



FortiVoice™ Enterprise Phone System 4.0.0 Administration Guide



FortiVoice Enterprise Phone System 4.0.0 Administration Guide

February 18, 2015

2nd Edition

Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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 General Counsel, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Introduction.....	8
Registering your Fortinet product.....	8
Customer service & technical support.....	8
Training	8
Documentation	9
Fortinet Tools & Documentation CD	9
Fortinet Knowledge Base	9
Comments on Fortinet technical documentation	9
Scope.....	9
Conventions.....	9
IP addresses	9
Cautions and notes.....	10
Typographical conventions.....	10
Command syntax conventions	11
Connecting to the FortiVoice System.....	14
Connecting to the web-based manager or CLI	14
Connecting to the web-based manager	15
Connecting to the CLI.....	16
Setting up the system using the wizard.....	18
Testing the setup	18
Configuring setups for phone users	19
Accessing the user web portal.....	19
Changing the user PIN	20
Receiving and sending fax.....	20
Using the operator console.....	20
Setting user privileges and preferences	20
Setting the feature codes.....	20
Monitoring the FortiVoice System	21
Viewing overall system status.....	21
Viewing the dashboard	21
Viewing the Call Statistics.....	24
Using the CLI Console	24
Viewing phone system status	24
Viewing active calls.....	24
Viewing parked calls	25
Viewing conference calls	25
Viewing extension status	25
Viewing hot desking configurations	26
Viewing trunk status.....	27
Viewing unassigned phones	27
Viewing DHCP client list	28

Viewing call/fax storage	30
Playing recorded calls.....	30
Viewing current fax accounts.....	30
Viewing archived faxes	30
Viewing fax queues	30
Viewing call records.....	31
Viewing generated reports.....	31
Viewing log messages	32
Displaying and arranging log columns.....	34
Using the right-click pop-up menus	35
Searching log messages.....	36
Viewing phone directories	37
Configuring System Settings.....	38
Configuring network settings.....	38
About IPv6 Support	38
About the management IP	39
About FortiVoice logical interfaces	39
Configuring the network interfaces.....	40
Configuring static routes.....	45
Configuring DNS	46
Configuring DHCP server.....	46
Capturing voice and fax packets	48
Configuring administrator accounts and access profiles	50
Configuring administrator accounts.....	50
Configuring administrator profiles.....	52
Using high availability	53
About high availability	53
About the heartbeat and synchronization.....	55
How to use HA.....	56
Monitoring the HA status	57
Configuring the HA mode and group.....	60
Example: Failover scenarios	67
Configuring system time, system options, SNMP, email setting, and GUI appearance.....	73
Configuring the time and date	74
Configuring system options	78
Configuring SNMP queries and traps	81
Configuring email settings	87
Customizing the GUI appearance.....	89
Managing certificates.....	91
Managing local certificates	92
Obtaining and installing a local certificate	93
Managing certificate authority certificates.....	98
Managing the certificate revocation list	99

Maintaining the system	99
Maintaining the system configuration	99
Downloading a trace file	100
Configuring Phone System Settings.....	101
Configuring phone system settings	101
Setting PBX location and contact information.....	101
Configuring PBX options.....	102
Customizing email history report and notification email templates	105
Configuring advanced phone system settings	109
Configuring SIP settings	109
Configuring SIP phone auto-provisioning.....	111
Adding prompt languages	113
Managing phone configurations	115
Configuring system capacity	116
Managing sound files and music on hold	116
Working with FortiVoice profiles	118
Configuring SIP profiles	118
Modifying caller IDs	120
Scheduling the FortiVoice unit	121
Configuring phone profiles.....	122
Configuring LDAP profiles.....	125
Configuring user privileges	132
Configuring Extensions.....	133
Setting up local extensions.....	133
Configuring IP extensions	133
Modifying analog extension (200D-T model only)	142
Setting up remote extensions	145
Configuring fax extensions	148
Setting extension user preferences	152
Resetting voice messages	159
Creating extension groups.....	159
Creating user groups	159
Creating extension departments.....	160
Creating ring groups	160
Creating page groups	163
Creating pickup groups	164
Setting up general voice mailboxes.....	164
Working with virtual numbers	168
Configuring Trunks.....	170
Setting up VoIP trunks	170
Testing SIP trunks.....	175
Creating a SIP trunk with FortiCall service	176

Modifying PSTN/PRI trunks (200D-T and 2000E-T2 only).....	177
Configuring the T1/E1 span	181
Configuring the analog voice trunk	185
Configuring office peers.....	185
Configuring Call Routing	189
Configuring inbound dial plans	189
Configuring direct inward dialing	193
Mapping DIDs	194
Configuring outbound dial plans.....	196
Testing outbound dial plans.....	198
Creating dialed number match	199
Configuring call handling actions.....	201
Working with Property Management System	203
Configuring hotel management settings.....	203
Configuring hotel room status	204
Configuring Call Features	206
Configuring auto attendants	206
Viewing auto attendant hierarchies.....	209
Configuring key actions	211
Configuring user privileges	213
Configuring account codes.....	218
Mapping speed dials	218
Configuring conference calls	219
Recording calls	221
Configuring call recordings	221
Setting the recorded file format	222
Archiving recorded calls	223
Creating call queues	224
Configuring call parking	230
Configuring fax.....	230
Receiving Faxes.....	231
Sending faxes	232
Configuring other fax settings.....	238
Archiving faxes.....	239
Modifying feature access codes.....	241
Configuring Logs and Reports	244
About FortiVoice logging	244
FortiVoice log types	244
Log message severity levels	245

Configuring logging.....	246
Configuring logging to the hard disk.....	246
Choosing which events to log.....	247
Configuring logging to a Syslog server or FortiAnalyzer unit.....	248
Configuring report profiles and generating call reports	250
Configuring the report query selection	252
Configuring the report time period.....	253
Configuring report email notifications.....	254
Configuring the report schedule	254
Choosing call rate	254
Generating a report manually.....	255
Setting call rates	255
Configuring Station Messaging Detail Record (SMDR)	256
Configuring SMDR settings	256
Setting SMDR formats	256
Configuring alert email.....	257
Configuring alert recipients.....	258
Configuring alert categories.....	258
Installing firmware.....	260
Testing firmware before installing it	260
Installing firmware.....	262
Reconnecting to the FortiVoice unit.....	264
Restoring the configuration.....	265
Verifying the configuration	266
Upgrading	266
Clean installing firmware.....	267
Appendix A: Installing Click-to-Dial software.....	269
Index	270

Introduction

Welcome, and thank you for selecting Fortinet products.

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

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

This document describes how to configure and use the FortiVoice phone system. Only the configuration procedures through the web-based manager are provided. For configuration procedures through the CLI, see the *FortiVoice CLI Reference*.

This topic includes:

- [Registering your Fortinet product](#)
- [Training](#)
- [Documentation](#)
- [Scope](#)
- [Conventions](#)

Registering your Fortinet product

Before you begin, take a moment to register your Fortinet product at the Fortinet Technical Support web site, <https://support.fortinet.com>.

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

For more information, see the Fortinet Knowledge Base article [Registration Frequently Asked Questions](#).

Customer service & technical support

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

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at <https://support.fortinet.com>.

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

Training

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

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at <http://training.fortinet.com>, or email them at training@fortinet.com.

Documentation

The Fortinet Technical Documentation web site, <http://docs.fortinet.com>, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

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

Fortinet Tools & Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, <http://docs.fortinet.com>.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at <http://kb.fortinet.com>.

Comments on Fortinet technical documentation

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

Scope

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

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

Conventions

Fortinet technical documentation uses the following conventions:

- IP addresses
- Cautions and notes
- Typographical conventions
- Command syntax conventions

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, available at <http://ietf.org/rfc/rfc1918.txt?number=1918>.

Cautions and notes

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



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



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

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input	<pre>config system dns set primary <address_ipv4> end</pre>
CLI output	<pre>FGT-602803030703 # get system settings comments : (null) opmode : nat</pre>
Emphasis	HTTP connections are <i>not</i> secure and can be intercepted by a third party.
File content	<pre><HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4></pre>
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com .
Keyboard entry	Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .

Table 1: Typographical conventions in Fortinet technical documentation

Navigation	Go to <i>Monitor > Status > DHCP</i> .
Publication	For details, see the <i>FortiGate Administration Guide</i> .

Command syntax conventions

The command line interface (CLI) requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Table 2: Command syntax notation

Convention	Description
Square brackets []	A non-required word or series of words. For example: <code>[verbose {1 2 3}]</code> indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as: <code>verbose 3</code>

Table 2: Command syntax notation

Angle brackets < >	<p>A word constrained by data type.</p> <p>To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (<code>_</code>) and suffix that indicates the valid data type. For example:</p> <p><code><retries_int></code></p> <p>indicates that you should enter a number of retries, such as 5.</p> <p>Data types include:</p> <ul style="list-style-type: none">• <code><xxx_name></code>: A name referring to another part of the configuration, such as <code>policy_A</code>.• <code><xxx_index></code>: An index number referring to another part of the configuration, such as 0 for the first static route.• <code><xxx_pattern></code>: A regular expression or word with wild cards that matches possible variations, such as <code>*@example.com</code> to match all email addresses ending in <code>@example.com</code>.• <code><xxx_fqdn></code>: A fully qualified domain name (FQDN), such as <code>mail.example.com</code>.• <code><xxx_email></code>: An email address, such as <code>admin@mail.example.com</code>.• <code><xxx_url></code>: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as <code>http://www.fortinet.com/</code>.• <code><xxx_ipv4></code>: An IPv4 address, such as <code>192.168.1.99</code>.• <code><xxx_v4mask></code>: A dotted decimal IPv4 netmask, such as <code>255.255.255.0</code>.• <code><xxx_ipv4mask></code>: A dotted decimal IPv4 address and netmask separated by a space, such as <code>192.168.1.99 255.255.255.0</code>.• <code><xxx_ipv4/mask></code>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as <code>192.168.1.99/24</code>.• <code><xxx_ipv6></code>: A colon (<code>:</code>)-delimited hexadecimal IPv6 address, such as <code>3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234</code>.• <code><xxx_v6mask></code>: An IPv6 netmask, such as <code>/96</code>.• <code><xxx_ipv6mask></code>: An IPv6 address and netmask separated by a space.• <code><xxx_str></code>: A string of characters that is not another data type, such as <code>P@ssw0rd</code>. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences.• <code><xxx_int></code>: An integer number that is not another data type, such as 15 for the number of minutes.
---------------------------------	---

Table 2: Command syntax notation

Curly braces { }	<p>A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces.</p> <p>You must enter at least one of the options, unless the set of options is surrounded by square brackets [].</p>
Options delimited by vertical bars 	<p>Mutually exclusive options. For example:</p> <pre>{enable disable}</pre> <p>indicates that you must enter either <code>enable</code> or <code>disable</code>, but must not enter both.</p>
Options delimited by spaces	<p>Non-mutually exclusive options. For example:</p> <pre>{http https ping snmp ssh telnet}</pre> <p>indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:</p> <pre>ping https ssh</pre> <p>To change the options, you must re-type the entire list. For example, to add <code>snmp</code> to the previous example, you would type:</p> <pre>ping https snmp ssh</pre> <p>If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.</p>

Connecting to the FortiVoice System

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

This topic includes:

- [Connecting to the web-based manager or CLI](#)
- [Setting up the system using the wizard](#)
- [Testing the setup](#)
- [Configuring setups for phone users](#)

Connecting to the web-based manager or CLI

There are two methods to connect to the FortiVoice unit:

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

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

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

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



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

After you connect, you can use the web-based manager or CLI to configure basic network settings and access the CLI and/or web-based manager through your network. However, if you want to update the firmware, you may want to do so before continuing. See [“System Information widget”](#) on page 22.



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

This topic includes:

- [Connecting to the web-based manager](#)
- [Connecting to the CLI](#)

Connecting to the web-based manager

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

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

Table 3: Default settings for connecting to the web-based manager

Network Interface	port1
URL	https://192.168.1.99/admin
Administrator Account	admin
Password	(none)

To connect to the web-based manager

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 with a netmask of 255.255.255.0.
2. Using the Ethernet cable, connect your computer's Ethernet port to the FortiVoice unit's port1.
3. Start your browser and enter the URL <https://192.168.1.99/admin>. (Remember to include the "s" in https://.)

To support HTTPS authentication, the FortiVoice unit ships with a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiVoice unit. When you connect, depending on your web browser and prior access of the FortiVoice unit, your browser might display two security warnings related to this certificate:

- The certificate is not automatically trusted because it is self-signed, rather than being signed by a valid certificate authority (CA). Self-signed certificates cannot be verified with a proper CA, and therefore might be fraudulent. You must manually indicate whether or not to trust the certificate.
- The certificate might belong to another web site. The common name (CN) field in the certificate, which usually contains the host name of the web site, does not exactly match the URL you requested. This could indicate server identity theft, but could also simply indicate that the certificate contains a domain name while you have entered an IP address. You must manually indicate whether this mismatch is normal or not.

Both warnings are normal for the default certificate.

4. Verify and accept the certificate, either permanently (the web browser will not display the self-signing warning again) or temporarily. You cannot log in until you accept the certificate. For details on accepting the certificate, see the documentation for your web browser.
5. In the *Name* field, type `admin`, then click *Login*. (In its default state, there is no password for this account.)

Login credentials entered are encrypted before they are sent to the FortiVoice unit. If your login is successful, the web UI appears. To continue by updating the firmware, see "[System Information widget](#)" on [page 22](#). Otherwise, to continue by following the configuration wizard.

Connecting to the CLI

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

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

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

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

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

- a computer with an RJ-45 Ethernet port
- a crossover Ethernet cable
- an SSH client, such as [PuTTY](#)

Table 4: Default settings for connecting to the CLI by SSH

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



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

For more information on available CLI commands, see the [FortiVoice CLI Reference](#).



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

To connect to the CLI using a local serial console connection

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

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

8. Press Enter.

The terminal emulator connects to the CLI and the CLI displays a login prompt.

9. Type `admin` and press Enter twice. (In its default state, there is no password for this account.)

The CLI displays a prompt, such as:

```
FortiVoice #
```

10. Type `admin` and press Enter twice. (In its default state, there is no password for this account.)

The CLI displays the following text:

```
Type ? for a list of commands.
```

You can now enter commands. For information about how to use the CLI, including how to connect to the CLI using SSH or Telnet, see the [FortiVoice CLI Reference](#).



The following procedure uses [PuTTY](#). Steps may vary with other SSH clients.

To connect to the CLI using an SSH connection

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 with a netmask of 255.255.255.0.
2. Using the Ethernet cable, connect your computer's Ethernet port to the FortiVoice unit's port1.
3. Verify that the FortiVoice unit is powered on.
4. On your management computer, start your SSH client.
5. In *Host Name (or IP Address)*, type 192.168.1.99.
6. In *Port*, type 22.
7. From *Connection type*, select *SSH*.
8. Select *Open*.

The SSH client connects to the FortiVoice unit.

The SSH client may display a warning if this is the first time you are connecting to the FortiVoice unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiVoice unit but it used a different IP address or SSH key. If your management computer is directly connected to the FortiVoice unit with no network hosts between them, this is normal.

9. Click *Yes* to verify the fingerprint and accept the FortiVoice unit's SSH key. You cannot log in until you accept the key.

The CLI displays a login prompt.

10. Type `admin` and press Enter twice. (In its default state, there is no password for this account.)

The CLI displays the following text:

Type `?` for a list of commands.

You can now enter commands. For information about how to use the CLI, including how to connect to the CLI using SSH or Telnet, see the [FortiVoice CLI Reference](#).

Setting up the system using the wizard

The FortiVoice unit's *Configuration Wizard* leads you through required configuration steps, helping you to quickly set up your FortiVoice system. Once the setup is complete, you can make phone calls through the FortiVoice unit.

While all settings configured by the *Configuration Wizard* can also be configured through the web-based manager, the wizard presents each setting in the necessary order.

The wizard is a reusable tool and you can modify the configuration settings. Each time you click the *Next* button, the configuration is saved.



To start the wizard, open the web-based manager in a browser and click *Wizard* in the top-right button row.

Testing the setup

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



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

If you make a office peer test call, make sure that your FortiVoice unit and the peer office PBX are mutually registered. For more information, see [“Configuring office peers” on page 185](#).

Depending on the phone you use, the procedure to connect the phone may vary. Refer to the phone user manuals for instructions.

Generally, you need to configure the following on the phone after powering it up and connecting it to the network:

- Enter the IP address of the phone if it is not DHCP-enabled.
- Enter the SIP server IP address and port number (5060 by default) of the FortiVoice unit. You can find the SIP serve IP by the *Configuration Wizard* and going to *System Setting > Network Setting*.
- Enter the extension number and SIP password you have configured and make sure the extension is enabled. You can find the information by opening the *Configuration Wizard* and going to *Extension > Import/Add/Edit* and double-click an extension.

If you have not imported or added any extensions, do it first. For more information, see [“Configuring IP extensions” on page 133](#). The extension number on the FortiVoice unit and your phone should match.

Configuring setups for phone users

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

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

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

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

This topic includes:

- [Accessing the user web portal](#)
- [Changing the user PIN](#)
- [Receiving and sending fax](#)
- [Using the operator console](#)
- [Setting user privileges and preferences](#)
- [Setting the feature codes](#)

Accessing the user web portal

FortiVoice user web portal is a special web site located on a FortiVoice unit. This web portal allows a phone user to:

- check your voicemail including playing, deleting, or saving the voicemails
- receive and send fax
- Use the agent console to manage queue calls
- Use the operator console to process company calls
- check your call record for received, placed, or missed calls
- check your recorded calls including playing, deleting, or saving the voicemails
- view your corporate phone directory
- check the feature codes that you can dial on your phone keypad
- configure your extension according to your preferences
- manage calls
- configure phone profiles
- customize sound files

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

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

- the web portal URL (same with that of the FortiVoice unit except without `/admin` in the end)
- their extension numbers, and
- the default user PINs.

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

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

For information on adding extension numbers and user PINs, see [“Configuring IP extensions” on page 133](#).

Changing the user PIN

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

Receiving and sending fax

Inform the phone users that they can receive and send faxes on the user web portal. For more information, see [“Configuring fax” on page 230](#).

Using the operator console

If you have enabled the operator role for an extension, inform the extension user so that the user can process corporate calls on the user web portal. For more information, see [“Operator role” on page 214](#).

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 213](#) and [“Setting extension user preferences” on page 152](#).

Setting the feature codes

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

For details, see [“Modifying feature access codes” on page 241](#).

Monitoring the FortiVoice System

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

This topic includes:

- Viewing overall system status
- Viewing phone system status
- Viewing call/fax storage
- Viewing call records
- Viewing generated reports
- Viewing log messages
- Viewing phone directories

Viewing overall system status

The *Status* menu displays system status, most of which pertain to the entire system, such as service status and system resource.

This topic includes:

- Viewing the dashboard
- Viewing the Call Statistics
- Using the CLI Console

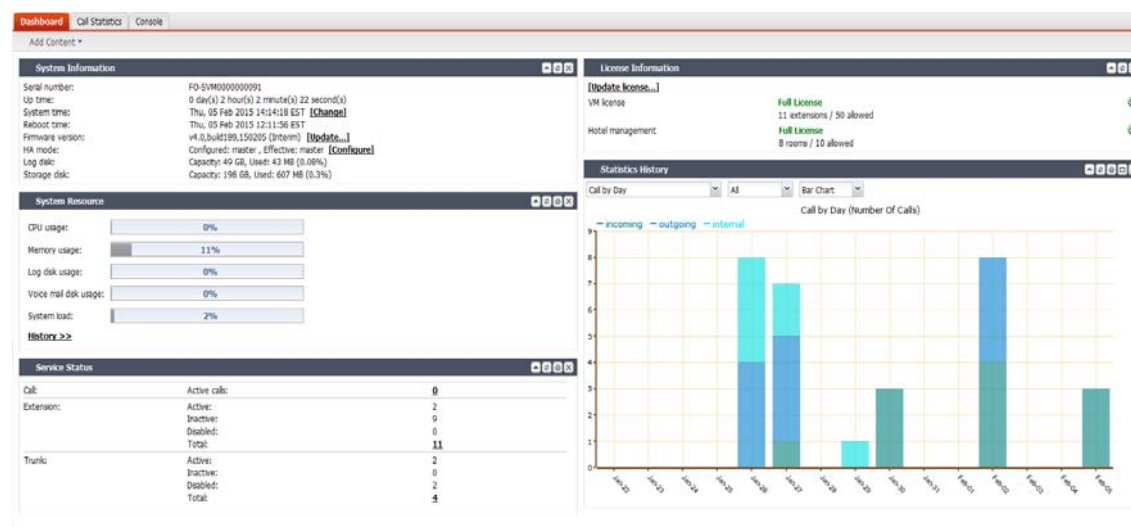
Viewing the dashboard

Status > Dashboard displays first after you log in to the web-based manager. It contains a dashboard with widgets that each indicates 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, service status, firmware version, system time, and statistics history.

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

Figure 1: Monitor system status



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, in the upper left-hand corner, click *Add Content*, then mark the check boxes of widgets that you want to show.

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

Figure 2: A minimized widget on the dashboard



System Information widget

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

In addition to displaying basic system information, the *System Information* widget lets you change the firmware. To change the firmware, click *Update* for *Firmware version*. For more information, see "Installing firmware" on page 260.

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

License Information widget

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

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

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



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

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

Service Status widget

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

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

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

- *Connected*: The port is connected to a device.
- *Disconnected*: The port is not connected to any device and is ready for use.
- *Alarmed*: The port has an error and is not usable.
- *Occupied*: The port is being used.

System Resource widget

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

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

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

Statistics History widget

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

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

Also see [“Viewing the Call Statistics” on page 24](#).

System Command widget

The *System Command* widget lets you restart, shut down, or reload the configuration of the FortiVoice unit.

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

Before rebooting or halting the FortiVoice unit, consider notifying your phone users, as it could result in temporary interruptions to connectivity.

Reloading allows the FortiVoice unit to reload its configuration from its last saved version, and log you out. Any changes that were in progress but not yet saved, such as GUI pages that were not applied or CLI commands where you had not yet entered `next` or `end`, are lost. If you want to continue configuring the FortiVoice unit, refresh your browser and log in again.

Recent Calls widget

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

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

The maximum call records shown is 8.

Viewing the Call Statistics

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

To view call statistics, go to *Status > Dashboard > Call Statistics*.

Using the CLI Console

Go to *Status > Dashboard > Console* to access the CLI without exiting from the web-based manager.

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

For more information about CLI commands, see the [FortiVoice CLI Reference](#).

Viewing phone system status

Status > Phone System displays all the ongoing phone calls, parked calls, conference calls, extensions, trunks, call queues, DHCP clients, and unassigned phones.

This topic includes:

- [Viewing active calls](#)
- [Viewing parked calls](#)
- [Viewing conference calls](#)
- [Viewing extension status](#)
- [Viewing hot desking configurations](#)
- [Viewing trunk status](#)
- [Viewing unassigned phones](#)
- [Viewing DHCP client list](#)

Viewing active calls

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

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

The call statuses include:

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

Viewing parked calls

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

To view parked calls, go to *Status > Phone System > Parked Calls*.

For more information on call parking, see [“Configuring call parking” on page 230](#).

Viewing conference calls

Status > 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* icon.

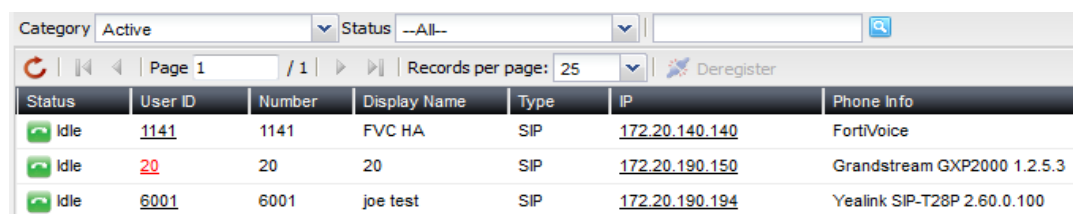
For more information, see [“Configuring conference calls” on page 219](#).

Viewing extension status

Status > Phone System > Extensions displays all the extensions in realtime, including their statuses, IDs, numbers, display names, types, IPs for SIP extensions, and phone information.

For more information, see [“Configuring Extensions” on page 133](#).

