 380-SLA-member

Phone model: FortiFone-380

Description:

Number of Reserved Line keys: 1

Mode: SLA Member

Number of pages to be used on this phone: 2

Page 1 | Page 2

Option	Mode	Function	Resource		Label
1.	User Admin	Reserved	Reserved		Reserved
2.	User Admin	Shared Line Appearance	Account 2	Line 1	SLA:%%NAME%%:%%LINE%%
3.	User Admin	Shared Line Appearance	Account 2	Line 2	SLA:%%NAME%%:%%LINE%%
4.	User Admin				

10. Click *OK*.
11. To assign the programmable key profile to the member extensions:
    a. Go to *Extension* > *Extension* > *IP Extension*.
    b. Double-click on extension 101.
    c. Go to *Device Setting* > *Programmable keys* and select the profile. For our example, it's 380-SLA-member.
    d. Click *OK*.
    e. Repeat steps 11 b. to d. to assign the programmable key profile to the remaining member extensions (201 and 301).

Updating the phone configurations

Update the FortiFone-380 phones with the SLA changes.

1. In the top banner, click the phone maintenance icon .
2. Keep *Type* as *Configuration update*.
3. Keep *All related devices* enabled.
4. To update the phones immediately, click *Now*.
5. To update the phones later, click *At* and schedule a time.
6. Click *OK*.
   When the configuration is complete, the phone screen displays the following message: *Configuration has been updated*.

Viewing SLA configuration details for an extension

1. Go to *Extension* > *Extension* > *IP Extension*.
2. Double-click an extension that is included in an SLA group.
3. In *Device Setting*, click the *SLA* tab.
4. For a primary extension, you can view SLA group settings (*Members*, *Members' Ring Pattern*, and *Ring Mode*)

related to this extension. For a member extension, you can view which SLA group this member is part of.

5. To view programmable key details, click *Phone Keys Preview*.

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.