Figure 3: Viewing extension status



Status	User ID	Number	Display Name	Type	IP	Phone Info
Idle	1141	1141	FVC HA	SIP	172.20.140.140	FortiVoice
Idle	20	20	20	SIP	172.20.190.150	Grandstream GXP2000 1.2.5.3
Idle	6001	6001	joe test	SIP	172.20.190.194	Yealink SIP-T28P 2.60.0.100

GUI field	Description
Category/Status	Select to view the extensions by categories. Each category has its corresponding statuses. <ul style="list-style-type: none">All: Displays extensions in all statuses.Active: Can display extensions in each of the following statuses once selected:<ul style="list-style-type: none">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.Other: The status other than the above.Inactive: Can display extensions in each of the following statuses once selected:<ul style="list-style-type: none">Not registered: The extension is not registered with the FortiVoice unit and is not in service.Unavailable: The extension is not reachable.Disable: Displays all disabled extensions.
Deregister	Select an extension and click this icon to remove the extension assigned to the phone.
Status	The status of the extension. See “Category/Status” on page 26.
User ID	This is the system-generated ID based on the extension number.
Number	The extension number.
Display Name	The name displaying on the extension. This is usually the name of the extension user.
Type	The type for this extension, such as SIP or analog (for the FortiVoice 200D-T and 2000E-T2 models).
IP	The link to the IP address of the phone using the extension number. Click to interface with the extension and configure it remotely by entering the login information. See “IP” on page 140.
Phone Info	The phone brand and model.

Viewing hot desking configurations

Status > Phone System > Hot Desking displays all of the extensions configured for hot desking,

including:

- *Status*: the status of the hot desking extension: logged in or logged out.
- *User ID*: the system-generated ID for the hot desking extension.
- *Number*: the hot desking extension number.
- *Display Name*: the name displayed on the hot desking extension.
- *Host Device*: the extension number or MAC address (for a unassigned phone) of the phone that a hot desking user logs into.
- *Last Login*: the last login time at the host device.
- *Expiry*: the login expiry time.

Hot desking enables users to log into another phone. However, unlike using Follow Me or Call Forwarding which simply redirect a user's calls to another user's phone, hot desking takes total control of another phone by applying all of the user's own phone 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.

For information on configuring hot desking, see [“Hot-desking” on page 217](#).

Viewing trunk status

Status > Phone System > Trunks displays all the trunks in realtime, including their names, IPs, types, statuses, and registration/connection status with the VoIP or PSTN service provider.

The trunk statuses include:

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

When you click the IP address of a SIP extension, you can interface with the extension and configure it remotely.

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

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

For more information, see [“Configuring Trunks” on page 170](#).

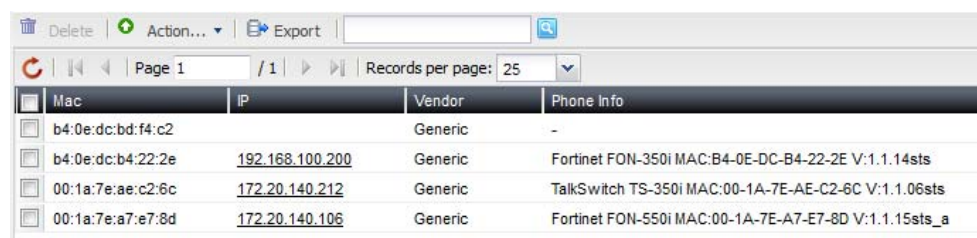
Viewing unassigned phones

Status > Phone System > Unassigned Phone lists the supported phones auto-discovered by the FortiVoice unit but not assigned to any extensions yet.

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

After assigning an extension to the phone, the extension's full configuration file will be sent to the phone if the auto-provisioning option is selected in the user privilege applied to the extension. For details, see [“Setting up local extensions” on page 133](#) and [“Configuring user privileges” on page 213](#).

Figure 4: Unassigned phones



Mac	IP	Vendor	Phone Info
b4:0e:dc:bd:f4:c2		Generic	-
b4:0e:dc:b4:22:2e	192.168.100.200	Generic	Fortinet FON-350i MAC:B4-0E-DC-B4-22-2E V:1.1.14sts
00:1a:7e:ae:c2:6c	172.20.140.212	Generic	TalkSwitch TS-350i MAC:00-1A-7E-AE-C2-6C V:1.1.06sts
00:1a:7e:a7:e7:8d	172.20.140.106	Generic	Fortinet FON-550i MAC:00-1A-7E-A7-E7-8D V:1.1.15sts_a

GUI field	Description
Action	<ul style="list-style-type: none">• <i>Assign to new extension:</i> Select an unassigned phone and click this option to add an extension and assign this client to the user at the same time. The phone record disappears from the <i>Unassigned Phone</i> list. For more information, see “To assign a new extension user to an unassigned phone” on page 28.• <i>Apply to existing extension:</i> Select an unassigned phone and click this option to assign this client to an existing user. The phone record disappears from the <i>Unassigned Phone</i> list. For more information, see “To assign an existing extension user to an unassigned phone” on page 28.
Export	Select to save the unassigned phone list in <code>csv</code> format.
MAC	The Media Access Control address (MAC address) of the unassigned phone.
IP	The IP address of the unassigned phone assigned by the FortiVoice unit.
Vendor	The brand name of the unassigned phone.
Phone Info	The phone brand and model.

To assign a new extension user to an unassigned phone

1. Go to *Status > Phone System > Unassigned Phone*.
2. Select an unassigned phone.
3. Click *Action* and select *Assign to new extension*.
4. Configure the extension associated with the unassigned phone following [“Configuring IP extensions”](#) on page 133.
5. Click *Create*.

To assign an existing extension user to an unassigned phone

1. Go to *Status > Phone System > Unassigned Phone*.
2. Select an unassigned phone.
3. Click *Action* and select *Assign to existing extension*.
4. Select the extension to associate with the unassigned phone.
5. Click *Apply to existing extension*.

Viewing DHCP client list

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

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

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

- In the FortiVoice DHCP server configuration, select DHCP option 66 (an advanced option on the web-based manager) and include the IP address of the FortiVoice interface connected to the same network as the SIP phones to be auto-provisioned. For more information, see [“Configuring DHCP server” on page 46](#).

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 46](#).
- 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.

Figure 5: DHCP client list

Export						
Page 1 / 2 Records per page: 25						
Mac	Interface	IP	Expired	Vendor	Extension	Configuration Status
00:30:4f:74:5d:f1	port1	172.20.190.172	2014-02-26 08:21:03	FortiFone-110	7608	Not assigned
00:0f:8f:4a:29:c5	port1	172.20.190.229	2014-02-25 19:16:37	Generic	7528	Not assigned
00:0f:34:ec:b9:cf	port1	172.20.190.228	2014-02-25 19:07:23	Generic	7819	Misconfigured
00:0b:82:0e:f8:b4	port1	172.20.190.218	2014-02-25 05:20:01	Grandstream	7417	OK

GUI field	Description
Export	Select to save the DHCP client list in <code>csv</code> format.
MAC	The Media Access Control address (MAC address) of the DHCP client.
Interface	The FortiVoice unit port to which the DHCP client connects. For information on FortiVoice interfaces, see “Configuring network settings” on page 38 .
IP	The IP address of the DHCP client assigned by the FortiVoice DHCP server.
Expired	The expiration time of the DHCP client IP address.
Vendor	The brand names of the DHCP clients.
Extension	When a DHCP-enabled device connects to the FortiVoice unit, the FortiVoice unit assigns a temporary ID to the device if it is a supported device. If an extension number is assigned to the phone, the extension number appears. For information on assigning extensions, see “Viewing unassigned phones” on page 27 .
Configuration Status	<ul style="list-style-type: none"> • <i>OK</i>: The DHCP client is assigned to a new or an existing extension user. • <i>Not assigned</i>: The DHCP client is not assigned to a new or an existing extension user. • <i>Misconfigured</i>: The DHCP client's configuration has errors.

Viewing call/fax storage

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

This topic includes:

- [Playing recorded calls](#)
- [Viewing current fax accounts](#)
- [Viewing archived faxes](#)
- [Viewing fax queues](#)

Playing recorded calls

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

To listen to a call, go to *Status > Storage > Recorded Calls* and select a call record folder to open the archived call files. Select a call file and click the *Play* button.

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

To search the locally archived calls, click *Search*.

For information on configuring recording calls, see [“Recording calls” on page 221](#).

Viewing current fax accounts

The *Fax* tab lists the fax accounts created on the FortiVoice unit. For more information about creating fax accounts, see [“Configuring fax” on page 230](#).

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

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

Viewing archived faxes

The *Fax Archive* tab lists the faxes sent and received through the FortiVoice unit. For more information about fax, see [“Configuring fax” on page 230](#).

To view fax configurations, go to *Status > Storage > Fax Archive*. The fax configurations are listed with their names, numbers, storage sizes, and faxes stored.

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

To search the locally archived faxes, click *Search*.

Viewing fax queues

The *Fax Queue* tab lists the faxes waiting to be sent on the FortiVoice unit. For more information about fax, see [“Configuring fax” on page 230](#).

You can also click *Download PDF* to save a fax in queue.

Viewing call records

Status > Call Detail Records (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, and call type.

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

You can filter the call records display by clicking the *Search* button and enter criteria that records must match in order to be visible. You can also save the call records by clicking the *Download* button.

Viewing generated reports

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

FortiVoice units can generate reports automatically according to the report schedules that you configure. For more information, see [“Configuring report profiles and generating call reports” on page 250](#).

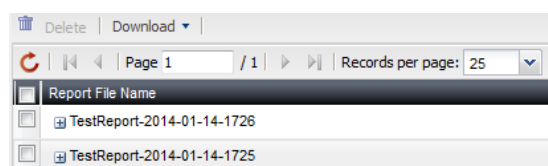


To reduce the amount of hard disk space consumed by reports, regularly download then delete generated reports from the FortiVoice unit.

To view call or call center reports

1. Go to *Status > Call Reports > Reports/Call Center Reports*.

Figure 6: Reports tab



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

2. To view the report in PDF file format, mark the check box in the corresponding row 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, mark the check box in the row corresponding to the report, such as 1-2012-03-31-2112, then click *Download* and select *Download HTML*. Your browser downloads a file with an archive (.tgz.gz) file extension to your management computer. To view the report, first extract the report files from the archive, then open the HTML files in your web browser.
 - Each *Query Selection* in the report becomes a separate HTML file. You can view the report as individual HTML files. In the row corresponding to the report that you want to view, click + next to the report name to expand the list of sections, then double-click the file name of the section that you want to view, such as report1.html. The report appears in a new browser window.

Viewing log messages

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

Logs stored remotely cannot be viewed from the web-based manager of the FortiVoice unit. If you want to view logs from the web-based manager, also enable local storage. For details, see “Configuring Logs and Reports” on page 244.

Status > Logs displays the logs of administrator activities and system events as well as voice, fax, and queue.

To view the list of log files and their contents

1. Go to *Status > Logs > Event/Voice/Fax/Queue*.

The list of log files appears with the beginning and end of a log file's time range and the size of a log file in bytes. The queue log files display more information.

2. To download an event, voice, and fax log file, select it and click *Download* to save it in one of the three formats:

- *Normal Format* for a log file that can be viewed with a plain text editor such as Microsoft Notepad.
- *CSV Format* for a comma-separated value (.csv) file that can be viewed in a spreadsheet application such as Microsoft Excel or OpenOffice Calc.
- *Compressed Format* for a plain text log file like *Normal Format*, except that it is compressed and stored within a .gz archive.

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 36](#).

4. To view messages contained in logs, double-click a log file.

To view the current page's worth of the log messages as an HTML table, right-click and select *Export to Table*. The table appears in a new tab. To download the table, click and drag to select the whole table, then copy and paste it into a rich text editor such as Microsoft Word or OpenOffice Writer.

Log messages can appear in either raw or formatted views.

- Raw view displays log messages exactly as they appear in the plain text log file.
- Formatted view displays log messages in a columnar format. Each log field in a log message appears in its own column, aligned with the same field in other log messages, for rapid visual comparison.

By default, log messages always appear in columnar format, with one log field per column. However, when viewing this columnar display, you can also view the log message in raw format by hovering your mouse over the index number of the log message, in the # column, as shown in [Figure 7](#).

Figure 7: Log message view

The screenshot shows a web interface for viewing log messages. At the top, there are controls for 'Level' (set to Information), 'Go to line', 'Search...', and 'Back'. Below these are navigation buttons (back, forward, first, last), 'Page 1 / 3', 'Records per page: 25', and a 'Save View' button. The main content area displays a table of log messages. The first view, 'Log message in raw format', shows a single message with its full details in a text area. The second view, 'Log message in columnar format', shows a table with columns for #, Date, Time, and Message. The table contains 12 rows of log messages, with the first row selected.

#	Date	Time	Message
1	2014-02-20	10:39:35	Fax from 'hao operator <6003>' to '6136881237': 'sent success
2	2014-02-20	10:04:11	Fax from " to ": 'sending failed. Extra Info: {Status String = The c
3	2014-02-20	10:04:11	Fax from 'hao operator <6003>' to '6136881237': 'sending failed
4	2014-02-20	10:01:10	Fax from 'Fortinet Techno' <6132259381>' to 'freephone8423': 'r
5	2014-02-20	09:55:51	Fax from "" <6132259381>' to 'freephone8423': 'receiving FAX fa
6	2014-02-20	05:00:01	Expired '2' faxes from 'inbox' folder for extension '6003'
7	2014-02-20	05:00:01	Expired '2' faxes from 'sent' folder for extension '6003'
8	2014-02-20	05:00:01	Expired '2' faxes from 'sent' folder for extension '6003'
9	2014-02-20	05:00:01	Expired '2' faxes from 'sent' folder for extension '6003'
10	2014-02-20	05:00:01	Expired '2' faxes from 'sent' folder for extension '6003'
11	2014-02-20	05:00:01	Expired '2' faxes from 'sent' folder for extension '6003'
12	2014-02-19	15:11:43	Fax from 'hao operator <6003>' to '6136881237': 'sent success

Log message in raw format

Log message in columnar format

The log messages vary by levels. For more information, see [“Configuring Logs and Reports” on page 244](#).

The log messages are also filtered by subtypes:

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

You can click the *Save View* button to save the 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 36](#).

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.

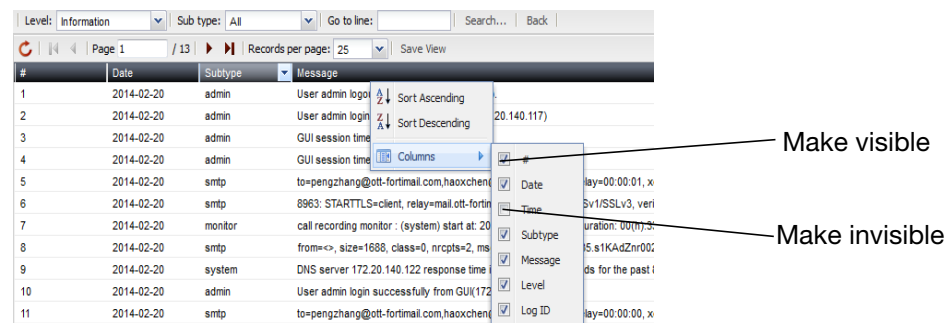
Depending on your currently selected theme:

- 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 *Status > Logs > Event/Voice/Fax/Queue/Hotel*.
2. Double-click the row corresponding to time period whose log messages you want to view.
3. Position your mouse cursor over a column heading to display the down arrow on its right-hand side, click the down arrow and move your cursor over *Columns* to display the list of available columns, then mark the check boxes of columns that you want to display.

Figure 8: Hiding and showing log columns



4. Click *Save View*.

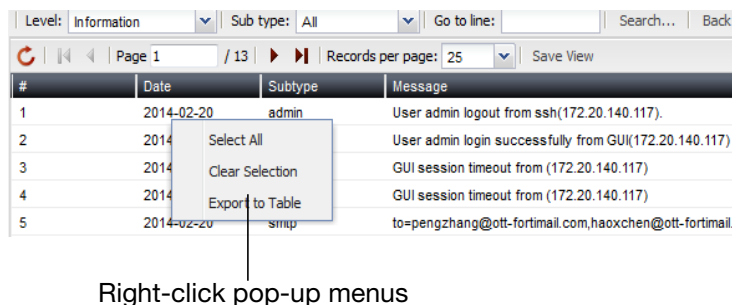
To change the order of the columns

1. Go to *Status > Logs > Event/Voice/Queue/Hotel*.
2. Double-click the row corresponding to time period whose log messages you want to view.
3. For each column whose order you want to change, click and drag its column heading to the left or right.
4. Click *Save View*.

Using the right-click pop-up menus

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

Figure 9: Using the right-click menus on log reports



Right-click pop-up menus

Table 5: Log report right-click menu options

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 to Table	Select to export the selected log messages to a table format. A new tab named <i>Exported Table</i> appears, displaying the exported information. The table format allows you to copy the information and paste it elsewhere.

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 *Status > Logs > Event/Voice/Fax/Queue/Hotel*.
2. To search **all** log files, click *Search*.
3. To search **one** of the log files, first double-click the name of a log file to display the contents of the log file, then click *Search*.

Figure 10: Log search dialog

FortiVoice
seconds for the past 8 DNS UDP request

Event Log Search

Keyword:

Message:

Log ID:

Time: and hour(s) before

Match condition:

4. Enter your search criteria by configuring one or more of the following:

GUI field	Description
Keyword	Enter any word or words to search for within the log messages. For example, you might enter GUI session to locate all log messages containing that exact phrase in any log field.
Message	Enter all or part of the <i>Message</i> log field.
Log ID	Enter all or part of the log ID in the log message.

Time	<p>Select the time span of log messages to include in the search results.</p> <p>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.</p>
Match condition	<ul style="list-style-type: none"> • <i>Contain</i>: searches for the exact match. • <i>Wildcard</i>: supports wildcards in the entered search criteria.

5. Click *Apply*.

The FortiVoice unit searches your currently selected log file for log messages that match your search criteria, and displays any matching log messages.

Viewing phone directories

The *Directory* tab displays the local, remote, and peer office extensions. It also shows the virtual numbers and ring groups.

To display the peer office extensions, you need to enable fetching office directory on the local and peer office FortiVoice units. For more information, see [“Configuring office peers” on page 185](#).

To view or download the phone directory, go to *Status > Directory*.








Figure 11: Viewing directory

Search:

Clear Search

Type: --All--

Location: --All--

   Page 1 / 2   Records per page: 25  Download 

Number	Display Name	Location	Type
*	*	Local	Analog
1141	FVC HA	Local	Sip
190	190	Local	Sip
191	Operator_test	Local	Sip

GUI field	Description
Download	Select to save all directories or search result.
Number	The extension number. For information on creating extension numbers, see “Setting up local extensions” on page 133 .
Display Name	The name displaying on the extension. This is usually the name of the extension user.
Office	The name of the remote office trunk. For more information, see “Configuring office peers” on page 185 .
Type	The extension type.

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](#)
- [Configuring administrator accounts and access profiles](#)
- [Using high availability](#)
- [Configuring system time, system options, SNMP, email setting, and GUI appearance](#)
- [Managing certificates](#)
- [Maintaining the system](#)

Configuring network settings

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

This topic includes:

- [About IPv6 Support](#)
- [About the management IP](#)
- [About FortiVoice logical interfaces](#)
- [Configuring the network interfaces](#)
- [Configuring static routes](#)
- [Configuring DNS](#)
- [Configuring DHCP server](#)
- [Capturing voice and fax packets](#)

About IPv6 Support

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

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

The FortiVoice unit supports the following IPv6 features:

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

About the management IP

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

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

You can access the web-based manager and the FortiVoice user account using the management IP address. For details, see [“Connecting to the web-based manager” on page 15](#).

About FortiVoice logical interfaces

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

- [VLAN subinterfaces](#)
- [Redundant interfaces](#)
- [Loopback interfaces](#)

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 40](#).

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 40](#).

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 40](#).

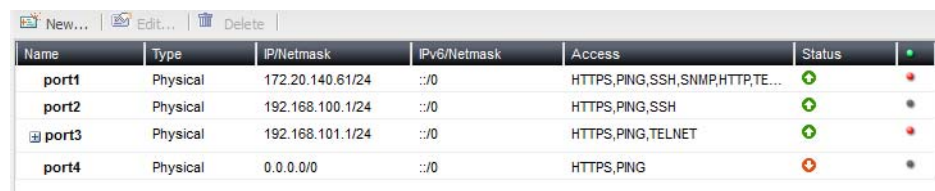
Configuring the network interfaces

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 39](#), and [“Editing network interfaces” on page 41](#).

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

Figure 12: Network tab



Name	Type	IP/Netmask	IPv6/Netmask	Access	Status	
port1	Physical	172.20.140.61/24	::/0	HTTPS,PING,SSH,SNMP,HTTP,TE...	Up	●
port2	Physical	192.168.100.1/24	::/0	HTTPS,PING,SSH	Up	●
port3	Physical	192.168.101.1/24	::/0	HTTPS,PING,TELNET	Up	●
port4	Physical	0.0.0.0/0	::/0	HTTPS,PING	Down	●

GUI field	Description
Name	Displays the name of the network interface, such as <i>port1</i> .

Type	Displays the interface type: physical, VLAN, redundant, or loopback. For details, see “About FortiVoice logical interfaces” on page 39.
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 38.
Access	Displays the administrative access and phone user access that are enabled on the network interface, such as HTTPS for the web-based manager.
Status	<p>Indicates the up (available) or down (unavailable) administrative status for the network interface.</p> <ul style="list-style-type: none"> • <i>Green up arrow</i>: The network interface is up and can receive traffic. • <i>Red down arrow</i>: The network interface is down and cannot receive traffic. <p>To change the administrative status (that is, bring up or down a network interface), see “Editing network interfaces” on page 41.</p>

Editing network interfaces

You can edit FortiVoice’s physical network interfaces to change their IP addresses, netmasks, administrative access protocols, and other settings. 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 50.](#)

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:

Edit Interface

Interface name: port1 (50:e5:49:e8:e3:92)

Addressing Mode

☒ Manual

IP/Netmask: /

IPv6/Netmask: /

☐ DHCP Update request

Access: ☒ HTTPS ☒ PING ☒ HTTP

☒ SSH ☒ SNMP ☒ TELNET

MTU: ☐ Override default MTU value (1500)

(bytes)

Administrative status: ☒ Up ☐ Down

OK Cancel

Interface name:

Type:

VLAN

Interface:

port1

VLAN ID:

0

Addressing Mode

☒ Manual

IP/Netmask:

0.0.0.0

/

0

IPv6/Netmask:

::

/

0

☐ DHCP

Update request

Access

☐ HTTPS
 ☐ PING
 ☐ HTTP

☐ SSH
 ☐ SNMP
 ☐ TELNET

MTU

1500

(bytes)

Administrative status

☒ Up
 ☐ Down

Create

Cancel

<i>GUI field</i>	<i>Description</i>
Interface Name	<p>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.</p> <p>If you are creating a logical interface, enter a name for the interface.</p>

Type	<p>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 39.</p> <ul style="list-style-type: none"> • <i>VLAN</i>: 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. • <i>Redundant</i>: If you want to create a redundant interface, select the interface members from the available interfaces. Usually, you need to include two or more interfaces as the redundant interface members. • <i>Loopback</i>: 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	<ul style="list-style-type: none"> • <i>Manual</i>: Select to enter the IP address or IPv6 address and netmask for the network interface in <i>IP/Netmask</i> or <i>IPv6/Netmask</i>. • <i>DHCP</i>: Select and click <i>Update request</i> to retrieve a dynamic IP address using DHCP.

Access

Enable protocols that this network interface should accept for connections **to** the FortiVoice unit itself. (These options do not affect connections that will travel **through** the FortiVoice unit.)

- **HTTPS:** Enable to allow secure HTTPS connections to the web-based manager, and extension user account through this network interface.
- **HTTP:** Enable to allow HTTP connections to the web-based manager, and extension user account through this network interface.

Enable this option if you select *Centralized phonebook* when configuring programmable phone key. For more information, see [“Set Programmable Phone Key” on page 125](#).

- **PING:** Enable to allow ICMP ECHO (ping) responses from this network interface.

For information on configuring the network interface from which the FortiVoice unit itself will send pings, see the [FortiVoice CLI Reference](#).

- **SSH:** Enable to allow SSH connections to the CLI through this network interface.
- **SNMP:** Enable to allow SNMP connections (queries) to this network interface.

For information on further restricting access, or on configuring the network interface that will be the source of traps, see [“Configuring the network interfaces” on page 40](#).

- **TELNET:** Enable to allow Telnet connections to the CLI through this network interface.

Caution: HTTP and Telnet connections are **not** secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiVoice unit. For information on further restricting access of administrative connections, see [“Configuring administrator accounts” on page 50](#).

MTU

Override default MTU value (1500): Enable to change the maximum transmission unit (MTU) value, then enter the maximum packet or Ethernet frame size in bytes.

If network devices between the FortiVoice unit and its traffic destinations require smaller or larger units of traffic, packets may require additional processing at each node in the network to fragment or defragment the units, resulting in reduced network performance. Adjusting the MTU to match your network can improve network performance.

The default value is 1500 bytes. The MTU size must be between 576 and 1500 bytes. Change this if you need a lower value; for example, RFC 2516 prescribes a value of 1492 for the PPPoE protocol.

Administrative status	Select either: <ul style="list-style-type: none"> • <i>Up</i>: Enable (that is, bring up) the network interface so that it can send and receive traffic. • <i>Down</i>: Disable (that is, bring down) the network interface so that it cannot send or receive traffic.
------------------------------	--

Configuring static routes

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

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

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

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

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

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

To view or configure static routes

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

Figure 15: Static routes

Destination IP/Netmask	Gateway	Interface
0.0.0.0/0	172.20.190.249	
192.168.110.0/24	192.168.110.5	
172.16.100.0/24	192.168.110.5	
10.2.2.0/24	172.20.190.245	

<i>GUI field</i>	<i>Description</i>
Destination IP/Netmask	Displays the destination IP address and subnet of packets subject to the static route. A setting of 0.0.0.0/0.0.0.0 indicates that the route matches all destination IP addresses.
Interface	The interface that this route applies to.

Gateway	Displays the IP address of the next-hop router to which packets subject to the static route will be forwarded.
----------------	--

2. Either click *New* to add a route or double-click a route to modify it.
A dialog appears.
3. 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.
4. Select the interface that this route applies to.
5. 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.
6. 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:

Figure 16:DHCP server configuration

Network Interface Setting

ID:

0

Enabled:

☒

Interface:

port1

Please make sure slave mode has the same interfaces

Gateway:

192.168.2.99

DNS options:

Default

Primary DNS server:

0.0.0.0

Secondary DNS server:

0.0.0.0

Domain:

Netmask:

255.255.255.0

Advanced Setting

TFTP server (Opt66):

port1

Lease time (Seconds):

604800

Vender Class Identifier option:

☐

VCI string:

DHCP IP Range

New... Edit... Delete

Start

End

DHCP Excluded IP Range

Reserved IP Address

Create

Cancel

GUI field	Description
Network Interface Setting	
ID	The system will generate an ID for this configuration. This is view only.
Enabled	Select to enable the DHCP server.
Interface	Select an interface for the DHCP server from the drop-down list. If this FortiVoice is in HA mode, make sure that the slave unit has the same interface as the master unit. For information on HA, see “Using high availability” on page 53 .
Gateway	Enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
DNS options	Select to use either a specific DNS server or the system’s DNS settings. If you select a specific DNS server, enter the <i>Primary DNS server</i> and the <i>Secondary DNS server</i> fields. For more information, see “Configuring DNS” on page 46 .
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	

TFTP server (Opt66)	The default TFTP server (192.168.2.99) is where the configuration files for the supported phones are stored. This is also the IP address of the default gateway that the DHCP server assigns to the DHCP clients. If you have your own TFTP server for such information, enter its IP address in this field. However, SIP phone auto-provisioning will not work in this case. For more information, see “Configuring SIP phone auto-provisioning” on page 111.
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 or by checking <i>Monitor > PBX Status > DHCP > VCI</i> .
VCI string	Enter the phone VCI string supplied by the vendor.
DHCP IP Range	Click <i>New</i> to enter the start and end for the range of IP addresses that this DHCP server assigns to the DHCP clients.
DHCP Excluded IP Range	Click <i>New</i> to enter a range of IP addresses that this server should not assign to the DHCP clients.
Reserved IP Address	Click <i>New</i> to 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

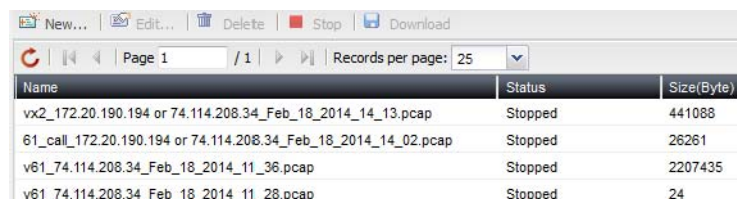
resolution is correct, and if the traffic is returning to the source as expected. You can also use packet switching to verify that NAT or other configuration is translating addresses or routing traffic the way that you want it to.

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*.

Figure 17: Traffic capture list



Name	Status	Size(Byte)
vx2_172.20.190.194 or 74.114.208.34_Feb_18_2014_14_13.pcap	Stopped	441088
61_call_172.20.190.194 or 74.114.208.34_Feb_18_2014_14_02.pcap	Stopped	26261
v61_74.114.208.34_Feb_18_2014_11_36.pcap	Stopped	2207435
v61_74.114.208.34_Feb_18_2014_11_28.pcap	Stopped	24

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

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

Configuring administrator accounts and access profiles

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

This topic includes:

- [Configuring administrator accounts](#)
- [Configuring administrator profiles](#)

Configuring administrator accounts

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

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

To view and configure administrator accounts

1. Go to *System > Admin > Administrators*.

Figure 18: Administrators tab



Enab...	Name	Extension	Authentication Type	Authentication Profile	Trusted Hosts	Admin Profile
<input checked="" type="checkbox"/>	admin	-	Local		0.0.0.0/0::/0	super_admin_prof
<input checked="" type="checkbox"/>	admin_temp	-	Local		0.0.0.0/0::/0	super_admin_prof
<input checked="" type="checkbox"/>	akaye	-	LDAP	corp ldap ottawa	0.0.0.0/0::/0	read_only
<input checked="" type="checkbox"/>	dbodinariuc	-	LDAP	corp ldap ottawa	0.0.0.0/0::/0	super_admin_prof

GUI field	Description
Name	Displays the name of the administrator account.
Extension	Displays the extension associated with the administrator account.
Authentication Type	The administrator authentication type: <i>Local</i> or <i>LDAP</i> .
Authentication Profile	The LDAP authentication profile. For more information, see “Configuring LDAP profiles” on page 125 .
Trusted Hosts	Displays the IP address and netmask from which the administrator can log in.
Admin Profile	The administrator profile that determines which functional areas the administrator account may view or affect.

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

Figure 19: New Administrator dialog

New Administrator

Administrator:

Associate extension:

--None--

New...

Edit...

Authentication type:

Local

☒ ▼ Create password

Password:

Confirm password:

Trusted hosts:

0.0.0.0 / 0

Admin profile:

acc_monitor

New...

Edit...

Select language:

--Default--

Select theme:

Red Grey

Use Current

Create

Cancel

GUI field	Description
Administrator	<p>Enter the name for this administrator account.</p> <p>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.</p>
Associate extension	<p>Enter the extension for the administrator account.</p> <p>If you add an extension, a <i>User portal</i> icon appears at the top of the web-based manager when you log into the FortiVoice unit. Clicking the icon opens the user web portal.</p> <p>Click <i>Edit</i> to modify the selected extension or click <i>New</i> to configure a new one. For more information on extensions, see “Configuring IP extensions” on page 133.</p>
Authentication type	<p>Select an administrator authentication type: <i>Local</i> or <i>LDAP</i>.</p>
Create password	<ul style="list-style-type: none"><i>Password</i>: Enter this account’s password. The password can contain any character except spaces. This field does not appear if <i>Authentication type</i> is <i>LDAP</i>. Caution: Do not enter a FortiVoice administrator password less than six characters long. For better security, enter a longer password with a complex combination of characters and numbers, and change the password regularly. Failure to provide a strong password could compromise the security of your FortiVoice unit.<i>Confirm password</i>: Enter this account’s password again to confirm it. This field does not appear if <i>Authentication type</i> is <i>LDAP</i>.
LDAP profile	<p>If you select <i>LDAP</i> for <i>Authentication type</i>, select an LDAP authentication profile. For more information, see “Configuring LDAP profiles” on page 125.</p>

Trusted Hosts	<p>Enter an IPv4 or IPv6 address or subnet from which this administrator can log in.</p> <p>If you want the administrator to access the FortiVoice unit from any IP address, use 0.0.0.0/0.0.0.0.</p> <p>Enter the IP address and netmask in dotted decimal format. For example, you might permit the administrator to log in to the FortiVoice unit from your private network by typing 192.168.1.0/255.255.255.0.</p> <p>Note: 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 <i>Trusted Host #1</i>, <i>Trusted Host #2</i>, and <i>Trusted Host #3</i> fields.</p> <p>Note: For information on restricting administrative access protocols that can be used by these hosts, see “Editing network interfaces” on page 41.</p> <p>Click the + sign to add additional IP addresses or subnets from which the administrator can log in.</p>
Admin profile	<p>Select the name of an admin profile that determines which functional areas the administrator account may view or affect.</p> <p>Click <i>New</i> to create a new profile or <i>Edit</i> to modify the selected profile. For details, see “Configuring administrator profiles” on page 52.</p>
Select language	Select this administrator account’s preference for the display language of the web-based manager.
Select theme	<p>Select this administrator account’s preference for the display theme or click <i>Use Current</i> to choose the theme currently in effect.</p> <p>The administrator may switch the theme at any time during a session by clicking <i>Next Theme</i>.</p>

4. Click *Create*.

Configuring administrator profiles

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

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

To configure administrator access profiles

1. Go to *System > Admin > 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. In the *Configure the privileges* table, 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*.

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 [“How to use HA” on page 56](#).

This section contains the following topics:

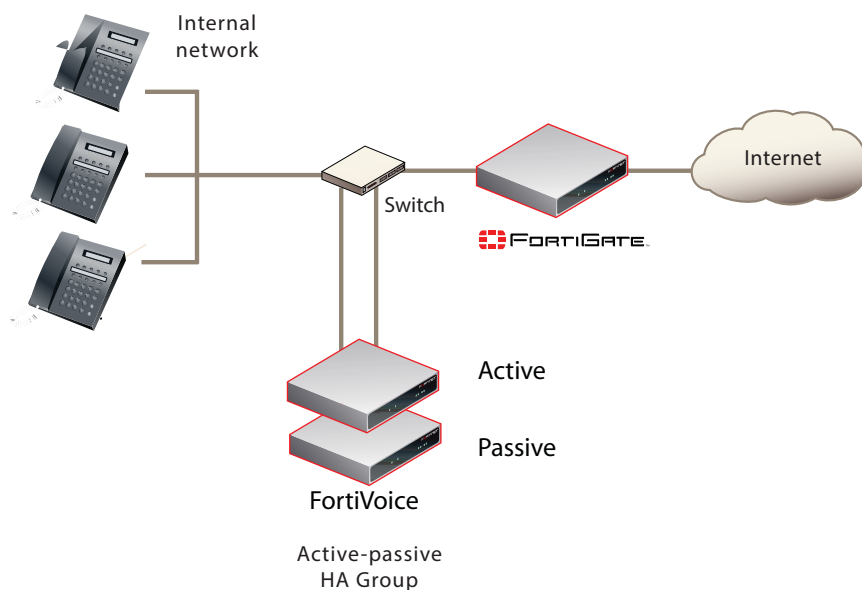
- [About high availability](#)
- [About the heartbeat and synchronization](#)
- [How to use HA](#)
- [Monitoring the HA status](#)
- [Configuring service-based failover](#)
- [Example: Failover scenarios](#)

About high availability

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

- 2 FortiVoice units in the HA group
- Both configuration and data synchronized (For exceptions to synchronized configuration items, see [“Configuration settings that are not synchronized” on page 55](#).
- Only primary unit processes phone calls
- No data loss when hardware fails although active calls are disconnected and line appearance and extension appearance take time to restore
- Has failover protection, but no increased processing capacity.

Figure 20:Active-passive HA group



You can mix different FortiVoice models in the same HA group. However, all units in the HA group must have the same firmware version with the same hardware. For example, FortiVoice 200D and 200D-T models cannot be in the same HA group due to hardware differences, but 200D and FortiVoice VM can be in the same group because neither of them has PRI or FXS/FXO ports.



When mixing FortiVoice models, the HA group is limited by the capacity and configuration limits of the least powerful model.

Communications between HA members occur through the heartbeat and synchronization connection. For details, see [“About the heartbeat and synchronization” on page 55](#).

To configure FortiVoice units operating in HA mode, you usually connect only to the primary unit (*master*). The primary unit’s configuration is almost entirely synchronized to secondary units (*slave*), 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 settings that are not synchronized. For details, see [“Configuration settings that are not synchronized” on page 55](#).

For instructions of how to enable and configure HA, see [“How to use HA” on page 56](#).

About the heartbeat and synchronization

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



Service monitoring traffic can also, for short periods, be used as a heartbeat. For details, see [“Remote services as heartbeat” on page 63](#).

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 [“Configuration settings that are not synchronized” on page 55](#).

- to synchronize system and user data from the primary unit to the secondary unit

Call data consists of the FortiVoice call detailed records, recorded calls, voicemail, call directories, fax, and voice prompts.

When the primary unit's configuration changes, it immediately synchronizes the change to the secondary unit through the primary heartbeat interface. If this fails, or if you have inadvertently de-synchronized the secondary unit's configuration, you can manually initiate synchronization. For details, see [“click HERE to start a configuration/data sync” on page 59](#). 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. For details, see the [FortiVoice CLI Reference](#).

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 68](#).

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 69](#).

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 70](#) and [“Configuring alert email” on page 257](#).

Configuration settings that are not synchronized

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

Table 6: HA settings not synchronized

Host name	The host name distinguishes members of the cluster. For details, see “Host name” on page 349 .
Static route	Static routes are not synchronized because the HA units may be in different networks (see “Configuring static routes” on page 45).

Table 6: HA settings not synchronized

Interface configuration	<p>Each FortiVoice unit in the HA group must be configured with different network interface settings for connectivity purposes. For details, see “Configuring the network interfaces” on page 40.</p> <p>Exceptions include some active-passive HA settings which affect the interface configuration for failover purposes. These settings are synchronized.</p>
Main HA configuration	<p>The main HA configuration, which includes the HA mode of operation (such as <i>master</i> or <i>slave</i>), 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 60.</p>
HA service monitoring configuration	<p>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 failover” on page 66.</p> <p>Note: 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.</p>
System appearance	<p>The appearance settings you configured under <i>System > Configuration > Appearance</i> are not synchronized.</p>

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.

How to use HA

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

1. Physically connect the FortiVoice units that will be members of the HA group.
You must connect at least one of their network interfaces for heartbeat and synchronization traffic between members of the group. For reliability reasons, Fortinet recommends that you connect both a primary and a secondary heartbeat interface, and that they be connected directly or through a dedicated switch that is not connected to your overall network.
2. On each member of the group:
 - Enable the HA mode that you want to use and select whether the individual member will act as a primary unit or secondary unit. For information about the differences between the HA modes, see [“About high availability” on page 53](#).
 - Configure the local IP addresses of the primary and secondary heartbeat and synchronization network interfaces.
 - Configure a virtual IP address that is shared by the HA group and remains the same after a failover. The virtual IP address is used to auto-provision the server IP address and the SIP trunk client IP address.
 - Configure the behavior on failover, and how the network interfaces should be configured for whichever FortiVoice unit is currently acting as the primary unit.
3. If you want to trigger failover when hardware or a service fails, even if the heartbeat connection is still functioning, configure service monitoring. For details, see [“Configuring service-based failover” on page 66](#).
4. Monitor the status of each group member. For details, see [“Monitoring the HA status” on page 57](#). 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 246](#).

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 [“How to use HA” on page 56](#).

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

Figure 21:Active-passive HA status (primary unit)

The screenshot shows the 'Status' tab for High Availability. At the top, there is a dropdown menu set to 'None' and a 'Refresh' button. Below this, the 'Mode Status' section displays 'Configured Operating Mode: master' and 'Effective Operating Mode: master'. The 'Actions' section contains two links: 'click HERE to start a configuration/data sync...' and 'click HERE to switch to SLAVE mode...'.

Table 7: Viewing HA status

<i>GUI item</i>	<i>Description</i>
Mode Status	
Configured Operating Mode	<p>Displays the HA operating mode that you configured, either:</p> <ul style="list-style-type: none">• <i>master</i>: Configured to be the primary unit of an active-passive group.• <i>slave</i>: Configured to be the secondary unit of an active-passive group. <p>For information on configuring the HA operating mode, see “Mode of operation” on page 62.</p> <p>After a failure, the FortiVoice unit may not be acting in its configured HA operating mode. For details, see “Effective Operating Mode” on page 58.</p>
Effective Operating Mode	<p>Displays the mode that the unit is currently operating in, either:</p> <ul style="list-style-type: none">• <i>master</i>: Acting as primary unit.• <i>slave</i>: Acting as secondary unit.• <i>off</i>: 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 62.• <i>failed</i>: 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 62. <p>The configured HA operating mode matches the effective operating mode unless a failure has occurred.</p> <p>For example, after a failover, a FortiVoice unit configured to operate as a secondary unit could be acting as a primary unit.</p> <p>For explanations of combinations of configured and effective HA modes of operation, see Table 8.</p> <p>For information on restoring the FortiVoice unit to an effective HA operating mode that matches the configured operating mode, see “click HERE to restore configured operating mode” on page 59.</p>
Daemon Status	<p>This option appears only for secondary units in active-passive HA groups.</p>

Table 7: Viewing HA status

GUI item	Description
Monitor	<p>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.</p> <p>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.</p> <p>For details, see “HA base port” on page 63.</p>
Configuration	<p>Displays the time at which the secondary unit's HA daemon will synchronize the FortiVoice configuration from the primary unit to the secondary unit.</p> <p>The message <code>slave unit is currently synchronizing</code> appears when the HA daemon is synchronizing the configuration.</p> <p>For information on items that are not synchronized, see “Configuration settings that are not synchronized” on page 55.</p>
Data	<p>Displays the time at which the secondary unit HA daemon will synchronize mail data from the primary unit to the secondary unit.</p> <p>The message <code>slave unit is currently synchronizing</code> appears when the HA daemon is synchronizing data.</p>
Actions	
click HERE to start a configuration/data sync	<p>Click to manually initiate synchronization of the configuration and call data. For information on items that are not synchronized, see “Configuration settings that are not synchronized” on page 55.</p>
click HERE to restore configured operating mode	<p>Click to reset the FortiVoice unit to an effective HA operating mode that matches the FortiVoice unit's configured operating mode.</p> <p>For example, for a configured primary unit whose effective HA operating mode is now <code>slave</code>, 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 slave role.</p> <p>Note: Before selecting this option, if the effective HA operating mode changed due to failover, you should resolve any issues that caused the failover.</p>

Table 8: Combinations of configured and effective HA modes of operation

Configured operating mode	Effective operating mode	Description
master	master	Normal for the primary unit of an active-passive HA group.
slave	slave	Normal for the secondary unit of an active-passive HA group.
master	off	The primary unit has experienced a failure, or the FortiVoice unit is in the process of switching to operating in HA mode. HA processes and call processing are stopped.
slave	off	The secondary unit has detected a failure, or the FortiVoice unit is in the process of switching to operating in HA mode. After the secondary unit starts up and connects with the primary unit to form an HA group, the first configuration synchronization may fail in special circumstances. To prevent both the secondary and primary units from simultaneously acting as primary units, the effective HA mode of operation becomes <i>off</i> . If subsequent synchronization fails, the secondary unit's effective HA mode of operation becomes <i>master</i> .
master	failed	The remote service monitoring or local network interface monitoring on the primary unit has detected a failure, and will attempt to connect to the other FortiVoice unit. If the problem that caused the failure has been corrected, the effective HA mode of operation switches from <i>failed</i> to <i>slave</i> , or to match the configured HA mode of operation, depending on the <i>On failure</i> setting.
master	slave	The primary unit has experienced a failure but then returned to operation. When the failure occurred, the unit configured to be the secondary unit became the primary unit. When the unit configured to be the primary unit restarted, it detected the new primary unit and so switched to operating as the secondary unit.
slave	master	The secondary unit has detected that the FortiVoice unit configured to be the primary unit failed. When the failure occurred, the unit configured to be the secondary unit became the primary unit.

Configuring the HA mode and group

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

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

HA 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 on heartbeat and synchronization, see [“About the heartbeat and synchronization” on page 55](#).

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

To configure HA options

1. Go to *System > High Availability > Configuration*.

Figure 22: Active-passive HA (primary unit)

The screenshot displays the FortiVoice configuration interface for High Availability (HA). It is divided into three main sections: HA Configuration, Interface, and Service Monitor.

HA Configuration:

- Mode of operation: master
- On failure: switch off
- Shared password: change_me
- Advanced options: (collapsed)
- Buttons: Apply, Cancel

Interface:

Port	Heartbeat Status	Peer IP Address	Virtual IP Action	Virtual IP Address	Port Monitor
port1	Disable	[IPv4] 172.20.140.35 [IPv6] ::	Use	[IPv4] 172.20.140.110/24 [IPv6] ::0	✗
port2	Primary	[IPv4] 192.168.100.2 [IPv6] ::	Use	[IPv4] 192.168.100.100/24 [IPv6] ::0	✓
port3	Disable	[IPv4] 0.0.0.0 [IPv6] ::	Use	[IPv4] 192.168.101.100/24 [IPv6] ::0	✗
port4	Disable	[IPv4] 0.0.0.0 [IPv6] ::	Ignore	[IPv4] 0.0.0.0/0 [IPv6] ::0	✗

Service Monitor:

Name	Remote IP	Port	Timeout	Interval	Retries	Enabled
Remote HTTP	0.0.0.0	80	30	120	3	✗
SIP UDP	0.0.0.0	5060	30	120	3	✗
Interface monitor				120	3	—
Local hard drives				120	3	✗

2. Configure the following sections, as applicable:

- “Configuring the primary HA options” on page 61
- “Configuring the advanced options” on page 62
- “Configuring interface monitoring” on page 63
- “Configuring service-based failover” on page 66

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.

Table 9: HA main options

GUI item	Description
Mode of operation	<p>Enables or disables HA, and selects the initial configured role this FortiVoice unit in the HA group.</p> <ul style="list-style-type: none">• <i>off</i>: The FortiVoice unit is not operating in HA mode.• <i>master</i>: The FortiVoice unit is the primary unit in an active-passive HA group.• <i>slave</i>: The FortiVoice unit is the secondary unit in an active-passive HA group.
On failure	<p>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.</p> <ul style="list-style-type: none">• <i>switch off</i>: 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 59 and “click HERE to restore configured operating mode” on page 59).• <i>wait for recovery then restore original role</i>: On recovery, the failed primary unit’s effective HA mode of operation resumes its configured master role. This also means that the secondary unit needs to give back the master 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.• <i>wait for recovery then restore slave role</i>: On recovery, the failed primary unit’s effective HA mode of operation becomes <i>slave</i>, and the secondary unit continues to assume the <i>master</i> role. The primary unit then synchronizes with the current master unit. The new master unit can then deliver phone calls. For information on manually restoring the FortiVoice unit to acting in its configured HA mode of operation, see “click HERE to restore configured operating mode” on page 59. <p>In most cases, you should select the <i>wait for recovery then restore slave role</i> option.</p> <p>For details on the effects of this option on the <i>Effective Operating Mode</i>, see Table . For information on configuring service/interface monitoring, see “Configuring service-based failover” on page 66.</p> <p>This option appears only if “Mode of operation” is <i>master</i>.</p>
Shared password	<p>Enter an HA password for the HA group. You must configure the same <i>Shared password</i> value on both the primary and secondary units.</p>

Configuring the advanced options

Go to *System > High Availability > Configuration* to configure the advanced options.

Table 10:HA advanced options

GUI item	Description
HA base port	<p>Keep the default TCP port number (20000) that will be used for:</p> <ul style="list-style-type: none">• the heartbeat signal• synchronization control• data synchronization• configuration synchronization <p>Note: In addition to configuring the heartbeat, you can configure service monitoring. For details, see “Configuring service-based failover” on page 66.</p> <p>Note: 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 59.</p>
Heartbeat lost threshold	<p>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.</p> <p>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.</p> <p>Note: If the failure detection time is too short, the secondary unit may falsely detect a failure when during periods of high load.</p> <p>Caution: If the failure detection time is too long the primary unit could fail and a delay in detecting the failure could mean that call is delayed or lost. Decrease the failure detection time if email is delayed or lost because of an HA failover.</p>
Remote services as heartbeat	<p>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, if remote service monitoring still detects that the primary unit is available, a failover will not occur.</p> <p>Note: 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, physical heartbeat connections will be checked first. If the physical connections are not found, the remote service monitoring does not take effect anymore.</p> <p>Note: 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.</p>

Configuring interface monitoring

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

To configure interface monitoring

1. Go to *System > High Availability > Configuration*.
2. Select master or slave as the mode of operation.
3. Expand the *Interface* area, if required.
4. Click on the port/interface name to configure the interface. For details, see [“Configuring the network interfaces” on page 40](#).



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.

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

<i>GUI item</i>	<i>Description</i>
Port	Displays the interface name you're configuring.
Enable port monitor	Enable to monitor a network interface for failure. If the port fails, the primary unit will trigger a failover.

GUI item	Description
Heartbeat status	<p>Specify if this interface will be used for HA heartbeat and synchronization.</p> <ul style="list-style-type: none"> • 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 55. This network interface must be connected directly or through a switch to the <i>Primary heartbeat</i> 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 55. 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 <i>Secondary heartbeat</i> network interfaces of the other member in the HA group. <p>Caution: 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.</p> <p>Note: 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.</p>
Peer IP address	<p>Enter the IP address of the matching heartbeat network interface of the other member of the HA group.</p> <p>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.</p> <p>Similarly, for the secondary heartbeat network interface, enter the IP address of the other unit’s secondary heartbeat network interface.</p> <p>For information about configuration synchronization and what is not synchronized, see “About the heartbeat and synchronization” on page 55.</p>

GUI item	Description
Virtual IP action	<p>Select whether and how to configure the IP addresses and netmasks of the FortiVoice unit whose effective HA mode of operation is currently <i>master</i>.</p> <p>For example, a primary unit might be configured to receive phone call traffic through <i>port1</i> and receive heartbeat and synchronization traffic through <i>port3</i> and <i>port4</i>. In that case, you would configure the primary unit to set the IP addresses or add virtual IP addresses for <i>port1</i> of the secondary unit on failover in order to mimic that of the primary unit.</p> <ul style="list-style-type: none"> • <i>Ignore</i>: Do not change the network interface configuration on failover, and do not monitor. For details on service monitoring for network interfaces, see “Configuring the network interfaces” on page 40. • <i>Use</i>: 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.

Configuring service-based failover

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

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

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

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

If service monitoring detects a failure, the effective HA operating mode of the primary unit switches to *off* or *failed* (depending on the *On failure* setting). A failover then occurs, and the effective HA operating mode of the secondary unit switches to *master*. For information on the *On failure* option, see [“Configuring the HA mode and group” on page 60](#). For information on the effective HA operating mode, see [“Monitoring the HA status” on page 57](#).

To configure service monitoring

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

GUI item	Description
Enable	Select to enable connection responsiveness tests for SMTP.
Name	Displays the service name.
Remote IP	Enter the peer IP address.
Port	Enter the port number of the peer SMTP service.

GUI item	Description
Timeout	Enter the timeout period for one connection test.
Interval	Enter the frequency of the tests.
Retries	Enter the number of consecutively failed tests that are allowed before the primary unit is deemed unresponsive and a failover occurs.

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

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

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

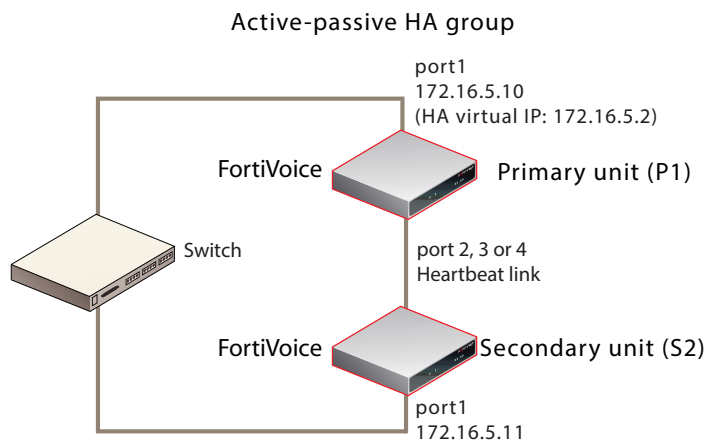
GUI item	Description
Enable	<p>Select to enable local hard drive monitoring. Interface monitoring is enabled when you configure interface monitoring. See “Configuring interface monitoring” on page 63.</p> <p>Network interface monitoring tests all active network interfaces whose:</p> <ul style="list-style-type: none"> • “Virtual IP action” setting is not ignore • “Configuring interface monitoring” setting is enabled <p>For details, see “Configuring interface monitoring” on page 63 and “Virtual IP action” on page 66.</p>
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.

Example: Failover scenarios

This section describes basic FortiVoice active-passive HA failover scenarios. For each scenario, refer to the HA group shown in [Figure 23](#). To simplify the descriptions of these scenarios, the following abbreviations are used:

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

Figure 23:Example active-passive HA group



This section contains the following HA failover scenarios:

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

Failover scenario 1: Temporary failure of the primary unit

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

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

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

Here is what happens during this process:

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

This is the HA machine at 172.16.5.11.

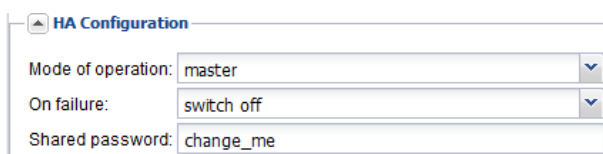
The following event has occurred
'MASTER heartbeat disappeared'
The state changed from 'SLAVE' to 'MASTER'

6. S2 records event log messages (among others) indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

Recovering from temporary failure of the primary unit

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

Figure 24: HA On Failure settings



HA Configuration	
Mode of operation:	master
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 59).

- *wait for recovery then restore original role*

On recovery, P1's effective HA operating mode resumes its configured master role. This also means that S2 needs to give back the master role to P1. This behavior may be useful if the cause of failure is temporary and rare, but may cause problems if the cause of failure is permanent or persistent.

In the case, the S2 will send out another alert email similar to the following:

This is the HA machine at 172.16.5.11.

The following event has occurred

'SLAVE asks us to switch roles (recovery after a restart)

The state changed from 'MASTER' to 'SLAVE'

After recovery, P1 also sends out an alert email similar to the following:

This is the HA machine at 172.16.5.10.

The following critical event was detected

The system was shutdown!

- *wait for recovery then restore slave role*

On recovery, P1's effective HA operating mode becomes *slave*, and S2 continues to assume the *master* role. P1 then synchronizes with the current master unit, S2. For information on manually restoring the FortiVoice unit to acting in its configured HA mode of operation, see [“click HERE to restore configured operating mode”](#) on page 59.

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

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

- P1 will send a holdoff command to S2 so that S2 will not take over the master 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 master role.
- S2 will send out an alert email, indicating that S2 received the holdoff command from P1. This is the HA machine at 172.16.5.11.

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

After P1 is up again:

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

The following event has occurred
'peer command appeared'
The state changed from 'HOLD_OFF' to 'SLAVE'

- S2 logs the event in the HA logs.

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

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

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

The following event has occurred
'ha: SLAVE heartbeat disappeared'

- S2 will send out an alert email similar to the following: This is the HA machine at 172.16.5.11.

The following critical event was detected
The system is rebooting (or reloading)!

- P1 will also log this event in the HA logs.

Failover scenario 4: System shutdown of the secondary unit

If you shut down S2:

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

Failover scenario 5: Primary heartbeat link fails

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

secondary unit (S2) changes to operating as a primary unit, and **both** FortiVoice units are acting as primary units.

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

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

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

This is the HA machine at 172.16.5.11.

The following event has occurred

'MASTER heartbeat disappeared'

The state changed from 'SLAVE' to 'MASTER'

6. S2 records event log messages (among others) indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

Recovering from a heartbeat link failure

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

To return to normal operation after the heartbeat link fails

1. Reconnect the primary heartbeat interface by reconnecting the heartbeat link Ethernet cable.
Even though the effective HA operating mode of S2 is *master*, S2 continues to attempt to find the other primary unit. When the heartbeat link is reconnected, S2 finds P1 and determines that P1 is also operating as a primary unit. So S2 sends a heartbeat signal to notify P1 to stop operating as a primary unit. The effective HA operating mode of P1 changes to *off*.
2. P1 sends an alert email similar to the following, indicating that P1 has stopped operating as the primary unit.
This is the HA machine at 172.16.5.10
The following event has occurred
'SLAVE asks us to switch roles (user requested takeover)'
The state changed from 'MASTER' to 'OFF'
3. P1 records event log messages (among others) indicating that P1 is switching to *off* mode.
The configured HA mode of operation of P1 is *master* and the effective HA operating mode of P1 is *off*.
The configured HA mode of operation of S2 is *slave* and the effective HA operating mode of S2 is *master*.
4. Connect to the web-based manager of P1, go to *System > High Availability > Status*.

5. Check for synchronization messages.

Do not proceed to the next step until P1 has synchronized with S2.

6. Connect to the web-based manager of S2, go to *System > High Availability > Status* and select *click HERE to restore configured operating mode*.

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

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

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

Depending on your network configuration, the network connection between the primary and secondary units can fail for a number of reasons. In the network configuration shown in [Figure 23 on page 68](#), the connection between port1 of primary unit (P1) and port1 of the secondary unit (S2) can fail if a network cable is disconnected or if the switch between P1 and S2 fails.

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

In this scenario, remote service monitoring has been configured to make sure that S2 can connect to P1. The *On failure* setting located in the HA main configuration section is *wait for recovery then restore slave role*. For information on the *On failure* setting, see ["On failure" on page 62](#). For information about remote service monitoring, see ["Configuring service-based failover" on page 66](#).

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

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

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

This is the HA machine at 172.16.5.11.

The following event has occurred
'MASTER remote service disappeared'
The state changed from 'SLAVE' to 'MASTER'

8. S2 logs the event (among others) indicating that S2 has determined that P1 has failed and that S2 is switching its effective HA operating mode to *master*.

9. P1 sends an alert email similar to the following, indicating that P1 has stopped operating in HA mode.

This is the HA machine at 172.16.5.10.

The following event has occurred

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

The state changed from 'MASTER' to 'FAILED'

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

Recovering from a network connection failure

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

To return to normal operation after the heartbeat link fails

1. Reconnect power to the switch.

Because the effective HA operating mode of P1 is *failed*, P1 is using remote service monitoring to attempt to connect to S2 through the switch.

2. When the switch resumes operating, P1 successfully connects to S2.

P1 has determined the S2 can connect to the network and process calls.

3. The effective HA operating mode of P1 switches to *slave*.

4. P1 logs the event.

5. P1 sends an alert email similar to the following, indicating that P1 is switching its effective HA operating mode to *slave*.

This is the HA machine at 172.16.5.10.

The following event has occurred

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

The state changed from 'FAILED' to 'SLAVE'

6. Connect to the web-based manager of P1 and go to *System > High Availability > Status*.

7. Check for synchronization messages.

Do not proceed to the next step until P1 has synchronized with S2.

8. Connect to the web-based manager of S2, go to *System > High Availability > Status* and select *click HERE to restore configured operating mode*.

9. Connect to the web-based manager of P1, go to *System > High Availability > Status* and select *click HERE to restore configured operating mode*.

P1 should return to operating as the primary unit and S2 should return to operating as the secondary unit.

P1 and S2 synchronize again. P1 can now process phone calls normally.

Configuring system time, system options, SNMP, email setting, and GUI appearance

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

This topic includes:

- [Configuring the time and date](#)
- [Configuring system options](#)
- [Configuring SNMP queries and traps](#)
- [Configuring email settings](#)
- [Customizing the GUI appearance](#)

Configuring the time and date

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

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

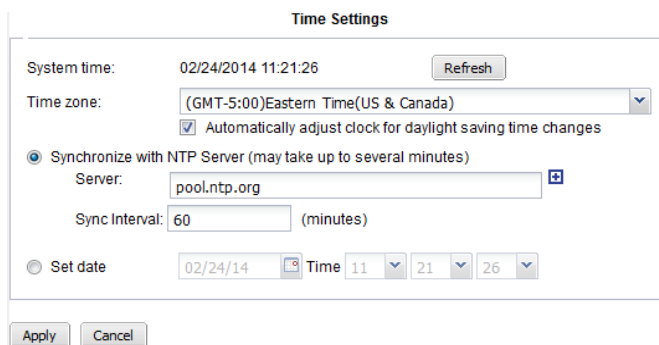


For many features to work, including scheduling, logging, and certificate-dependent features, the FortiVoice system time must be accurate. FortiVoice units support daylight savings time (DST), including recent changes in the USA, Canada and Western Australia.

To configure the system time

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

Figure 25: Time Settings tab



GUI field	Description
System time	Displays the date and time according to the FortiVoice unit's clock at the time that this tab was loaded, or when you last selected the <i>Refresh</i> button.

Time zone	<p>Select the time zone in which the FortiVoice unit is located.</p> <ul style="list-style-type: none"> <i>Automatically adjust clock for daylight saving time changes:</i> Enable to adjust the FortiVoice system clock automatically when your time zone changes to daylight savings time (DST) and back to standard time. <p>When selecting time zone in CLI, use the command <code>config system time manual</code> and enter the code before the time zone in Table 11 on page 75.</p>
Synchronize with NTP Server	<p>Select to use a network time protocol (NTP) server to automatically set the system date and time, then configure <i>Server</i> and <i>Sync Interval</i>.</p> <ul style="list-style-type: none"> <i>Server:</i> Enter the IP address or domain name of an NTP server. You can add a maximum of 10 NTP servers. The FortiVoice unit uses the first NTP server based on the selection mechanism of the NTP protocol. Click the + sign to add more servers. Click the - sign to remove servers. Note that you cannot remove the last server. To find the NTP servers that you can use, see http://www.ntp.org. <i>Sync Interval:</i> Enter how often, in minutes, the FortiVoice unit should synchronize its time with the NTP server. For example, entering 1440 causes the FortiVoice unit to synchronize its time once a day. <p>Depending on your network traffic, it may take some time for the FortiVoice unit to synchronize its time with the NTP server.</p>
Set date	<p>Select this option to manually set the date and time of the FortiVoice unit's clock, then select the <i>Year</i>, <i>Month</i>, <i>Day</i>, <i>Hour</i>, <i>Minute</i>, and <i>Second</i> fields before you click <i>Apply</i>.</p> <p>Alternatively, configure <i>Synchronize with NTP server</i>.</p>

3. Click *Apply*.

Table 11:Time zone codes for CLI configuration

Code	Time Zone
0	(GMT-12:00) Eniwetok, Kwajalein
1	(GMT-11:00) Midway Island, Samoa
2	(GMT-10:00) Hawaii
3	(GMT-9:00) Alaska
4	(GMT-8:00) Pacific Time (US& Canada)
5	(GMT-7:00) Arizona
6	(GMT-7:00) Mountain Time (US& Canada)

Table 11:Time zone codes for CLI configuration

Code	Time Zone
7	(GMT-6:00) Central America
8	(GMT-6:00) Central Time
9	(GMT-6:00) Mexico City
10	(GMT-6:00) Saskatchewan
11	(GMT-5:00) Bogota, Lima, Quito
12	(GMT-5:00) Eastern Time (US & Canada)
13	(GMT-5:00) Indiana (East)
14	(GMT-4:30) Venezuela Standard Time
15	(GMT-4:00) Atlantic Time (Canada)
16	(GMT-4:00) Caracas, La Paz
17	(GMT-4:00) Santiago
18	(GMT-3:30) Newfoundland
19	(GMT-3:00) Brasilia
20	(GMT-3:00) Buenos Aires, Georgetown
21	(GMT-3:00) Greenland
22	(GMT-2:00) Mid-Atlantic
23	(GMT-1:00) Azores
24	(GMT-1:00) Cape Verde Is.
25	(GMT) Casablanca, Monrovia
26	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
27	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
28	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
29	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris
30	(GMT+1:00) Sarajevo, Skopje, Sofia, Vilnius, Warsaw, Zagreb
31	(GMT+1:00) West Central Africa
32	(GMT+2:00) Athens, Istanbul, Minsk
33	(GMT+2:00) Bucharest
34	(GMT+2:00) Cairo
35	(GMT+2:00) Harare, Pretoria

Table 11:Time zone codes for CLI configuration

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

Table 11:Time zone codes for CLI configuration

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

Configuring system options

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

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

To view and configure the system options

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

Figure 26: Options tab

Configuration Options

Idle timeout: 45 (1-480 minutes)

▲ Password / PIN Policy

Enable

Minimum password length: 8

Password must contain:

Uppercase letter

Lowercase letter

Number (0-9)

Non alphanumeric character

Apply password policy to:

Administrators

SIP users

Minimum PIN length: 6

PIN must contain:

Number (0-9)

PIN special

Apply PIN policy to:

Voicemail users

▲ Administration Ports

HTTP port number: 80

HTTPS port number: 443

SSH port number: 22

TELNET port number: 23

Web action hostIP:

Apply

Cancel

GUI field	Description
Idle timeout	Enter the amount of time that an administrator may be inactive before the FortiVoice unit automatically logs out the administrator. For better security, use a low idle timeout value.

Fortinet Technologies Inc.

Page 79 FortiVoice Enterprise Phone System 4.0.0 Administration Guide

Password / PIN Policy

Displays the SIP password and user PIN policy for administrators and extension users. For information on setting SIP password and user PIN, see [“Configuring IP extensions” on page 133](#).

- *Enable*: Select to enable the password/PIN policy.
- *Minimum password length*: Set the minimum acceptable length (8) for passwords.
- *Password must contain*: Select any of the following special character types to require in a password. Each selected type must occur at least once in the password.
 - *Uppercase letters* — A, B, C, ... Z
 - *Lowercase letters* — a, b, c, ... z
 - *Number* — 0 ... 9
 - *Non alphanumeric character* — punctuation marks, @, #, ... %
- *Apply password policy to*: Select where to apply the password policy:
 - *Administrators* — Apply to administrator 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.
- *Minimum PIN length*: Set the minimum acceptable length (6) for the user PIN.
- *PIN must contain*:
 - *Number*: Select to include a number (0-9) in the PIN.
 - *PIN special*: Select to include * or # or both 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.

Administration Ports

Specify the TCP ports for administrative access on all interfaces.

Default port numbers:

HTTP: 80

HTTPS: 443

SSH: 22

TELNET: 23

Web action host/IP

Enter the host name or IP address from where a email notification is sent to you when a voice mail or fax is delivered to your extension. This IP address is included in the email notification. You can open the link to view or manage the voice mail or fax. If you leave this field empty, port1 IP will be used instead.
The value entered here replaces the default *Url host* variable for customizing messages. See [“Customizing email history report and notification email templates” on page 105](#).

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 85.

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

The FortiVoice SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Before you can use its SNMP queries, you must enable SNMP access on the network interfaces that SNMP managers will use to access the FortiVoice unit. For more information, see “[Editing network interfaces](#)” on page 41.

This topic includes:

- [Configuring an SNMP threshold](#)
- [Configuring email settings](#)
- [Configuring an SNMP v3 user](#)

Configuring an SNMP threshold

Configure under what circumstances an event is triggered.

To set SNMP thresholds

1. Go *System > Configuration > SNMP*.

SNMP System Information

SNMP agent enable: ☒

Description:

Location:

Contact:

SNMP Threshold

Trap Type	Trigger	Threshold	Sample Period (s)	Sample Freq (s)
CPU Usage	5%	1	600	30
Memory Usage	10%	3	600	30
Log Disk Usage	10%	1	7200	3600
Voice Disk Usage	10%	1	7200	3600

Apply Cancel

Community

New... Edit... Delete

Name	Status	Queries	Traps
fortivoice	✓	✓	✓

User

New... Edit... Delete

Name	Status	Queries	Traps	Security Level
yong	✓	✓	✓	Authentication, privacy

2. Configure the following:

GUI field	Description
SNMP agent enable	Enable to activate the FortiVoice SNMP agent. This must be enabled to accept queries from SNMP managers or send traps from the FortiVoice unit.
Description	Enter a descriptive name for the FortiVoice unit.
Location	Enter the location of the FortiVoice unit.
Contact	Enter administrator contact information.
SNMP Threshold	To change a value in the four editable columns, select the value in any row. It becomes editable. Change the value and click outside of the field. A red triangle appears in the field's corner and remains until you click <i>Apply</i> .
Trap Type	Displays the type of trap, such as <i>CPU Usage</i> .
Trigger	<p>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.</p> <p>For example, using the default value, if the mailbox disk is 90% or more full, it will trigger.</p>
Threshold	<p>Sets the number of triggers that will result in an SNMP trap.</p> <p>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.</p>
Sample Period(s)	<p>Sets the time period in seconds during which the FortiVoice unit SNMP agent counts the number of triggers that occurred.</p> <p>This value should not be less than the <i>Sample Freq(s)</i> value.</p>
Sample Freq(s)	<p>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.</p> <p>This value should be less than the <i>Sample Period(s)</i> value.</p>
Community	Displays the list of SNMP communities (for SNMP v1 and v2c) added to the FortiVoice configuration. For information on configuring a community, see either “Configuring email settings” or “Configuring an SNMP v3 user” on page 84.
Name	Displays the name of the SNMP community. The SNMP Manager must be configured with this name.
Status	A green check mark icon indicates that the community is enabled.
Queries	A green check mark icon indicates that queries are enabled.
Traps	A green check mark icon indicates that traps are enabled.

User	Displays the list of SNMP v3 users added to the FortiVoice configuration. For information on configuring a v3 user, see “Configuring an SNMP v3 user” on page 84 .
Name	Displays the name of the SNMP v3 user. The SNMP Manager must be configured with this name.
Status	A green check mark icon indicates that the user is enabled.
Queries	A green check mark icon indicates that queries are enabled.
Traps	A green check mark icon indicates that traps are enabled.
Security Level	The security level of the SNMP v3 user.

Configuring an SNMP v1 and v2c community

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

To configure an SNMP community

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

GUI field	Description
Name	Enter a name to identify the SNMP community. If you are editing an existing community, you cannot change the name. You can add up to 16 communities.
Enable	Enable to send traps to and allow queries from the community's SNMP managers.
Community Hosts	Lists SNMP managers that can use the settings in this SNMP community to monitor the FortiVoice unit. Click <i>Create</i> 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.
Delete (button)	Click to remove this SNMP manager.
Create (button)	Click to add a new default entry to the <i>Hosts</i> list that you can edit as needed.

Queries	Enter the <i>Port</i> number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiVoice unit. Mark the <i>Enable</i> check box to activate queries for each SNMP version.
Traps	Enter the <i>Local Port</i> and <i>Remote Port</i> numbers (162 local, 162 remote by default) that the FortiVoice unit uses to send SNMP v1 and SNMP v2c traps to the SNMP managers in this community. Enable traps for each SNMP version that the SNMP managers use.
SNMP Event	<p>Enable each SNMP event for which the FortiVoice unit should send traps to the SNMP managers in this community.</p> <p>Note: Since FortiVoice checks its status in a scheduled interval, not all the events will trigger traps. For example, FortiVoice checks its hardware status every 60 seconds. This means that if the power is off for a few seconds but is back on before the next status check, no system event trap will be sent.</p>

4. Click *Create*.

Configuring an SNMP v3 user

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

To configure an SNMP v3 user

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

GUI field	Description
User name	Enter a name to identify the SNMP user. If you are editing an existing user, you cannot change the name.
Enable	Enable to send traps to and allow queries from the user's SNMP managers.
Security level	<p>Choose one of the three security levels:</p> <ul style="list-style-type: none"> • <i>No authentication, no privacy</i>: This option is similar to SNMP v1 and v2. • <i>Authentication, no privacy</i>: 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). • <i>Authentication, privacy</i>: 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 <i>Security level</i> , if you select either <i>Authentication</i> 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 <i>Security level</i> , if you select <i>Privacy</i> , 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 <i>Create</i> to create a new entry. You can add up to 16 host.
IP Address	Enter the IP address of an SNMP manager. By default, the IP address is 0.0.0.0, so that any SNMP manager can use this SNMP user.
Delete (button)	Click to remove this SNMP manager.
Create (button)	Click to add a new default entry to the <i>Hosts</i> list that you can edit as needed.
Queries	Enter the <i>Port</i> number (161 by default) that the SNMP managers use for SNMP v3 queries to receive configuration information from the FortiVoice unit. Select the <i>Enable</i> check box to activate queries.
Traps	Enter the <i>Local Port</i> and <i>Remote Port</i> numbers (162 local, 162 remote by default) that the FortiVoice unit uses to send SNMP v3 traps to the SNMP managers. Select the <i>Enable</i> check box to activate traps.
SNMP Event	<p>Enable each SNMP event for which the FortiVoice unit should send traps to the SNMP managers.</p> <p>Note: Since FortiVoice checks its status in a scheduled interval, not all the events will trigger traps. For example, FortiVoice checks its hardware status every 60 seconds. This means that if the power is off for a few seconds but is back on before the next status check, no system event trap will be sent.</p>

4. Click *Create*.

FortiVoice MIBs

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

The FortiVoice MIBs are listed in [Table 12](#). 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.

Table 12:FortiVoice MIBs

<i>MIB file name</i>	<i>Description</i>
FortiVoice.mib	Displays the proprietary Fortinet MIB includes detailed FortiVoice system configuration information. Your SNMP manager requires this information to monitor FortiVoice configuration settings. For more information, see “MIB fields” on page 86.

FortiVoice traps

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

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

MIB fields

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

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

Table 13:System session MIB fields

MIB field	Description
fvSysModel	FortiVoice model number, such as 400 for the FortiVoice-400.
fvSysSerial	FortiVoice unit serial number.
fvSysVersion	The firmware version currently running on the FortiVoice unit.
fvSysCpuUsage	The current CPU usage (%).
fvSysMemUsage	The current memory utilization (%).
fvSysLogDiskUsage	The log disk usage (%).
fvSysStorageDiskUsage	The storage disk usage (%).
fvSysEventCode	System component events.
fvSysload	Current system load.
fvSysHA	<ul style="list-style-type: none">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 settings

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



For phone users to receive the notifications, you need to add their email addresses when configuring the extensions. See [“Configuring Extensions” on page 133](#).

To configure email settings

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

Figure 27: Mail server settings

Local Host

Host name:

fvc61-callcenter

Local domain name:

fortivoice.com

Mail Queue

Maximum time for email in queue (1-240 hours):

24

Time interval for retry (10-120 minutes):

10

Relay Server

Relay server name:

mail.ott-fortimail.com

Relay server port:

465

Use SMTPs

☒

☒ Authentication Required

Customize email template

Apply

Cancel

GUI field	Description
Local Host	
Host name	Enter the host name of the FortiVoice unit, such as <code>fortivoice-200D</code> .
Local domain name	Enter the local domain name of the FortiVoice unit, such as <code>example.com</code> .
Mail Queue	
Maximum time for email in queue (1-240 hours)	Enter the maximum number of hours that deferred email messages can remain in the deferred email queue, during which the FortiVoice unit periodically retries to send the message. After it reaches the maximum time, the FortiVoice unit sends a final delivery status notification (DSN) email message to notify the sender that the email message was undeliverable.
Time interval for retry (10-120 minutes)	Enter the number of minutes between delivery retries for email messages in the deferred mail queues.
Relay Server	
Configure an SMTP relay, if needed, to which the FortiVoice unit will relay outgoing email. This is typically provided by your Internet service provider (ISP), but could be a mail relay on your internal network.	
Relay server name	Enter the domain name of an SMTP relay.
Relay server port	Enter the TCP port number on which the SMTP relay listens. This is typically provided by your Internet service provider (ISP).

Use SMTPs	<p>Enable to initiate SSL- and TLS-secured connections to the SMTP relay if it supports SSL/TLS. When disabled, SMTP connections from the FortiVoice unit's built-in MTA or proxy to the relay will occur as clear text, unencrypted.</p> <p>This option must be enabled to initiate SMTPS connections.</p>
Authentication Required:	<p>Select the checkbox and click the arrow to expand the section and configure:</p> <ul style="list-style-type: none"> • <i>User name</i>: Enter the name of the FortiVoice unit's account on the SMTP relay. • <i>Password</i>: Enter the password for the FortiVoice unit's user name. • <i>Authentication type</i>: Available SMTP authentication types include: <ul style="list-style-type: none"> • <i>AUTO</i> (automatically detect and use the most secure SMTP authentication type supported by the relay server) • <i>PLAIN</i> (provides an unencrypted, scrambled password) • <i>LOGIN</i> (provides an unencrypted, scrambled password) • <i>DIGEST-MD5</i> (provides an encrypted hash of the password) • <i>CRAM-MD5</i> (provides an encrypted hash of the password, with hash replay prevention, combined with a challenge and response mechanism)
Customize email template	<p>View and reword the default email history report and notification email templates. For more information, see "Customizing email history report and notification email templates" on page 105.</p>

3. Click *Apply*.

Customizing the GUI appearance

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

To customize the GUI appearance

1. Go to *System > Configuration > Appearance*.
2. Click the arrow to expand *Administration interface* and *Voicemail interface*.
3. Configure the following to change appearance:

Figure 28: Appearance tab

New Appearance

Administration interface

Product name:

FortiVoice

Product icon:

The icon should be in .ico format, and 16*16 in size.

Change...

Reset

Top logo (460*36):

FortiVoice 200D

Change...

Reset

Default UI language:

English

Voicemail interface

Voicemail login:

Voicemail Login

Login user name hint:

Input your extension number

Voicemail theme:

Red Grey

Voicemail UI language:

English

Voicemail top logo (460*36):

FortiVoice 200D

Change...

Reset

(Maximum image file size is 512 KB)

Apply

Reset

Cancel

GUI field	Description
Administration interface	
Product name	Enter the name of the product. This name will precede <i>Administrator Login</i> in the title on the login page of the web-based manager.
Product icon	Click <i>Change</i> to browse for the product icon. The icon should be in .ico format, and 16 pixels wide x16 pixels tall in size.
Top logo	<p>Click <i>Change</i> to upload a graphic that will appear at the top of all pages in the web-based manager. The image’s dimensions must be 460 pixels wide by 36 pixels tall.</p> <p>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.</p> <p>Note: Uploading a graphic overwrites the current graphic. The FortiVoice unit does not retain previous or default graphics. If you want to revert to the current graphic, use your web browser to save a backup copy of the image to your management computer, enabling you to upload it again at a later time.</p> <p>Click <i>Reset</i> to return to the default setting.</p>
Default UI language	<p>Select the default language for the display of the web-based manager.</p> <p>You can configure a separate language preference for each administrator account. For details, see “Configuring administrator accounts” on page 50.</p>
Voicemail interface	

Voicemail login	Enter a word or phrase that will appear on top of the voicemail login page, such as Voicemail Login.
Login user name hint	Enter a hint for the user name, such as Your Email Address. This hint will appear as a mouse-over display on the login name field.
Voicemail theme	Select a theme for the voicemail GUI.
Voicemail UI language	Select the language in which voicemail pages will be displayed. By default, the FortiVoice unit will use the same language as the web-based manager
Voicemail top logo	<p>Click <i>Change</i> to upload a graphic that will appear at the top of all webmail pages. The image's dimensions must be 460 pixels wide by 36 pixels tall.</p> <p>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.</p> <p>Note: Uploading a graphic overwrites the current graphic. The FortiVoice unit does not retain previous or default graphics. If you want to revert to the current graphic, use your web browser to save a backup copy of the image to your management computer, enabling you to upload it again at a later time.</p> <p>Click <i>Reset</i> to return to the default setting.</p>

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

Managing certificates

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

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

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

Table 14: Certificate types

Certificate type	Usage
Server certificates	The FortiVoice unit must present its local server certificate for the following secure connections: <ul style="list-style-type: none">• the web-based manager (HTTPS connections only)• phone user web interface (HTTPS connections only)• phone and FortiVoice unit (TLS and SRTP connections only), see “Configuring SIP profiles” on page 118. For details, see “Managing local certificates” on page 92 .
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 98 .
Personal certificates	Phone users’ personal certificates are used for S/MIME encryption.

This section contains the following topics:

- [Managing local certificates](#)
- [Obtaining and installing a local certificate](#)
- [Managing certificate authority certificates](#)
- [Managing the certificate revocation list](#)

Managing local certificates

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

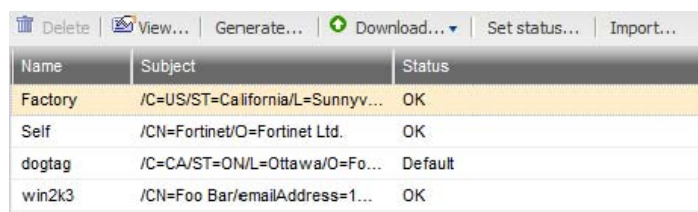
On this tab, you can also generate certificate signing requests and import signed certificates in order to install them for local use by the FortiVoice unit.

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

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

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

Figure 29: Local Certificate tab



Name	Subject	Status
Factory	/C=US/ST=California/L=Sunnyv...	OK
Self	/CN=Fortinet/O=Fortinet Ltd.	OK
dogtag	/C=CA/ST=ON/L=Ottawa/O=Fo...	Default
win2k3	/CN=Foo Bar/emailAddress=1...	OK

GUI field	Description
View	Select a certificate and click <i>View</i> to display its issuer, subject, and range of dates within which the certificate is valid.
Generate	Click to generate a local certificate request. For more information, see “Generating a certificate signing request” on page 94.
Download	<p>Click the row of a certificate file or certificate request file in order to select it, then click this button and select either:</p> <ul style="list-style-type: none">• <i>Download</i>: 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 96.• <i>Download PKCS12 File</i>: Download a PKCS #12 (.p12) file. For details, see “Downloading a PKCS #12 certificate” on page 98.
Set status	<p>Click the row of a certificate in order to select it, then click this button to use it as the “default” (that is, currently chosen for use) certificate. The <i>Status</i> column changes to indicate that the certificate is the current (<i>Default</i>) certificate.</p> <p>This button is not available if the selected certificate is already the “default.”</p>
Import	Click to import a signed certificate for local use. For more information, see “Importing a certificate” on page 97.

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 97.](#)
- 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](#)
- [Downloading a certificate signing request](#)
- [Submitting a certificate request to your CA for signing](#)
- [Importing a certificate](#)

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 93.

To generate a certificate request

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

Figure 30: Generate Certificate Signing Request dialog

Generate Certificate Signing Request

Certification name:

Subject Information

ID type:

IP:

Optional Information

Organization unit:

Organization:

Locality(City):

State/Province:

Country:

E-mail:

Key type:

Key size:

<i>GUI field</i>	<i>Description</i>
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.

ID type	<p>Select the type of identifier to be used in the certificate to identify the FortiVoice unit:</p> <ul style="list-style-type: none"> • Host IP • Domain name • E-mail <p>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.</p> <p>For example, if your FortiVoice unit has both a static IP address and a domain name, but you will primarily use the local certificate for HTTPS connections to the web-based manager by the domain name of the FortiVoice unit, you might prefer to generate a certificate based on the domain name of the FortiVoice unit, rather than its IP address.</p> <ul style="list-style-type: none"> • <i>Host IP</i> 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. • <i>Domain name</i> 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. • <i>E-mail</i> 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	<p>Enter the static IP address of the FortiVoice unit.</p> <p>This option appears only if <i>ID type</i> is <i>Host IP</i>.</p>
Domain name	<p>Type the fully-qualified domain name (FQDN) of the FortiVoice unit.</p> <p>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 40 and “Configuring DNS” on page 46.</p> <p>If a domain name is not available and the FortiVoice unit subscribes to a dynamic DNS service, an <code>unable to verify certificate</code> message may appear in the user’s browser whenever the public IP address of the FortiVoice unit changes.</p> <p>This option appears only if <i>ID type</i> is <i>Domain name</i>.</p>
E-mail	<p>Type the email address of the owner of the FortiVoice unit.</p> <p>This option appears only if <i>ID type</i> is <i>E-mail</i>.</p>
Optional Information	<p>Information that you may include in the certificate, but which is not required.</p>
Organization unit	<p>Type the name of your organizational unit, such as the name of your department. (Optional)</p> <p>To enter more than one organizational unit name, click the + icon, and enter each organizational unit separately in each field.</p>
Organization	<p>Type the legal name of your organization. (Optional)</p>

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)
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 <i>512 Bit</i> , <i>1024 Bit</i> , <i>1536 Bit</i> or <i>2048 Bit</i> . Larger keys are slower to generate, but provide better security.

4. Click **OK**.

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 96](#).

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 93](#).

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 93](#).

To submit a certificate request

1. Using the web browser on the management computer, browse to the web site 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 97](#).

Importing a certificate

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

DER encoding is not supported in FortiVoice version 2.0 GA.

Importing a certificate may be useful when:

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

If you generated the certificate request using the FortiVoice unit, after you submit the certificate request to CA, the CA will verify the information and register the contact information in a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA will then sign the certificate and return it to you for installation on the FortiVoice unit. To install the certificate, you must import it. For other related steps, see [“Obtaining and installing a local certificate” on page 93](#).

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. From *Type*, 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 93](#).
 - *PKCS12 Certificate*: Select this option if you are importing an existing certificate whose certificate file and private key are stored in a PKCS #12 (.p12) password-encrypted file.
 - *Certificate*: Select this option if you are importing an existing certificate whose certificate file (.cert) and key file (.key) are stored separately. The private key is password-encrypted.The remaining fields vary by your selection in *Type*.
4. Configure the following:
 - *Certificate file*: Enter the location of the previously .cert or .pem exported certificate (or, for PKCS #12 certificates, the .p12 certificate-and-key file), or click *Browse* to locate the file.
 - *Key file*: Enter the location of the previously exported key file, or click *Browse* to locate the file.

This option appears only when *Type* is *Certificate*.
 - *Password*: Enter the password that was used to encrypt the file, enabling the FortiVoice unit to decrypt and install the certificate.

This option appears only when *Type* is *PKCS12 certificate* or *Certificate*.
5. Click *OK*.

Downloading a PKCS #12 certificate

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

To download a PKCS #12 file

1. Go to *System > Certificate > Local Certificate*.
2. Click the row that corresponds to the certificate in order to select it.
3. Click *Download*, then select *Download PKCS12 File* on the pop-up menu.

A dialog appears.
4. In *Password* and *Confirm password*, enter the password that will be used to encrypt the exported certificate file. The password must be at least four characters long.
5. Click *Download*.
6. If your browser prompts you for a location to save the file, select a location.
7. Your web browser downloads the PKCS #12 (.p12) file. For information on importing a PKCS #12 file, see [“Importing a certificate” on page 97](#).

Managing certificate authority certificates

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

Managing the certificate revocation list

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

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

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

Maintaining the system

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

This topic includes:

- [Maintaining the system configuration](#)
- [Downloading a trace file](#)
- [Capturing voice and fax packets](#)

Maintaining the system configuration

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

Backing up configuration

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

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

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

To back up the configuration file

1. Go to *System > Maintenance > Configuration*.
2. In the *Backup Configuration* 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 659](#).

To schedule a configuration backup

1. Go to *System > Maintenance > Configuration*.
2. Under *Scheduled Backup*, configure the schedule time and the maximum backup number. When the maximum number is reached, the oldest version will be overwritten.

3. Enable *Local backup* if you want to back up locally.
4. Enable *Remote backup* and configure the FTP/SFTP server credentials if you want to back up remotely.
5. Click *Apply*.

Restoring the configuration

In the *Restore Configuration* area under *System > Maintenance > Configuration*, you can restore the backup FortiVoice configuration from your local PC. For details, see [“Restoring the configuration” on page 265](#).

Restoring the firmware

In the *Restore Firmware* area under *System > Maintenance > Configuration*, you can install a FortiVoice firmware from your local PC. For details, see [“Installing firmware” on page 262](#).

Downloading a trace file

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

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

To download a trace file

1. Go to *System > Maintenance > Configuration*.
2. At the bottom of the tab, click *Download trace log*.
Your web browser downloads trace.log.gz.

Configuring Phone System Settings

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](#)
- [Configuring advanced phone system settings](#)
- [Managing sound files and music on hold](#)
- [Working with FortiVoice profiles](#)

Configuring phone system settings

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



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

This topic includes:

- [Setting PBX location and contact information](#)
- [Configuring PBX options](#)
- [Customizing email history report and notification email templates](#)

Setting PBX location and contact information

Identify the FortiVoice unit's location and its number.

To set the PBX location

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

GUI field	Description
Country	Select the country where the FortiVoice unit is in.
Emergency number	Click the default number (911) to enter the emergency call number of the selected country.
Long-distance prefix	Click the default number (1) to enter the prefix for dialing long-distance calls.
International prefix	Click the default number (011) to enter the prefix for dialing international calls.
Outside line prefix	Click the default number (9) to enter the prefix for making outbound calls.

Area code	Click the default number (613) to enter the <i>Area code</i> for the main number of the FortiVoice unit. This code is provided by your PSTN service provider.
Area code is 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	<p>Select a new default prompt language for the FortiVoice unit. The default is English.</p> <p>This setting affects all of the FortiVoice unit's voice prompts, such as auto attendant and voice mail. However, if you change the sound file for an individual component, such as auto attendant, to use a different language, it will override the default prompt language for this component.</p> <p>For information on adding prompt languages, see “Adding prompt languages” on page 113.</p>
Contact Information	Optionally, enter your contact information.
Emergency setting	<p>Configure to send an alert email when an emergency call is made.</p> <p>Select <i>Do nothing</i> if you don't want the FortiVoice unit to send an alert email. Otherwise, select <i>Send alert email</i> and enter the email address.</p>

3. Click *Apply*.

Configuring PBX options

The *Phone System > Settings > Options* 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 [“Setting up local extensions” on page 133](#).

The FortiVoice unit supports the following pattern-matching syntax:

Table 15:Pattern-matching syntax

Syntax	Description
X	Matches any single digit from 0 to 9.
Z	Matches any single digit from 1 to 9.
N	Matches any single digit from 2 to 9.
[15-7]	Matches a single character from the range of digits specified. In this case, the pattern matches a single 1, as well as any number in the range 5, 6, 7.

Table 15:Pattern-matching syntax

Syntax	Description
.	Wildcard match; matches one or more characters, no matter what they are.
!	Wildcard match; matches zero or more characters, no matter what they are.
, ; or (space)	These pattern delimiters allow you to enter multiple pattern strings at a time. For example, you can enter NXXX,6XXXX;[3-5]X





Table 16:Pattern-matching examples

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

To configure PBX options

1. Go to *Phone System > Settings > Options*.
2. Configure the following:

Number Management

Extension number pattern:
Speed dial pattern:
System prohibited prefix:  
System unrestricted prefix:  

Operator extension:
Supporting extension:

Default Setting

Default SIP user password: ☐ Specified ☒ Generated
Password:
Default user PIN: ☒ Specified ☐ Generated
User PIN:
User ID prefix:
Default ring duration:

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 133 .
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 218 .
System prohibited prefix	Enter the phone number prefix that you want to ban, such as 900. Click the + sign to add up to 10.
System unrestricted prefix	Enter the allowed phone number prefix, such as 800. Click the + sign to add up to 10.
Operator extension	Enter the extension for the operator of the FortiVoice unit.
Supporting extension	Enter the extension for technical support of the FortiVoice unit.
Default Setting	
Default SIP user password	<p>Enter your own password or let the FortiVoice unit generate one for you. This password is used for configuring your SIP phone from the phone or the Web. You need the phone's IP to access it from the Web. This password appears when you add an extension. For details, see “Configuring IP extensions” on page 133.</p> <ul style="list-style-type: none"> <i>Specified:</i> 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. <i>Generated:</i> Select to have a system-generated password.
Default user PIN	<p>Enter your own password or let the FortiVoice unit generate one for you. This password is for the extension user to access voice mail and the user web portal. This password appears when you add an extension. For details, see “Configuring IP extensions” on page 133.</p> <p>If you select <i>Specified</i>, the default password is 123123.</p>

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 133 .
Default ring duration	Enter the time, in seconds, for a phone connected to the FortiVoice unit to ring before the call is processed (for example, the call is sent to voice mail). The default is 20.

3. Click *Apply*.

Customizing email history report and notification email templates

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

The FortiVoice unit sends out email history reports based on your call report configuration (see [“Configuring report email notifications” on page 254](#)) and notification email when you have a new voicemail or fax in your mailbox or missed a call. You can customize the email templates for the email 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, see [Table 18 on page 106](#), [Table 22 on page 107](#), and [Table 23 on page 107](#).

To customize email templates

1. Go to *Phone System > Settings > Custom Message*.
2. Open *Email templates* to display the default templates.
3. To edit a template, double-click it or select it and click *Edit*.
4. To format email template in HTML, use HTML tags, such as `some bold text`.
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.

Table 17:Default generic alert email notification template variables

Variable	Description
%%NOTIFY_FROM%%	The email address, such as <code>notify@example.com</code> , used to send notifications.
%%SUBJECT%%	The subject of the notification.
%%CONTENT%%	The content of the notification.

Table 18: Default generic email notification template variables

Variable	Description
%%ORIG_ENVELOP_FROM%%	The mail sender's address. This is the address for bounce messages.
%%ORIG_FROM%%	The email address of the original notification sender.
%%ORIG_SUBJECT%%	The subject of the original notification.
%%ORIG_DATE%%	The date and time when the original notification is sent.
%%NOTIFY_FROM%%	The email address, such as <code>notify@example.com</code> , used to send the original notifications.
%%NOTIFICATION_TO%%	The email address of the notification receiver in the header of the notification.
%%ORIG_TO%%	The email address of the original notification receiver.

Table 19:Default emergency call email template variables

Variable	Description
%%EMGCALL_CALLER_NAME%%	The name of the person who made the emergency call.
%%EMGCALL_DATE%%	The date when the emergency call was made.
%%EMGCALL_DURATION%%	The duration of the emergency call.
%%EMGCALL_CALLER_NUM%%	The phone number of the person who made the emergency call.
%%EMGCALL_DIAL_NUM%%	The emergency number that was dialed.
%%EMGCALL_VIA_TRUNK%%	The trunk through which the emergency call was made.

Table 20:Default incoming fax notification email template variables

Variable	Description
%%FAX_CALLERID%%	The ID/number from where the fax is sent.
%%FAX_NUM%%	The number to which the fax was sent.
%%FAX_DATE%%	The date when the fax was received.

Table 21:Default outgoing fax notification email template variables

Variable	Description
%%FAX_DATE%%	The date when the fax was sent.
%%FAX_NUM%%	The number to which the fax was sent.
%%FAX_STATUS%%	The delivery status of the fax.
%%FAX_HEADER_INFO% %	The fax header information.
%%FAX_SENT_TIME%%	The time used to send the fax.

Table 22: Default missed call email template variables

Variable	Description
%%MISSED_CALLERID%%	The caller ID of the caller whose call is missed.
%%MISSED_CALLERNUM%%	The phone number of the caller whose call is missed.
%%MISSED_DIAL_NUM%%	The phone number that the missed phone caller dialed.
%%MISSED_DATE%%	The day, date, and time when the call was missed.

Table 23:Default voicemail notification email template variables

Variable	Description
%%VM_CALLERID%%	The phone number of the caller who left the voicemail.
%%VM_DUR%%	The duration of the voicemail.
%%VM_MSGNUM%%	The order of the voicemail out of the total number of messages in the voice mailbox.
%%VM_DATE%%	The day, date, and time when the voicemail was left.
%%VM_MAILBOX%%	The extension number of the mailbox where the voicemail was left.
%%VM_NAME%%	The name of the person to whom the notification is sent.

Table 24:Default trunk saturation alert email template variables

Variable	Description
%%CONFIG_MAX%%	The maximum channels configured on the trunk.
%%HOST_NAME%%	The host name of the PBX.
%%INUSED_CHANNEL%%	The total number of channels in use on the trunk.
%%IN_NUM%%	The total number of incoming channels on the trunk.
%%IP%%	The IP address of the PBX.
%%OUT_NUM%%	The total number of outgoing channels on the trunk.
%%TRUNK_NAME%%	The name of the trunk.

Creating variables

In addition to the predefined variables, you can create new ones to customize replacement messages and email templates. Typically, these variables represent messages that you will use frequently. You can modify the variables that you create, but you cannot edit or delete the predefined variables.

To create a new variable

1. To create new variables to be used in custom messages, go to *PBX > Setting > Custom Message*.
2. Select a replacement message or email template where you want to add a new variable, and click *Edit Variable*.

The *Edit Variable* page appears.

3. Click *New*.

A dialog appears.

4. Configure the following:

- In *Name*, enter the variable name to use in the replacement message. Its format is: %%<variable_name>%%. For example, if you enter the word `voicemail_callerid`, this variable will appear as %%voicemail_callerid%% in the replacement message if you select to insert it. This is usually a simple and short form for a variable.
- In *Display Name*, enter words to describe the variable. For example, use `voicemail date` for the variable `vm_date`. The display name appears in the variable list when you select *Insert Variables* while customizing a message or creating a variable.
- In *Content*, enter the variable's content. Click *Insert Variables* to include any other existing variables, if needed. For example, you may enter
Please be notified that you have a message from
%%voicemail_callerid%% in your mailbox on %%vm_date%%.

To add a color code, use HTML tags, such as `<tr bgcolor="#3366ff">`. You can select a color code, such as "#3366ff" in the HTML tag, from the color palette after selecting *Insert Color Code*.

5. Click *OK*.

Configuring advanced phone system settings

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

This topic includes:

- Configuring SIP settings
- Configuring SIP phone auto-provisioning
- Adding prompt languages
- Managing phone configurations
- Configuring system capacity

Configuring SIP settings

FortiVoice units support SIP communications.

To configure FortiVoice SIP settings

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

Figure 31: SIP settings

Transport Setting

☒ Enable UDP

UDP port: 5060

☐ Enable TCP

TCP port: 5060

☒ Enable TLS

TLS port: 5061

Registration Interval

Extension registration interval range: 1 ~ 480 (Minutes)

Internal extension registration interval: 30 (Minutes)

External extension registration interval: 120 (Seconds)

Networks

External static Host/IP: 64.26.140.151

Port: 5566

RTP Setting

RTP port start: 6000

RTP port end: 6200

RTP timeout: 60 (Seconds)

RTP hold timeout: 300 (Seconds)

TLS Client Setting

☐ Server certificate verification

TLS protocol: TLSv1

Security

☐ Allow anonymous call

Advanced Setting

Enable early media: ☐

Apply

Cancel

GUI field	Description
-----------	-------------

Transport Setting	<p>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).</p> <p>Enable the ports as required.</p>
Registration Interval	
Extension registration interval range	<p>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.</p> <p>The default range is 1-480.</p> <p>The start of the range is 1-60 and the end of the range is 30-1440.</p>
Internal extension registration interval	<p>Enter the default registration time interval for the extensions on your subnet as required by the FortiVoice unit in minutes. The default is 30 and the range is 10-480.</p> <p>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.</p>
External extension registration interval	<p>Enter the default registration time interval for the extensions on other subnets as required by the FortiVoice unit in seconds. The default is 30 and the range is 10-1800.</p> <p>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.</p>
Networks	
External static Host/IP	Enter the FortiVoice unit's external static IP address to which the external extensions register. Also enter the port number.
RTP Setting	
RTP port start	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.
RTP port end	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.
RTP 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.

RTP 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.
TLS Client Setting	<p>If you have enabled TLS, configure the following:</p> <ul style="list-style-type: none"> • <i>Server certificate verification</i>: Select this option for the TLS clients to confirm the validity of a server's credentials with a trusted root certification authority's (CA's) certificates. For information on uploading a CA certificate, see “Managing certificate authority certificates” on page 98. • <i>TLS protocol</i>: Select the TLS protocol version.
Security	By default, the FortiVoice unit screens out calls from callers who have blocked their caller ID information. If you want to change this default setting, select <i>Allow anonymous call</i> .
Advanced Setting	<p>Select <i>Enable early media</i> if you want the FortiVoice unit to relay a ring tone to the caller of an incoming call before the establishment of a call connection. A ring tone or a busy tone is early media.</p> <p>If you select this option, you also need to configure a specific trunk to send the ring tone. See “Inband ringtone” on page 173.</p>

3. Click *Apply*.

Configuring SIP phone auto-provisioning

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

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

The FortiVoice unit can only auto provision the supported FortiFones.

To configure auto-provisioning settings

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

Figure 32: Auto-provisioning settings

Auto Provisioning Setting

☒ Enabled

☒ Generate default configuration for unassigned phone

PIN for phone configuration:

Server Settings for Phone Configuration

☐ Standard (apply to all server settings)

☒ Use IP address of interface:

☐ Use static IP or host name:

☒ Advanced

SIP Server:

☒ Use IP address of interface:

☐ Use static IP or host name:

TFTP Server:

☒ Use IP address of interface:

☐ Use static IP or host name:

NTP Server:

☒ Use IP address of interface:

☐ Use static IP or host name:

Apply

Cancel

GUI field	Description
Auto Provisioning Setting	
Enabled	Select to activate the SIP phone auto-provisioning function for auto discovering the phones.
Generate default configuration for unassigned phone	<p>Select to generate phone configuration files for the supported unassigned SIP phones. For details, see “Viewing unassigned phones” on page 27.</p> <p>With this option selected, once a supported SIP 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.</p> <p>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.</p>
PIN for phone configuration	<p>Enter a password to be used by a FortiFone that connects to the FortiVoice unit to set mobile extension number.</p> <p>For example, you can press the default Configure Phone feature code *17 (See “Modifying feature access codes” on page 241) on any FortiFone that connects to the FortiVoice unit and enter this password. You can then enter an existing extension to set it as the extension of this phone.</p>
Server Settings for Phone Configuration	

Fortinet Technologies Inc.

Page 112FortiVoice Enterprise Phone System 4.0.0 Administration Guide

Standard (apply to all server settings)	<p>Select to configure the server settings for the supported phones. The same settings apply to the SIP server, TFTP server, and NTP server.</p> <ul style="list-style-type: none"> • <i>Use IP address of interface:</i> Select the interface for the server. The SIP phones connect to this server to register and receive the PBX setup information and use it as the NTP server. For information on interface configuration, see “Configuring the network interfaces” on page 40. • <i>Use static IP or host name:</i> Enter the current public IP address or public domain name of the server. The SIP phones connect to this server to register and receive the PBX setup information and use it as the NTP server.
Advanced	<p>If you use different servers for SIP, TFTP, and NTP, select to configure the settings of each server for the supported phones.</p> <ul style="list-style-type: none"> • <i>SIP server</i> <ul style="list-style-type: none"> • <i>Use IP address of interface:</i> Select the interface for the server. The SIP phones connect to this server to register. • <i>Use static IP or host name:</i> Enter the current public IP address or public domain name of the server. The SIP phones connect to this server to register. • <i>TFTP server</i> <ul style="list-style-type: none"> • <i>Use IP address of interface:</i> Select the interface for the server. The SIP phones connect to this server to receive the PBX setup information. • <i>Use static IP or host name:</i> Enter the current public IP address or public domain name of the server. The SIP phones connect to this server to receive the PBX setup information. • <i>NTP server</i> <ul style="list-style-type: none"> • <i>Use IP address of interface:</i> Select the interface for the server. The SIP phones connect to this server to synchronize time. • <i>Use static IP or host name:</i> Enter the current public IP address or public domain name of the server. The SIP phones connect to this server to synchronize time.

2. Click *Apply*.

Adding prompt languages

The prompt language affects all of the FortiVoice unit's voice prompts, such as auto attendant and voicemail. Prompt languages are used when configuring the PBX settings. For more information, see [“Setting PBX location and contact information” on page 101](#).

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

The default prompt language is English.

For information on generating a prompt language file, see [“Recording in FortiVoice audio format” on page 114](#).

To add a prompt language

1. Go to *Phone System > Advanced Settings > Prompt Languages*.
2. Click *New*.
3. In the *Upload* field, click *Browse* to upload the language file provided by Fortinet Technical Support.
4. Click *OK*.

Recording in FortiVoice audio format

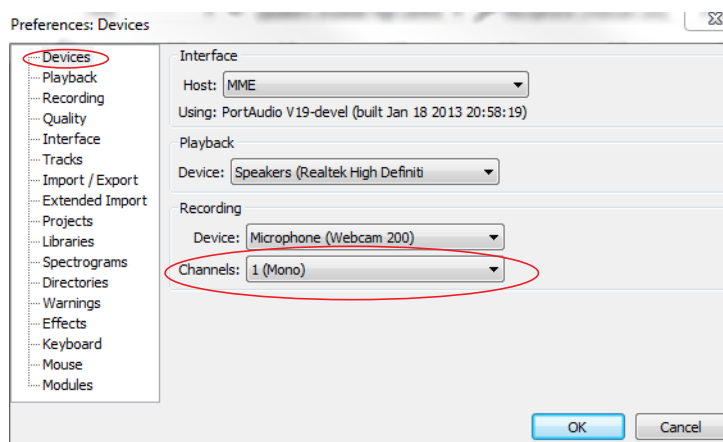
A prompt language file must be recorded in the FortiVoice language package format. This can be accomplished by using the free and robust audio program called Audacity which can be downloaded from <http://audacity.sourceforge.net> and a microphone.

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

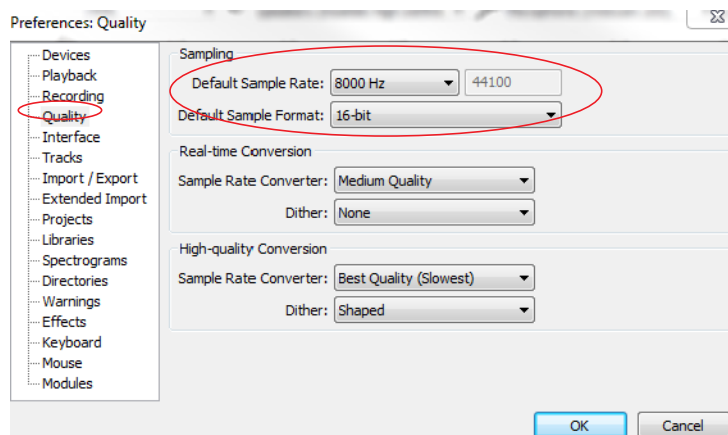
Audacity cannot natively record in the format that FortiVoice unit requires. Therefore, some adjustments need to be made in the software as described in the following procedure.

To generate a prompt language file

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



3. Click the *Quality* menu and set the *Default Sample Rate* to 8000 Hz and the *Default Sample Format* to 16 bit.

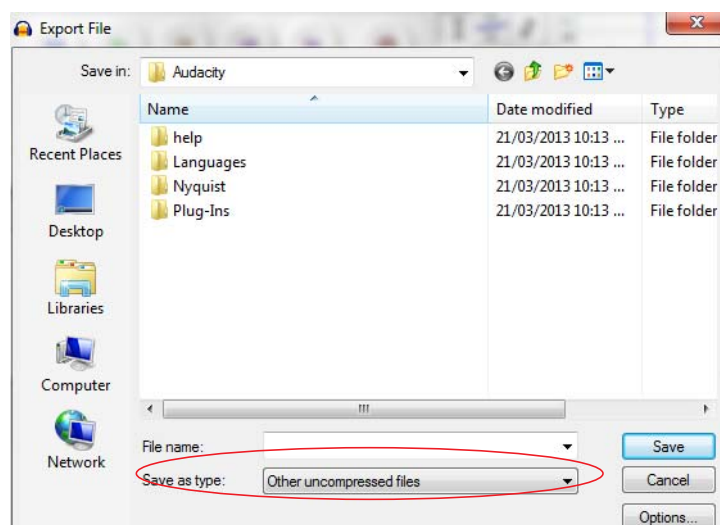


4. Click *OK*.

5. Click the *Record* button when ready to start recording the file. When finished recording, click *Stop*.

The completed recording can now be saved in a format to work with the FortiVoice unit.

6. Go to *File > Export*.
7. For *Save As Type*, select *Other compressed files*.



8. Click *Options*.
9. For *Encoding*, select *U-law*. Click *OK*.
- 10.. Select the directory in which to save the recording and then click *Save*.

The recording is now in a format that can be loaded into the FortiVoice unit.

Managing phone configurations

The FortiVoice unit provides the default configuration templates for the phone types with *Limited* support level. In most cases, there is no need to modify the templates. If you do need to make changes to a template (for example, change the IP address of the NTP server), make sure the format matches that of the default template. Otherwise, phone auto-provisioning will not be possible. This is because the template is part of the configuration file generated for the phone type and will be sent to a phone of this type through auto provisioning. For details, see [“Configuring SIP phone auto-provisioning” on page 111](#).

The phones with *Comprehensive* support level do not display their configuration templates because the FortiVoice unit fully supports the phones.

You can also manage the phone firmwares on the FortiVoice unit.

Once you have modified the templates or uploaded a new firmware, they are saved on the FortiVoice unit. To send them to the phones, choose a low traffic time and reboot the phones. For information on rebooting the phones, see [“Setting up local extensions” on page 133](#).

If your organization adds new FortiPhones that use a different range of MAC addresses than your current ones and you want to add them to the FortiVoice unit in order to auto-provision them, you can do so by adding the new phones' MAC address.

To manage a phone firmware

1. Go to *Phone System > Advanced Settings > Phone Management*.
2. Select the phone type of which you want to manage the firmware.
3. Click *Manage*.
4. In the pop-up window, double-click a firmware folder under *Name*.

5. Remove or save an existing firmware, or upload a new firmware in .tar format that does not include any subdirectories. You can also activate or deactivate a firmware.

To configure a phone profile

1. Go to *Phone System > Advanced Settings > Phone Management*.
2. Click *Phone Profile*.
3. See [“Configuring phone profiles” on page 122](#).

To add new FortiFones MAC address

1. Go to *Phone System > Advanced Settings > Phone Management*.
2. Click *Additional Phone/MAC*.
3. Click *New*.
4. For *MAC address*, enter the FortiFone MAC address in the following format:
AA:BB:CC:00:00:00.
5. Leave the *Phone Type* field as is. Currently, this feature only supports FortiFone.
6. Select *Status*.
7. Click *Create*.

The new FortiFones are recognized by the FortiVoice unit. You can auto-provision them now. For more information, see

Configuring system capacity

The *Phone System > Advanced Settings > Miscellaneous* tab lets you set the number of currently connected calls allowed on the FortiVoice unit, configure voicemail greeting and message length, set phone directory options, and configure CDR settings.

To configure system capacity

1. Go to *Phone System > Advanced Settings > Miscellaneous*.
2. Under *Concurrent Calls*, enter the outbound and inbound concurrent call limits you want.
3. Under *Voicemail*, enter the maximum message and greeting length you want.
4. Configure *Directory* to set phone directory options:
 - For *Dial-by-name option*, select how a caller can check the directory by dialing a name.
 - For *Dial-by-name digits*, enter the number of letters allowed for a caller to dial someone by name. The range is 3-9. This feature enables a caller to reach a specific person quickly by dialing, for example, the first three letters of their first or last name from any phone.
 - For *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.
5. Under *CDR*, enter the time in month that you want to keep the call log/call detail record and the maximum number of CDR records. For information about call log/CDR, see [“Viewing call records” on page 31](#).
6. Click *Apply*.

Managing sound files and music on hold

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

There are default sound files ready to use.

The sound files can be used when configuring music on hold, conference calls, and auto attendants. See [“To configure music on hold” on page 117](#) and [“Configuring Call Features” on page 206](#).

To manage a sound file

1. Go to *Phone System > Audio > Prompts*.
2. Click *New*.
3. Enter a name for the file.
4. Select a profile type.
5. Optionally, enter a description for the file.
6. For *Voice language*, configure the following:

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

- i. To record a sound file, click *Record*.
- ii. 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 133](#).
- iii. When the extension rings, record the sound file and hang up.
- iv. On the FortiVoice web-based manager, click *Yes* on the *Voice recording request sent to specified extension* dialog box.

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

7. Click *OK*.

To configure music on hold

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

<i>GUI field</i>	<i>Description</i>
Name	Enter a name for the music on hold file.
Mode	
Files	<p>If you select to use existing sound files, do the following:</p> <ul style="list-style-type: none">• For <i>Sound files</i>, select the <i>Available</i> sound files and click -> to move them into the <i>Selected</i> field. You can use the <i>Up</i> and <i>Down</i> buttons to reorder the files.• For <i>Play mode</i>, if you want to play the selected sound files randomly, select <i>Random</i>. If you want to play the files according to the order in the <i>Selected</i> field, select <i>Sequential</i>.

Stream	If you select to use streaming files, in the <i>Stream URL</i> 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 <i>Test stream</i> to see if the URL is added successfully. Before doing so, make sure to only use the legal stream sources.
Description	Optionally, enter a description for the file.

4. Click *Create*.

Working with FortiVoice profiles

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

This topic includes:

- [Configuring SIP profiles](#)
- [Modifying caller IDs](#)
- [Scheduling the FortiVoice unit](#)
- [Configuring phone profiles](#)
- [Configuring LDAP profiles](#)
- [Configuring user privileges](#)

Configuring SIP profiles

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



Communicate with your VoIP service provider because the profile 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 not be deleted.

For information on extensions, see [“Configuring Extensions” on page 133](#).

For information on SIP trunks, see [“Configuring Trunks” on page 170](#).

To configure a SIP profile

1. Go to *Phone System > Profiles > SIP* and click *New*.

2. Configure the following:

GUI field	Description
SIP	<ul style="list-style-type: none">• <i>Name</i>: Enter a name for this profile.• <i>DTMF</i>: Select the dual-tone multi-frequency (DTMF) method used by the VoIP provider. Options are RFC2833, Inband, Info, Shortinfo, and Auto. Auto means the VoIP provider's server and the FortiVoice unit will negotiate to select a DTMF method. You could also select a specific DTMF method if required.• <i>NAT</i>: Select if the VoIP service provider supports SIP NAT translation.• <i>Video</i>: Select if the service provider supports video calling over SIP.• <i>Direct media stream</i>: Select if the VoIP service provider supports direct media transfer to extensions by bypassing the PBX in between.• <i>T.38</i>: Select if the VoIP service provider supports fax over VoIP network.• <i>Monitor/Keep alive (SIP notify) interval</i>: 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.

Transport	<p><i>Encryption:</i> Select <i>TLS</i> to encrypt the system connection between an extension and the FortiVoice unit. Select <i>TLS and SRTP</i> to encrypt both the system connection and voice communication between an extension and the FortiVoice unit.</p> <p>This option only applies to FortiFone x60 series with firmware version of 1.2.0.4 or later.</p> <p>To make this option work, you need to select a SIP profile with <i>TLS</i> or <i>TLS and SRTP</i> selected for <i>Encryption</i> when configuring an extension. You also need to enable TLS on the FortiVoice unit by going to <i>Phone System > Advanced Settings > SIP</i>.</p> <p><i>Transport:</i> 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).</p> <p>Enable the protocols as required.</p> <p>This option, if applied to a user, overrides the system-wide transport settings. For more information, see “Configuring SIP settings” on page 109.</p> <p><i>Secure RTP:</i> Select to provide encryption, message authentication and integrity, and replay protection to the FortiVoice Real-time Transport Protocol data.</p>
Codec	<p>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.</p> <p>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.</p>

3. Click *Create*.

Modifying caller IDs

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

Caller ID modifications are used when configuring dial plans. For more information, see [“Configuring Call Routing” on page 189](#).

To modify a caller ID

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

<i>GUI field</i>	<i>Description</i>
Name	Enter the name for this caller ID modification record.
Match number	<p>Enter the extension number or number pattern you want to modify.</p> <p>For example, you can enter 8134 to modify a single extension, or 81xx to modify all the four-digit numbers starting with 81.</p>

Number Modification	<p>If you have entered a <i>Match number</i>, configure the following values to modify it:</p> <ul style="list-style-type: none"> • <i>Strip</i>: Enter a number to hide the starting part of an extension from displaying. 0 means no action. For example, if your <i>Match number</i> is 8134 and <i>Strip</i> is 2, only 34 will be displayed as caller ID. • <i>Truncate</i>: Enter a number to hide the ending part of an extension from displaying. 0 means no action. For example, if your <i>Match number</i> is 8134 and <i>Truncate</i> is 2, only 81 will be displayed as caller ID. • <i>Prefix</i>: Add a number before an extension. For example, if your <i>Match number</i> is 8134 and <i>Prefix</i> is 5, the caller ID will be 58134. • <i>Postfix</i>: Add a number after an extension. For example, if your <i>Match number</i> is 8134 and <i>Postfix</i> is 5, the caller ID will be 81345.
Match caller ID name	<p>Enter the caller ID that you want to map to another one.</p> <p>Caller IDs are created when configuring SIP extensions. See “Configuring IP extensions” on page 133.</p>
Map to new caller ID name	<p>Enter the new caller ID name to which you want to map the one entered in the <i>Match caller ID name</i> field.</p>

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

Scheduling the FortiVoice unit

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

For information on dial plan, see [“Configuring Call Routing” on page 189](#).

For information on virtual numbers, see [“Working with virtual numbers” on page 168](#).

For information on call management, see [“Setting extension user preferences”](#) on page 152.

To schedule the operation time

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

Figure 33: PBX scheduling

Day	AM Schedule	PM Schedule	Full Day
Mon	9 : 00 to 12 : 00	12 : 00 to 17 : 00	<input type="checkbox"/>
Tue	9 : 00 to 12 : 00	12 : 00 to 17 : 00	<input type="checkbox"/>
Wed	9 : 00 to 12 : 00	12 : 00 to 17 : 00	<input type="checkbox"/>
Thu	9 : 00 to 12 : 00	12 : 00 to 17 : 00	<input type="checkbox"/>
Fri	9 : 00 to 12 : 00	12 : 00 to 17 : 00	<input type="checkbox"/>
Sat	9 : 00 to 12 : 00	12 : 00 to 17 : 00	<input type="checkbox"/>
Sun	9 : 00 to 12 : 00	12 : 00 to 17 : 00	<input type="checkbox"/>

Date	Description
------	-------------

GUI field	Description
Name	Enter a name for the schedule.
Week Day	Select the days to include in the schedule and set the AM and PM time or select <i>Full Day</i> .
Holiday	Click <i>New</i> to set the holidays. For example, select 01/01/12 in the <i>Date</i> field and enter New Year's Day in the <i>Description</i> field, and click <i>Create</i> .

3. 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 133.

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

To configure a phone profile

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

Figure 34: Configuring a phone profile

Phone profile

Name:

Phone type:

FortiFone-350i/360i

Description:

Configuration mode:

☐ Automatic ☒ Manual

Manual Configuration

[LAN]

; uncomment and assign value to enable vlan

; pc_802_priority 3

; phone_802_priority 5

; pc_vlan_id 0

; phone_vlan_id 0

[NETTIME]

time_format 1

date_format m-DD

sntp_server_address %%FV_NTP_SERVER%%

timezone %%FV_TIMEZONE%%

dst_auto_adjust %%FV_DST_AUTO_ADJUST%%

dst_start_month 3

dst_start_day 0

dst_start_day_of_week 1

dst_start_week_of_month 2

dst_start_time 2

dst_stop_month 11

dst_stop_day 0

Reset To Default

Create

Cancel

GUI field	Description
Phone profile	
Name	Enter a name for the profile.
Phone type	Select a phone model for the profile.
Description	Enter any notes you have for this profile.
Configuration mode	Select the profile mode. <ul style="list-style-type: none"><i>Automatic</i>: the FortiVoice unit will generate a phone configuration file based on the information you provide. See “Automatic Configuration” on page 124. This option is only available for FortiFone-260i and above.<i>Manual</i>: This option allows you to manually edit the phone configuration file. See “Manual Configuration” on page 125

Vlan	<p>You may need to deploy phones using the existing IT infrastructure which only has one network drop for each employee. The network switch supports 802.1Q VLAN tagging and LLDP-MED. Some phones such as FortiFones have two network ports: LAN and PC. The recommended solution is to connect FortiFones to the switch using LAN port and connect the computer to the PC port of FortiFones. VLAN tag needs to be enabled to segregate FortiFone voice network and PC data network.</p>
Option	<p>If you select <i>Manual</i>, configure the following:</p> <p><i>ID for voice</i>: Enter your organization's VLAN ID for voice.</p> <p><i>ID for data</i>: Enter your organization's VLAN ID for data.</p> <p><i>Priority for voice/data</i>: Enter the traffic service level recommended by the IEEE. Each number represents a traffic type. The range is from 0-7, with 7 being the highest.</p> <ul style="list-style-type: none"> • 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 <p>If you select <i>LLDP</i> (Link Layer Discovery Protocol), the FortiVoice unit automatically generates the configuration file. You need to enable LLDP support on your network switch.</p>
Automatic Configuration	<p>This option is only available if you select <i>Automatic</i> for <i>Configuration mode</i>.</p>
Display option	<p>Select what to display on the extension: the extension user's name only or name and number.</p>
Provisioning lines	<p>Enter the number of phone lines to which this profile applies. The maximum lines that you can provision is 4.</p>
Digit map pause timer	<p>Enter the digit map timeout in seconds which defines the waiting time between the completion of dialing number entering and initiating the call.</p> <p>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.</p>

Digit map	<p>The FortiVoice unit uses digit map syntax definition to define the FortiFone dialing behavior. A phone needs to know when number entering is complete and therefore to initiate the call.</p> <p>You can enter the syntax or use the default syntax <code>x.T x+#</code> where:</p> <ul style="list-style-type: none"> • <code>x.T</code> means you can dial any number and the call is initiated after the digit map pause timeout is reached. • <code> </code> is a choice operator that matches the expression before or after the operator. For example, <code>abc def</code> matches "abc" or "def". • <code>x+#</code> means you can enter any number and then press the # key to initiate the call. <p>For more information about digit map syntax definitions, see Section 2.1.5 of RFC 3435.</p>
Set Programmable Phone Key	<p>Allows you to program the phone keys for FortiFone-260i to 560i. For FortiFones with expansion modules, you can select the module to program the keys.</p> <p>After completing programing the keys, you can click <i>Download printable label</i> to save and print out the configuration and label it on the phone.</p> <p>Note that keys 1 and 2 are reserved and cannot be programmed.</p> <p>If you select <i>One key dial</i> or <i>User defined</i> function for a key, you need to enter the information in the <i>Resource</i> field based on your phone configuration. For example, if you select <i>User defined</i> for key 3 and you want to map this key to your voicemail code such as *78, enter *78 in the <i>Resource</i> field.</p> <p>Selecting <i>Centralized phonebook</i> allows you to browse the phone book from a FortiFone. You can also search on FortiFones by name or number. Please note that this feature works on top of HTTP protocol which is disabled by default in system interface settings. If you want to use this feature, enable HTTP under <i>System > Network > Network</i>.</p>
Manual Configuration	<p>If you select <i>Manual</i> configuration mode, edit the phone configuration file.</p>

3. Click *Create*.

Configuring LDAP profiles

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



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

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

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

Figure 35:Viewing the list of LDAP profiles

Profile Name	Server	Port	Auth	Cache	
ldap169	172.20.140.169	389	✓	✗	•
qq	172.20.140.193	389	✓	✗	•

GUI field	Description
Clone	Click the row corresponding to the profile whose settings you want to duplicate when creating the new profile, then click <i>Clone</i> . A single-field dialog appears. Enter a name for the new profile. Click <i>OK</i> .
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 <i>User Authentication Options</i> 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 > Profiles > LDAP*.
2. Click *New* to add a profile or double-click a profile to modify it.
A multisection dialog appears.

Figure 36: Configuring an LDAP profile

Edit LDAP Profile

Profile name:

Server name/IP:

Port:

389

Fallback server name/IP:

Port:

389

Use secure connection:

None

[Test LDAP Query...]

Base DN:

Bind DN:

Bind password:

[Browse...]

User Authentication Options

Try common name with base DN as bind DN

Common name ID:

Search user and try bind DN

Schema:

InetOrgPerson

LDAP user query:

{&(objectClass=inetOrgPerson)(telephonenumber=\$u)}

Scope:

Subtree

Derefer:

Never

Advanced Options

Timeout (seconds):

20

Protocol version:

LDAP Version 3

Enable cache

TTL (minutes):

1440

Enable user password change

Password schema:

OpenLDAP

Create

Cancel

GUI field	Description
Profile name	For a new profile, enter its name.
Server name/IP	<p>Enter the fully qualified domain name (FQDN) or IP address of the LDAP server.</p> <p><i>Port:</i> Enter the port number where the LDAP server listens.</p> <p>The default port number varies by your selection in <i>Use secure connection</i>: port 389 is typically used for non-secure connections, and port 636 is typically used for SSL-secured (LDAPS) connections.</p>
Fallback server name/IP	<p>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.</p> <p><i>Port:</i> Enter the port number where the fallback LDAP server listens.</p> <p>The default port number varies by your selection in <i>Use secure connection</i>: port 389 is typically used for non-secure connections, and port 636 is typically used for SSL-secured (LDAPS) connections.</p>

Use secure connection	<p>Select whether to connect to the LDAP servers using an encrypted connection.</p> <ul style="list-style-type: none"> • <i>none</i>: Use a non-secure connection. • <i>SSL</i>: Use an SSL-secured (LDAPS) connection. <p>Click <i>Test LDAP Query</i> to test the connection. A pop-up window appears. For details, see “Testing LDAP profile queries” on page 131.</p>
Base DN	<p>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 <code>ou=People,dc=example,dc=com</code>.</p> <p>User objects should be child nodes of this location.</p>
Bind DN	<p>Enter the bind DN, such as <code>cn=FortiVoiceA,dc=example,dc=com</code>, of an LDAP user account with permissions to query the <i>Base DN</i>.</p> <p>This field may be optional if your LDAP server does not require the FortiVoice unit to authenticate when performing queries.</p>
Bind password	<p>Enter the password of the <i>Bind DN</i>.</p> <p>Click <i>Browse</i> to locate the LDAP directory from the location that you specified in <i>Base DN</i>, or, if you have not yet entered a <i>Base DN</i>, beginning from the root of the LDAP directory tree.</p> <p>Browsing the LDAP tree can be useful if you need to locate your <i>Base DN</i>, or need to look up attribute names. For example, if the <i>Base DN</i> is unknown, browsing can help you to locate it.</p> <p>Before using, first configure <i>Server name/IP</i>, <i>Use secure connection</i>, <i>Bind DN</i>, <i>Bind password</i>, and <i>Protocol version</i>, then click <i>Create</i> or <i>OK</i>. These fields provide minimum information required to establish the directory browsing connection.</p>

3. Configure the following sections:

- [“Configuring authentication options” on page 128](#)
- [“Configuring advanced options” on page 130](#)

4. Click *Create*, *OK* or *Apply*.

The LDAP profile appears in the LDAP profile list. To apply it, select the profile in features that support LDAP queries, such as protected domains and policies.

Before using the LDAP profile in other areas of the configuration, verify the configuration of each query that you have enabled in the LDAP profile. Incorrect query configuration can result in unexpected phone processing behavior. For information on testing queries, see [“Testing LDAP profile queries” on page 131](#).

Configuring authentication options

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see [“Configuring LDAP profiles” on page 125](#).

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

4. Configure the following:

Figure 37: Configuring user authentication LDAP options

User Authentication Options

☐ Try common name with base DN as bind DN
Common name ID:

☒ Search user and try bind DN
Schema:
LDAP user query:
Scope:
Derefer:

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 <code>cn</code> or <code>uid</code> 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:

- *Schema*: If your LDAP directory's user objects use a common schema style:
 - InetOrgPerson
 - Active Directory

Select the schema style. This automatically configures the query string to match that schema style.

If your LDAP server uses any other schema style, select *User Defined*, then manually configure the query string.

- *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*.

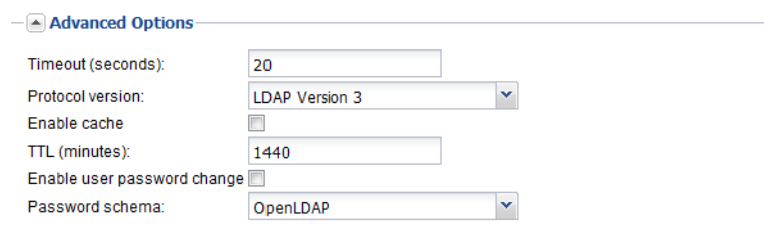
- *Scope*: Select which level of depth to query, starting from *Base DN*.
 - *One level*: Query only the one level directly below the Base DN in the LDAP directory tree.
 - *Subtree*: Query recursively all levels below the *Base DN* in the LDAP directory tree.
- *Derefer*: Select the method to use, if any, when dereferencing attributes whose values are references.
 - *Never*: Do not dereference.
 - *Always*: Always dereference.
 - *Search*: Dereference only when searching.
 - *Find*: Dereference only when finding the base search object.

Configuring advanced options

The following procedure is part of the LDAP profile configuration process. For general procedures about how to configure an LDAP profile, see [“Configuring LDAP profiles” on page 125](#).

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

Figure 38: Advanced Options section



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	<p>Enable to cache LDAP query results.</p> <p>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.</p> <p>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.</p>
TTL (minutes)	<p>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.</p> <p>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.</p> <p>This option is applicable only if <i>Enable cache</i> is enabled.</p>
Enable user password change	Enable if you want to allow FortiVoice web portal users to change their password.
Password schema	Select your LDAP server's user schema style, either <i>OpenLDAP</i> or <i>Active Directory</i> .

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 > Profiles > LDAP*.

2. Double-click the LDAP profile whose query you want to test.
3. Click *Test LDAP Query*.
4. A pop-up window appears allowing you to test the query.
5. From *Select query type*, select *Authentication*.
6. 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*.
7. In *Password*, enter the current password for that user.
8. 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 > Profiles > LDAP*.
2. Double-click the LDAP profile whose query cache you want to clear.
3. Click *Test LDAP Query*.
4. From *Select query type*, select *Clear Cache*.

A warning appears at the bottom of the window, notifying you that the cache for this LDAP profile will be cleared if you proceed. All queries will therefore be new again, resulting in decreased performance until the query results are again cached.

5. Click *Ok*.

The FortiVoice unit empties cached LDAP query responses associated with that LDAP profile.

Configuring user privileges

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

For more information, see [“Configuring user privileges” on page 213](#).

Configuring Extensions

The *Extensions* menu lets you configure local and remote extensions, virtual numbers, and extension department.

This topic includes:

- [Setting up local extensions](#)
- [Creating extension groups](#)
- [Setting up general voice mailboxes](#)
- [Working with virtual numbers](#)

Setting up local extensions

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

This topic includes:

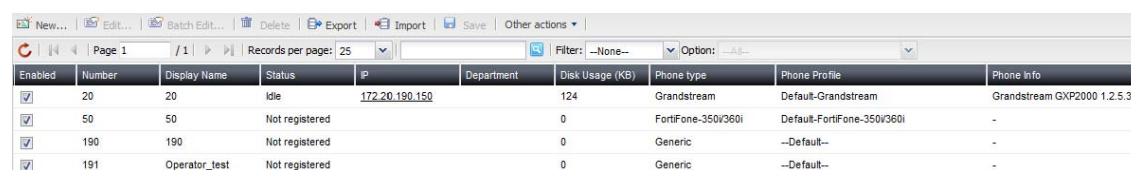
- [Configuring IP extensions](#)
- [Setting up general voice mailboxes](#)
- [Modifying analog extension \(200D-T model only\)](#)
- [Setting up remote extensions](#)
- [Configuring fax extensions](#)
- [Setting extension user preferences](#)

Configuring IP extensions

An IP extension is an IP phone connected through a network to a system. An internal IP extension is a phone connected on the same LAN as the system. An external IP extension is a phone connected outside the LAN.

To view the local IP extensions, go to *Extensions > Extensions > IP Extensions*.

Figure 39: IP extensions



Enabled	Number	Display Name	Status	IP	Department	Disk Usage (KB)	Phone type	Phone Profile	Phone Info
<input checked="" type="checkbox"/>	20	20	Idle	172.20.190.150		124	Grandstream	Default-Grandstream	Grandstream GXP2000 1.2.5.3
<input checked="" type="checkbox"/>	50	50	Not registered			0	FortiFone-350i/360i	Default-FortiFone-350i/360i	-
<input checked="" type="checkbox"/>	190	190	Not registered			0	Generic	--Default--	-
<input checked="" type="checkbox"/>	191	Operator_test	Not registered			0	Generic	--Default--	-

GUI field	Description
Batch Edit	If you want to apply the same changes to multiple extensions, select the extensions and click this option. Make the changes and click <i>Apply To All</i> .
Export	Select to save a copy of the extension list 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 141 .

Save	Click an extension's <i>Display name</i> or <i>Phone Type</i> to modify them and click this button to save the changes.
Other actions	<ul style="list-style-type: none"> • <i>Apply phone configuration</i>: If you have edited an extension configuration and want to apply it to the phone associated with this extension, select the extension and click this option. The selected phones will reboot and only the phones that meet the following conditions will receive the new configuration: <ul style="list-style-type: none"> • Phones supported by and registered to the FortiVoice unit. For the list of supported phones and auto provisioning prerequisites, see “Configuring SIP phone auto-provisioning” on page 111. • Phone type and MAC address is correctly configured. See “To create or edit an IP extension” on page 135. • Auto-provisioning is enabled for the extension associated with the phone through the user privilege applied to it. See “Configuring user privileges” on page 213. • <i>Maintenance</i>: Select an extension and click this button to manage a user's voicemail box. You can check the size of the box and empty the box. Click <i>Back</i> to return to the <i>SIP</i> tab. • <i>View phone configuration file</i>: Select a FortiFone extension and click this option to view the phone's configuration file. When a phone is associated with an extension, the FortiVoice unit generates a configuration file for the phone. For details, see “To create or edit an IP extension” on page 135. • <i>Check the password strength of SIP accounts</i>: See “Auditing SIP extension password” on page 140. • <i>Download programmable phone key labels</i>: If you need a copy of the programmable phone key labels of your users, select <i>All extensions</i> or <i>Selected extensions</i>, click <i>Yes</i> and then open or save the file.
Enabled	Select to activate an extension.
Number	The extension number.
Display Name	The name displaying on the extension. This is usually the name of the extension user.
Status	<p>The extension statuses, including:</p> <ul style="list-style-type: none"> • <i>Idle</i>: The extension is not in use. • <i>In Use</i>: The extension is in use. • <i>Busy</i>: The extension is busy. • <i>Ringing</i>: The extension is ringing. • <i>On Hold</i>: The extension has an on-hold call. • <i>Admin down</i>: The trunk of the extension is disabled • <i>Not registered</i>: The extension is not registered with the FortiVoice unit and is not in service. • <i>Unavailable</i>: The extension is not reachable. • <i>Alarm detected</i>: There is a problem with the phone line. • <i>Other</i>: The status other than the above.

IP	The link to the IP address of the phone using the extension number. See “IP” on page 140 .
Department	The link to the department of which this extension is a member. For information on creating departments, see “” on page 169 .
Disk Usage (KB)	Displays the size of disk space used by voicemails for the user in kilobytes (KB).
Phone Type	The type of phone for this extension.
Phone Profile	Displays the phone profile applied to the user. For information on phone profile, see “Configuring phone profiles” on page 122 .
Phone Info	The model of the phone for this extension.

To create or edit an IP extension

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

Figure 40: IP extension configuration

The screenshot displays the IP extension configuration interface, organized into three main sections:

- Extension Setting:** Contains fields for User ID (290), Number (290), Enabled (checked), Display name (870i_290), and External caller ID (e.g., Jim <612223>). It also includes a warning that the password policy is disabled, and fields for SIP password and User PIN, each with a Generate button and a View checkbox.
- Advanced Setting:** Includes dropdown menus for Location (Internal), SIP setting (t1srtp), User privilege (--None--), Department (--None--), and Phone type (FortiFone-870i). It also has fields for Handset ID (1) and Base MAC address (00:08:7b:0b:39:ae). The Phone profile section shows 'Admin defined' selected, with a dropdown set to 'Default-FortiFone-870i'.
- Extra Information:** Shows the IP address as 172.20.140.220.

At the bottom, there are 'OK' and 'Cancel' buttons.

GUI field	Description
-----------	-------------

Extension Setting	
--------------------------	--

User ID	<p>This is the system-generated ID based on the user ID prefix you set (see “User ID prefix” on page 105) and the extension number.</p> <p>This option is view only and only appears when you edit an extension. You can add a new user ID through the CLI. For more information, see the FortiVoice CLI Reference.</p>
Number	<p>Enter the extension number following the extension number pattern. See “Configuring PBX options” on page 102.</p>
Show suggested numbers	<p>Select and click in the <i>Number</i> field to display the extension numbers available for use. If it is deselected, clicking in the <i>Number</i> field displays the extension numbers already in use.</p> <p>This option also serves as a diagnostic tool for finding and fixing duplicate or missing numbers. Missing numbers are the extensions that have user IDs but not numbers.</p> <p>When there are duplicate or missing numbers, an orange exclamation mark icon appears beside this option. You can click the icon and fix the numbers. For more information, see “Fixing duplicate or missing numbers” on page 140.</p>
Enabled	<p>Select to activate the extension.</p>
Display name	<p>Enter the name displaying on the extension. This is usually the name of the extension user.</p>
External caller ID	<p>If you want to display a particular caller ID on a called phone instead of the FortiVoice main number (see “Main number” on page 102) or the trunk phone number (see “Phone Number” on page 175), enter it here. The format must be name<phone number>, such as HR<2221111234>.</p> <p>If this extension is mapped to a DID number and the <i>Outbound</i> option is also selected in DID mapping configuration, the external caller ID entry has priority. For information on DID mapping, see “Mapping DIDs” on page 194.</p>
SIP password	<p>Password policy warnings may appear above this field depending on your password/PIN policy configuration. You can click the warning notice to configure the policy. For details, see “Configuring system options” on page 78.</p> <p>Enter the password used for configuring your SIP phone from the phone or the Web. You need the phone's IP to access it from the Web.</p> <p>Click <i>Generate</i> to generate a strong password automatically. Select <i>View password</i> to display the password. This option is only available when you edit an extension.</p> <p>If you have configured the default SIP user password (see “Default SIP user password” on page 104), the password appears here. However, you can change it.</p>

User PIN	<p>Enter the password for the extension user to access voicemail and the user web portal.</p> <p>Click <i>Generate</i> to generate a strong password automatically. Select <i>View PIN</i> to display the password. This option is only available when you edit an extension.</p> <p>If you have configured the default user PIN (see “Default user PIN” on page 104), the password appears here. However, you can change it.</p>
Authentication type	Select the extension’s authentication type: <i>Local</i> or <i>LDAP</i> .
LDAP profile	<p>If you select <i>LDAP</i> for <i>Authentication type</i>, select an LDAP profile to apply to this extension. For information on LDAP profile, see “Configuring LDAP profiles” on page 125. You can click <i>New</i> to create a new profile or <i>Edit</i> to modify the selected one.</p>
Authentication ID	<p>If you select <i>Try common name with base DN as bind DN</i> as the user authentication option in the authentication profile you select, enter the authentication ID based on the user objects’ common name attribute you entered in the <i>Common name ID</i> field of the profile, such as <i>jdoe</i>.</p> <p>If you select <i>Search user and try bind DN</i> as the user authentication option in the authentication profile you select, leave this field blank.</p> <p>This option is only available if you select <i>LDAP</i> for <i>Authentication type</i>.</p>
Phone language	<p>Select the voice prompts for the extension, such as auto attendant and voicemail. The default is English.</p> <p>For information on adding prompt languages, see “Adding prompt languages” on page 113.</p>
Preference	<p>Select <i>Edit preference</i> to configure the extension user preferences. See “Setting extension user preferences” on page 152.</p> <p>This option is only available when you edit an extension.</p>
Advanced Setting	
Location	Select <i>Internal</i> if the extension does not traverse through Network Address Translation (NAT) to connect to the FortiVoice unit, and <i>External</i> if the extension does.
SIP setting	Select the SIP profile for the extension. Click <i>Edit</i> to modify the current profile or <i>New</i> to configure a new one. For more information, see “Working with FortiVoice profiles” on page 118 .
User privilege	Select the services for the extension. Click <i>Edit</i> to modify the current user privilege or click <i>New</i> to configure a new one. For more information on user privilege, see “Configuring user privileges” on page 213 .

Department	Select the department that the extension belongs to. Click <i>Edit</i> to modify the current department or click <i>New</i> to configure a new one. For more information on extension department, see “” on page 169.
Phone type	<p>Select a supported phone type for the extension.</p> <p>If you cannot find your phone type in the list, select <i>Generic</i>. This phone will not receive the PBX setup information from the FortiVoice unit.</p> <p>When you edit an extension assigned to a phone that does not match what you entered in this field, an orange exclamation mark icon appears. Clicking this icon enters the actual phone type into this field.</p>
MAC address	<p>Enter the MAC address of the SIP phone using the extension number. This option does not apply to FortiFone-850i/860i/870i.</p> <p>When you edit an extension assigned to a FortiFone that does not match what you entered in the <i>Phone type</i> field, an orange exclamation mark icon appears. Clicking this icon enters the FortiFone into the <i>Phone type</i> field. An orange exclamation mark icon also appears beside the <i>MAC address</i> field. Clicking this icon enters the FortiFone MAC address into the <i>MAC address</i> field.</p>
Handset ID	If your <i>Phone type</i> is FortiFone-850i/860i/870i, you can enter the handset ID range (1-8) because these models support multiple handset and each handset is assigned an extension number.
Base MAC address	<p>If your <i>Phone type</i> is FortiFone-850i/860i/870i, enter the MAC address of the base supporting the handsets.</p> <p>When you edit an extension assigned to a FortiFone that does not match what you entered in the <i>Phone type</i> field, an orange exclamation mark icon appears. Clicking this icon enters the FortiFone into the <i>Phone type</i> field. An orange exclamation mark icon also appears beside the <i>Base MAC address</i> field. Clicking this icon enters the base MAC address into the field.</p>

Phone profile	<p>Select a profile type if your phone type is FortiFone 260i and above:</p> <ul style="list-style-type: none"> • <i>Admin defined</i>: This type allows you to choose a system level phone profile. You can also create a new profile or modify the selected one. • <i>User defined</i>: This type allows phone users to set the programmable phone keys on the user web portal when the profile is applied to their extensions. There is no need to choose a profile. <p>Select an <i>Admin defined</i> profile if your phone type is other than FortiFone 260i and above. You can also create a new profile or modify the selected one.</p> <p>For details on phone profiles, see “Configuring phone profiles” on page 122.</p> <p>The phone profile settings you select here synchronize with the same settings in extension preferences. For details, see “Phone profile” on page 157.</p>
Configure User Defined Profile	<p>This option is only available if you select the <i>User defined</i> profile type, save the extension configuration and re-open the extension.</p> <p>Click to configure the user defined phone profile. For details, see “Configuring phone profiles” on page 122.</p>
Voice Mailbox	<p>Configure the extension’s voice mailbox.</p> <p>In some cases, you may want other users or groups to share this voice mailbox. For example, a supervisor wants his/her co-workers to access his/her voice mailbox while he/she is away.</p>
Main voice mailbox	<p>Select the extension’s own voice mailbox (<i>Default</i>) or that of another extension as the voice mailbox of this extension.</p> <p>Typically, you use the default mailbox.</p> <p>If you select the voice mailbox of another extension, you can click <i>Edit</i> to modify that extension.</p>
Notify message waiting light to	<p>You can let the FortiVoice unit turn on the message waiting light on the phones of a user or user group if you want to notify the user or group of a new voice message stored in the voice mailbox associated with this extension.</p> <p>To notify a user or user group, click <i>User(s)/Group(s)</i> and select the users/groups from the <i>Available</i> field and click -> to move them to the <i>Selected</i> field.</p> <p>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 241) and enter the user’s own voicemail PIN.</p> <p>For information on creating user groups, see “Creating extension groups” on page 159.</p>
Extra Information	<p>This option is only available when you edit an extension.</p>

IP

The link to the IP address of the phone using the extension number. This address is retrieved from a SIP phone after it is registered with the FortiVoice unit. Clicking the link opens the login page of the web interface of the phone. You need the user name and password of the phone to log in.

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

Auditing SIP extension password

You can verify the strength of SIP extension passwords. For information on setting SIP extension password, see [“Configuring IP extensions” on page 133](#).

To audit a SIP extension password

1. Go to *Extensions > Extensions > IP Extensions*.
2. Under *Other actions*, click *Check the password strength of SIP accounts*.
The *Audit SIP Passwords* page opens.
3. If a password policy warning appears, click the warning to view the password policy. To set the policy, see [“Configuring system options” on page 78](#).
4. If the *Password Strength* of an extension shows the *Weak* or *Very weak* icon, you can click the password and change it based on the policy until the *Password Strength* shows the *Strong* icon.
5. Click *Save*.

To modify the configuration of an extension

1. Go to *Extensions > Extensions > IP Extensions*.
2. Under *Other actions*, click *Check the password strength of SIP accounts*.
The *Audit SIP Passwords* page opens.
3. Select the extension that you want to modify.
4. Click *Edit* and follow the steps in [“To create or edit an IP extension” on page 135](#).

Fixing duplicate or missing numbers

When there are duplicate, missing, or conflicting extensions, an orange exclamation mark icon appears beside *Show suggested numbers*. You can click the icon and fix the numbers.

Duplicate numbers occur when there are more than one extension with the same number.

Missing numbers happen when you create an extension without assigning it a number. This rarely happens and can only be done through the CLI.

Conflicting numbers happen when the number assigned to an extension conflict with the same number used for other purposes, such as call parking, conference, or ring groups.

For information on the *Show suggested numbers* field, see [“Show suggested numbers” on page 168](#).

To fix duplicate, missing, or conflicting numbers

1. On any page that has *Show suggested numbers*, click the orange exclamation mark icon beside it.

The *Fix Numbers Issues in FortiVoice System* page displays.

Figure 41: Fixing numbers

Fix Number Issues in FortiVoice System		
Duplicate Number Missing Number Conflict Number		
Page 1 / 1 Records per page: 25 Total: 1		
Number	Duplicates	Duplicate Objects
999	2	999 555

2. To fix a duplicate number:
 - Click the *Duplicate Number* sub-menu.
 - Click the duplicate number's user ID (duplicate object) you want to remove. The duplicate number's configuration page displays.
 - Remove the duplicate number in the *Number* field and click *OK*. For information on configuring extensions, see ["Setting up local extensions" on page 133](#).
3. To fix a missing number:
 - Click the *Missing Number* submenu.
 - Double-click a missing number. The missing number's configuration page displays.
 - Enter an extension number in the *Number* field and click *OK*. For information on configuring extensions, see ["Setting up local extensions" on page 133](#).
4. To fix a conflicting number:
 - Click the *Conflict Number* submenu.
 - Double-click a conflicting number. The conflicting number's configuration page displays.
 - Enter an extension number in the *Number* field and click *OK*. For information on configuring extensions, see ["Setting up local extensions" on page 133](#).
5. Close the *Fix Numbers Issues in FortiVoice System* page.

Importing a list of extensions

The import feature provides a simple way to add a list of new extensions in one operation. You can create a CSV file in any spreadsheet and import the data as long as the columns match the FortiVoice format.



Your CSV file must have a headline containing the column names such as *User ID*, *Extension*, *Display name*, *Phone type*, *Mac address*, and *Phone profile*. Otherwise, the import will fail.

To import extension records

1. On the *IP Extensions* tab, click *Import*.

The *Import SIP extension from CSV file* page opens.
2. Select *Update existing extensions* if you want to overwrite the existing extensions with the matching imported records.

If you do not select this option, the uploaded extensions will be skipped if they already exist on the FortiVoice unit.
3. Select *The import CSV file contains 'User ID' field* if you want to import extension records with the *User ID* column.
4. Click *Browse* to locate the CSV file to import and click *Open*.
5. Optionally, click *Download sample* to see if the columns of your CSV file match those of the FortiVoice format.

6. Click *OK*.

A field appears showing the percentage of import completion.

A dialog appears showing the number of imported records.

Modifying analog extension (200D-T model only)

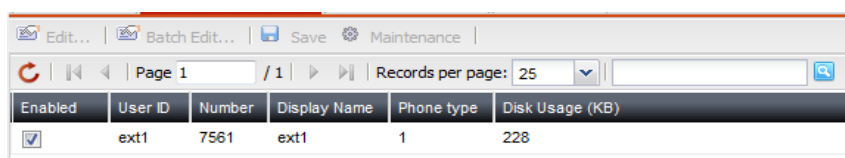
The FortiVoice 200D-T has one analog port and a default analog extension. You can edit the extension's default configuration.

Analog lines, also referred to as POTS (Plain Old Telephone Service), are used for standard phones, fax machines, and modems.

This option is only available on the FortiVoice 200D-T model.

To view the default analog extension, go to *Extensions > Extensions > Analog Extensions*.

Figure 42: Viewing analog extension



Enabled	User ID	Number	Display Name	Phone type	Disk Usage (KB)
<input checked="" type="checkbox"/>	ext1	7561	ext1	1	228

GUI field	Description
Batch Edit	If you want to apply the same changes to multiple extensions, select the extensions and click this option. Make the changes and click <i>Apply To All</i> .
Maintenance	Select an extension and click this button to manage its voicemail box. You can check the size of the box and empty the box. Click <i>Back</i> to return to the <i>Analog</i> tab.
Enabled	Select to activate the extension.
User ID	This is the system-generated ID for the analog extension.
Number	The analog extension number.
Display Name	The name displaying on the extension.
Phone Type	The type of phone for this extension.
Disk Usage (KB)	Displays the size of disk space used by voicemails for the user in kilobytes (KB).

To edit the default analog extension

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

Figure 43: Analog extension configuration

Extension Setting

User ID:

ext1

Number:

7561

Show suggested numbers

Enabled:


☒

Display name:

ext1


External caller ID:

e.g, Jim <612223>

 Password policy is disabled

User PIN:

.....



Generate

View PIN

Authentication type:

Local

Language:

--Default--

Preference:

[Edit preference...]

Advanced Setting

User privilege:

--None--

New...

Edit...

Department:

--None--

New...

Edit...

Analog port:

fxs1

Edit...

Enable fax:

☐

OK

Cancel

GUI field	Description
Extension Setting	
User ID	This is the system-generated ID for the extension and is read-only.
Number	Enter the extension number following the extension number pattern. See “Configuring PBX options” on page 102 .
Show suggested numbers	<p>Select and click in the <i>Number</i> field to display the extension numbers available for use. If it is deselected, clicking in the <i>Number</i> field displays the extension numbers already in use.</p> <p>This option also serves as a diagnostic tool for finding and fixing duplicate or missing numbers. Missing numbers are the extensions that have user IDs but not numbers.</p> <p>When there are duplicate or missing numbers, an orange exclamation mark icon appears beside this option. You can click the icon and fix the numbers. For more information, see “Fixing duplicate or missing numbers” on page 140.</p>
Enabled	Select to activate the extension.
Display name	Enter the name displaying on the extension. This is usually the name of the extension user.

External caller ID	<p>If you want to display a particular caller ID on a called phone instead of the FortiVoice main number (see “Main number” on page 102) or the trunk phone number (see “Phone Number” on page 175), enter it here. The format must be name<phone number>, such as HR<2221111234>.</p> <p>If this extension is mapped to a DID number and the <i>Outbound</i> option is also selected in DID mapping configuration, the external caller ID entry has priority. For information on DID mapping, see “Mapping DIDs” on page 194.</p>
User PIN	<p>Password policy warning icon may appear beside this field depending on your password/PIN policy configuration. You can click the warning icon to configure the policy. For details, see “Configuring system options” on page 78.</p> <p>Enter the password for the user to access voicemail (by dialing *98 or the customized code. See “Modifying feature access codes” on page 241) and the user web portal.</p> <p>Click <i>Generate</i> to generate a strong password automatically. Select <i>View PIN</i> to display the password.</p> <p>If you have configured the default user PIN (see “Default user PIN” on page 104), the password appears here. However, you can change it.</p>
Authentication type	Select the extension’s authentication type: <i>Local</i> or <i>LDAP</i> .
LDAP profile	<p>If you select <i>LDAP</i> for <i>Authentication type</i>, select an LDAP profile to apply to this extension. For information on LDAP profile, see “Configuring LDAP profiles” on page 125. You can click <i>New</i> to create a new profile or <i>Edit</i> to modify the selected one.</p>
Authentication ID	<p>If you select <i>Try common name with base DN as bind DN</i> as the user authentication option in the authentication profile you select, enter the authentication ID based on the user objects’ common name attribute you entered in the <i>Common name ID</i> field of the profile, such as <i>jdoe</i>.</p> <p>If you select <i>Search user and try bind DN</i> as the user authentication option in the authentication profile you select, leave this field blank.</p> <p>This option is only available if you select <i>LDAP</i> for <i>Authentication type</i>.</p>
Language	<p>Select the prompt language for the FortiVoice unit. The default is English.</p> <p>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.</p> <p>For information on adding prompt languages, see “Adding prompt languages” on page 113.</p>

Preference	Select <i>Edit preference</i> to configure the extension user preferences. See “ Setting extension user preferences ” on page 152.
Advanced Setting	
User privilege	Select the services for the extension. Click <i>Edit</i> to modify the current user privilege or click <i>New</i> to configure a new one. For more information on user privileges, see “ Configuring user privileges ” on page 213.
Department	Select the department that the extension belongs to. Click <i>Edit</i> to modify the current department or click <i>New</i> to configure a new one. For more information on extension department, see “ Creating extension departments ” on page 160.
Analog port	Enter the analog port number. By default, it is <i>fxs1</i> .
Enable fax	Select to activate facsimile function for the extension.

4. Click *OK*.

Setting up remote extensions

A remote extension reaches an external phone by automatically selecting a line from a trunk and dialing the phone number. For example, a remote extension could reach an employee’s cell phone or home phone, or a phone at a branch office.

A caller can connect to a remote extension through the auto attendant, or can be transferred to a remote extension by a call cascade. A user at a local extension can manually transfer a caller to a remote extension, or can dial a remote extension directly. If the remote extension is busy or unanswered, the system can route the call using the remote extension’s call cascade.

For example, a caller reaches the auto attendant and dials a local extension. The user is not there, so the call is unanswered. The call cascade of the local extension can be configured to transfer unanswered calls to a remote extension. The remote extension can be configured to dial the user’s cellular phone. This way the user is available outside the office.

Remote extensions are designed to operate with local major telephone service providers. The feature may not function correctly with some telephone and mobile operator’s networks, especially for international phone numbers and mobile phones roaming internationally.

To configure a remote extension

1. Go to *Extensions > Extensions > Remote Extensions*.
2. Click *New*.
3. Configure the following:

Figure 44: Adding a remote extension

Extension Setting

Number:

☐ Show suggested numbers

Remote number:

Enabled:

☒

Display name:

External caller ID:

e.g, Jim <612223>

User PIN:

123123

Generate

Authentication type:

Local

Voice Mailbox

Main voice mailbox:

--Default--

Edit...

Notify message waiting light to:

User(s)

Group(s)

Available : (281/281)

Selected : (0/281)

5230 (FortiVoiceTrunk5230) (sip)

535 (yong test) (mailbox)

7000 (Reception) (sip)

7002 (Ottawa Helpdesk) (mailbox)

7003 (Zhiqiang Test3) (sip)

7004 (7004) (sip)

7005 (Yong Test 7005) (sip)

7006 (Yong Test 7006) (sip)

7007 (Zhiqiang Huang) (sip)

7009 (joetest) (fax)

7010 (Robert Diao Vancouver) (sip)

->

<-

Create

Cancel

GUI field	Description
Extension Setting	
Number	Enter the local extension number from which calls are transferred to a remote extension.
Show suggested numbers	<p>Select and click in the <i>Number</i> field to display the extension numbers available for use. If it is deselected, clicking in the <i>Number</i> field displays the extension numbers already in use.</p> <p>This option also serves as a diagnostic tool for finding and fixing duplicate or missing numbers. Missing numbers are the extensions that have user IDs but not numbers.</p> <p>When there are duplicate or missing numbers, an orange exclamation mark icon appears beside this option. You can click the icon and fix the numbers. For more information, see “Fixing duplicate or missing numbers” on page 140.</p>

Remote number	<p>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 *.</p> <p>If you want to enter an auto attendant number followed by an extension, you can use comma (,) or semicolon (;) to pause the automatic dialing.</p> <p>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.</p> <p>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.</p>
Enabled	Select to activate the remote extension.
Display name	<p>The name displaying on the remote extension when a call is transferred.</p> <p>You can choose to display the name differently than the one you entered here. See “Modifying caller IDs” on page 120.</p>
External caller ID	<p>If you want to display a particular caller ID on a called phone instead of the FortiVoice main number (see “Main number” on page 102) or the trunk phone number (see “Phone Number” on page 175, enter it here. The format must be name<phone number>, such as HR<2221111234>.</p> <p>If this extension is mapped to a DID number and the <i>Outbound</i> option is also selected in DID mapping configuration, the external caller ID entry has priority. For information on DID mapping, see “Mapping DIDs” on page 194.</p>
User PIN	<p>Password policy warnings may appear above this field depending on your password/PIN policy configuration. You can click the warning notice to configure the policy. For details, see “Configuring system options” on page 78.</p> <p>Enter the password for the user to access voicemail (by dialing *98 or the customized code. See “Modifying feature access codes” on page 241) and the user web portal.</p> <p>Click <i>Generate</i> to generate a strong password automatically. Select <i>View PIN</i> to display the password. This option is only available when you edit an extension.</p> <p>If you have configured the default user PIN (see “Default user PIN” on page 104), the password appears here. However, you can change it.</p>
Authentication type	Select the extension’s authentication type: <i>Local</i> or <i>LDAP</i> .
LDAP profile	<p>If you select <i>LDAP</i> for <i>Authentication type</i>, select an LDAP profile to apply to this extension. For information on LDAP profile, see “Configuring LDAP profiles” on page 125.</p> <p>You can click <i>New</i> to create a new profile or <i>Edit</i> to modify the selected one.</p>

Authentication ID	<p>If you select <i>Try common name with base DN as bind DN</i> as the user authentication option in the authentication profile you select, enter the authentication ID based on the user objects' common name attribute you entered in the <i>Common name ID</i> field of the profile, such as <code>jdoe</code>.</p> <p>If you select <i>Search user and try bind DN</i> as the user authentication option in the authentication profile you select, leave this field blank.</p> <p>This option is only available if you select <i>LDAP</i> for <i>Authentication type</i>.</p>
Voice Mailbox	<p>Configure the extension's voice mailbox.</p> <p>In some cases, you may want other users or groups to share this voice mailbox. For example, a supervisor wants his/her co-workers to access his/her voice mailbox while he/she is away.</p>
Main voice mailbox	<p>Select the extension's own voice mailbox (<i>Default</i>) or that of another extension as the voice mailbox of this extension.</p> <p>Typically, you use the default mailbox.</p> <p>If you select the voice mailbox of another extension, you can click <i>Edit</i> to modify that extension.</p>
Notify message waiting light to	<p>You can let the FortiVoice unit turn on the message waiting light on the phones of a user or user group if you want to notify the user or group of a new voice message stored in the voice mailbox associated with this extension.</p> <p>To notify a user or user group, click <i>User(s)/Group(s)</i> and select the users/groups from the <i>Available</i> field and click <i>-></i> to move them to the <i>Selected</i> field.</p> <p>To listen to the message after being notified, the user can dial <i>*97</i> or the code you set (see “Modifying feature access codes” on page 241) and enter the user's own voicemail PIN.</p> <p>For information on creating user groups, see “Creating extension groups” on page 159.</p>

4. Click *Create*.

Configuring fax extensions

If you want to continue using your fax machine with the VoIP phone system, connect the fax machine to an adapter (such as OBIHAI OBi 200, Cisco SPA 112, or Grandstream HT 702) that supports T38 first before connecting it to the FortiVoice unit. T38 is a protocol designed to allow fax to travel over a VoIP network.

In this case, the fax machine is treated like an extension. The FortiVoice unit receives faxes and relays them to the fax machine. Faxes sent from the fax machine will follow the fax sending dial plans.

To use this option, you need to create and enable the fax extensions first. You then need to configure the FortiVoice unit to receive and relay the faxes to the fax machine.

For information on fax configuration, see [“Configuring fax” on page 230](#).

To view the list of fax extensions, go to *Extensions > Extensions > Fax Extensions*.

Figure 45: Fax extensions

Enabled	Number	Display Name
<input checked="" type="checkbox"/>	7009	joetest

GUI field	Description
Enabled	Select to activate this fax extension.
Number	The fax extension number.
Display Name	The name displaying on the fax extension.

To create or edit a fax extension

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

Figure 46: Fax extension configuration

Extension Setting

User ID:

Number: ☐ Show suggested numbers

Enabled: ☒

Display name:

External caller ID: e.g, Jim <612223>

Password policy is disabled

SIP password: ☒ Generate ☐ View password

User PIN: ☒ Generate ☐ View PIN

Authentication type:

Phone language:

Preference: [\[Edit preference... \]](#)

Advanced Setting

Location:

SIP setting:

User privilege:

Department:

MAC address:

Extra Information

IP: -

GUI field	Description
Extension Setting	

User ID	<p>This is the system-generated ID based on the user ID prefix you set (see “User ID prefix” on page 105) and the extension number.</p> <p>This option is view only and only appears when you edit an extension. You can add a new user ID through the CLI. For more information, see the FortiVoice CLI Reference.</p>
Number	<p>Enter the extension number following the extension number pattern. See “Configuring PBX options” on page 102.</p>
Show suggested numbers	<p>Select and click in the <i>Number</i> field to display the extension numbers available for use. If it is deselected, clicking in the <i>Number</i> field displays the extension numbers already in use.</p> <p>This option also serves as a diagnostic tool for finding and fixing duplicate or missing numbers. Missing numbers are the extensions that have user IDs but not numbers.</p> <p>When there are duplicate or missing numbers, an orange exclamation mark icon appears beside this option. You can click the icon and fix the numbers. For more information, see “Fixing duplicate or missing numbers” on page 140.</p>
Enabled	<p>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 230.</p>
Display name	<p>Enter the name displaying on the extension.</p>
External caller ID	<p>If you want to display a particular caller ID on a called phone instead of the FortiVoice main number (see “Main number” on page 102) or the trunk phone number (see “Phone Number” on page 175), enter it here. The format must be name<phone number>, such as HR<2221111234>.</p> <p>If this extension is mapped to a DID number and the <i>Outbound</i> option is also selected in DID mapping configuration, the external caller ID entry has priority. For information on DID mapping, see “Mapping DIDs” on page 194.</p>
SIP password	<p>Password policy warnings may appear above this field depending on your password/PIN policy configuration. You can click the warning notice to configure the policy. For details, see “Configuring system options” on page 78.</p> <p>Enter the password used for configuring your SIP phone from the phone or the Web. You need the phone's IP to access it from the Web.</p> <p>Click <i>Generate</i> to generate a strong password automatically. Select <i>View password</i> to display the password. This option is only available when you edit an extension.</p> <p>If you have configured the default SIP user password (see “Default SIP user password” on page 104), the password appears here. However, you can change it.</p>

User PIN	<p>Enter the password for the extension user to access voicemail and the user web portal.</p> <p>Click <i>Generate</i> to generate a strong password automatically. Select <i>View PIN</i> to display the password. This option is only available when you edit an extension.</p> <p>If you have configured the default user PIN (see “Default user PIN” on page 104), the password appears here. However, you can change it.</p>
Authentication type	Select the extension’s authentication type: <i>Local</i> or <i>LDAP</i> .
LDAP profile	<p>If you select <i>LDAP</i> for <i>Authentication type</i>, select an LDAP profile to apply to this extension. For information on LDAP profile, see “Configuring LDAP profiles” on page 125. You can click <i>New</i> to create a new profile or <i>Edit</i> to modify the selected one.</p>
Authentication ID	<p>If you select <i>Try common name with base DN as bind DN</i> as the user authentication option in the authentication profile you select, enter the authentication ID based on the user objects’ common name attribute you entered in the <i>Common name ID</i> field of the profile, such as <i>jdoe</i>.</p> <p>If you select <i>Search user and try bind DN</i> as the user authentication option in the authentication profile you select, leave this field blank.</p> <p>This option is only available if you select <i>LDAP</i> for <i>Authentication type</i>.</p>
Phone language	<p>Select the voice prompts for the extension, such as auto attendant and voicemail. The default is English.</p> <p>For information on adding prompt languages, see “Adding prompt languages” on page 113.</p>
Preference	<p>Select <i>Edit preference</i> to configure the extension user preferences. See “Setting extension user preferences” on page 152.</p> <p>This option is only available when you edit an extension.</p>
Advanced Setting	
Location	Select <i>Internal</i> if the extension does not traverse through Network Address Translation (NAT) to connect to the FortiVoice unit, and <i>External</i> if the extension does.
SIP setting	Select the SIP profile for the extension. Click <i>Edit</i> to modify the current profile or <i>New</i> to configure a new one. For more information, see “Working with FortiVoice profiles” on page 118 .
User privilege	Select the services for the extension. Click <i>Edit</i> to modify the current user privilege or click <i>New</i> to configure a new one. For more information on user privilege, see “Configuring user privileges” on page 213 .

Department	Select the department that the extension belongs to. Click <i>Edit</i> to modify the current department or click <i>New</i> to configure a new one. For more information on extension department, see “” on page 169.
MAC address	Enter the MAC address of the adapter through which the fax machine connects to the FortiVoice unit.
Extra Information	This option is only available when you edit an extension.
IP	The link to the IP address of the fax adapter using the extension number. This address is retrieved from the adapter after it is registered with the FortiVoice unit. Clicking the link opens the login page of the web interface of the adapter. You need the user name and password of the adapter to log in.

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

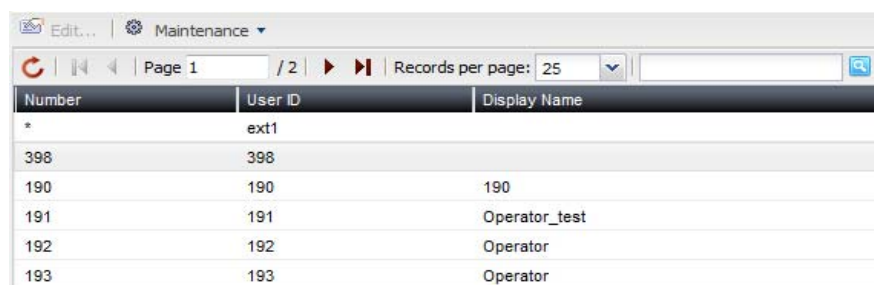
Setting extension user preferences

Each SIP and analog extension comes with its default user preferences, including voicemail settings and phone display preference. You can modify these settings.

Phone users can modify the preferences on the web user portal.

To view the list of extensions, go to *Extensions > Extensions > Preferences*.

Figure 47: Extension preferences



Number	User ID	Display Name
*	ext1	
398	398	
190	190	190
191	191	Operator_test
192	192	Operator
193	193	Operator

GUI field	Description
Maintenance	Select an extension and click this option to reset the user preferences to the default values.
Number	The extension number.
User ID	The system-generated ID based on the extension number.
Display Name	The name displaying on the extension. This is usually the name of the extension user.

To edit extension user preferences

1. Go to *Extensions > Extensions > Preferences*.
2. Select an extension and click *Edit*.
3. Configure the following:

Figure 48: Modifying extension user preferences

Extension User Preference

Voicemail Setting

User ID:

7314

Number:

7314

Display name:

Emergency caller ID:

External caller ID:

e.g. Jim <612223>

Ring duration:

18

(Seconds)

☐ Call forward

Forward to:

☒ Call waiting

☐ Do not disturb

☒ Message waiting indication

☐ voicemail handling (Caller press 0 during announcement)

Notification Options

Voicemail:

☐ None ☐ Simple ☒ With attachment

Fax:

☐ None ☐ Simple ☒ With attachment

Missed call:

☐ Off ☒ On

Email address:

Display Preference

Default portal:

☒ User portal ☐ Operator console ☐ Agent console

Prompt language:

--Default--

Web GUI language:

English

Theme:

Red Grey

Time zone:

(GMT-5:00)Eastern Time(US & Canada)

Account Management

PIN: [\[Change PIN number...\]](#)

Agent

☒ PIN required to login/logout from phone

☐ PIN required to pause/unpause from phone

☐ Pause after agent login queue

Speed Dial Setting

Follow Me

New... | Edit... | Delete |

Settings

Black List

New... | Delete |

Phone Number

Call Handling

[\[Configure call handling\]](#)

Phone Profile

Phone profile:

☒ Admin defined

Default-FortiFone-350i/360i

New... Edit...

☐ User defined

FortiFone Call Preference

☐ Direct call

Direct call number:

Direct call timer:

0

Seconds (0: hotline)

☐ Auto answer

OK

Cancel

<i>GUI field</i>	<i>Description</i>
Voicemail Setting	
User ID	This is the system-generated ID based on the extension number. This is not editable. You can add a new user ID through the CLI. For more information, see the FortiVoice CLI Reference .
Number	The extension number. This is not editable.
Display name	Enter the name displaying on the extension. This is usually the name of the extension user.
Emergency caller ID	<p>Enter the caller ID to display on the destination phone when you dial the emergency number, such as 911.</p> <p>If you also enter an external caller ID (see “External caller ID” on page 154), that ID will not override the 911 caller ID when dialing the 911 emergency number.</p>
External caller ID	<p>The caller ID you want to display on a called phone instead of the FortiVoice main number (see “Main number” on page 102) or the trunk phone number (see “Phone Number” on page 175). This is not editable.</p> <p>For details, see “External caller ID” on page 136 and “External caller ID” on page 144.</p>
Ring duration	Enter the phone ringing duration in seconds before an incoming call goes to voicemail.
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 213 .
Call waiting	Select to enable call waiting. This function only works if call waiting is enabled in the extension’s user privilege. See “Configuring user privileges” on page 213 .
Do not disturb	Select to enable DND. This function only works if DND is enabled in the extension’s user privilege. See “Configuring user privileges” on page 213 .
Message waiting indication	Select to enable phone indication that a message is received.
Voicemail handling (Caller press 0 during announcement)	Select to enable reaching the operator by pressing 0 when you hear the announcement of a callee’s voicemail.
Notification Options	

Voicemail	<p>Select the type of email notification when this extension has a voicemail:</p> <ul style="list-style-type: none"> • <i>None</i>: Do not send any notification. • <i>Simple</i>: Send an email notification. • <i>Attachment</i>: Send an email notification with the voicemail attached.
Fax	<p>Select the type of email notification when this extension has a fax:</p> <ul style="list-style-type: none"> • <i>None</i>: Do not send any notification. • <i>Simple</i>: Send an email notification. • <i>Attachment</i>: Send an email notification with the fax attached.
Missed call	Select <i>On</i> if you want to send an email notification when an incoming call is missed.
Email address	Enter the email address(es) to which the email notifications for voicemails, faxes, or missed calls are sent.
Display Preference	
Default portal	<p>Select the default user web portal interface.</p> <p>If <i>Operator console</i> or <i>Agent console</i> is disabled, it means that the operator mode function in the user privilege for this extension is not enabled. For more information, see “Configuring user privileges” on page 213.</p> <p>If <i>Agent console</i> is disabled, it means that the extension agent for this extension is not enabled. For more information, see “Agent” on page 127.</p>
Prompt language	<p>Select the prompt language for the extension. The default is English.</p> <p>For information on adding prompt languages, see “Adding prompt languages” on page 113.</p>
Web GUI language	Select the language for the FortiVoice user web portal.
Theme	Select the display theme for the FortiVoice user web portal.
Time zone	Select the time zone for the FortiVoice user web portal.
Account Management	Click <i>Change PIN number</i> to change the password for accessing the voice mailbox and the FortiVoice user web portal.
Agent	
PIN required to login/logout from phone	<p>Select to enable an agent to log into/log out of a queue from the extension using the user PIN.</p> <p>For information on feature access codes, see “Configuring account codes” on page 218.</p>

PIN required to pause/unpause from phone	<p>Select to enable an agent to pause/unpause a queue from the extension using the user PIN. To pause means the agent is not answering calls.</p> <p>For information on feature access codes, see “Configuring account codes” on page 218.</p>
Auto-pause after agent login queue	<p>Select to automatically put the agent in pause (not ready) status after the agent logs into a queue. The agent can unpause a queue to answer calls.</p> <p>For information on feature access codes, see “Configuring account codes” on page 218.</p>
Speed Dial Setting	<p>Map a phone key to a phone number for speed dialing by clicking <i>Number</i> and enter the phone number.</p> <p>You can enter digits 0–9, space, dash, comma, # and *.</p> <p>If you want to enter an auto attendant number followed by an extension, you can use comma (,) or semicolon (;) to pause the automatic dialing.</p> <p>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.</p> <p>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.</p>
Follow Me	<p>See “Configuring follow me settings” on page 157.</p>
Black list	<p>Click <i>New</i> to enter the phone number you want to block from calling this extension.</p> <p>This configuration serves as a profile for use in managing calls. See “Handling calls” on page 158.</p>
Call Handling	<p>For more information, see “Handling calls” on page 158.</p>

Phone profile	<p>For details on phone profiles, see “Configuring phone profiles” on page 122.</p> <p>Select a profile type if your phone type is FortiFone 260i and above:</p> <ul style="list-style-type: none"> • <i>Admin defined</i>: This type allows you to choose a system level phone profile. You can also create a new profile or modify the selected one. • <i>User defined</i>: This type allows phone users to set the programmable phone keys on the user web portal when the profile is applied to their extensions. There is no need to choose a profile. <p>Select an <i>Admin defined</i> profile if your phone type is other than FortiFone 260i and above. You can also create a new profile or modify the selected one.</p> <p>The phone profile settings you select here synchronize with the same settings in extension configuration. For details, see “Phone profile” on page 139.</p>
Configure User Defined Profile	<p>This option is only available if you select the <i>User defined</i> profile type, save the extension configuration and re-open the extension.</p> <p>Click to configure the user defined phone profile. For details, see “Configuring phone profiles” on page 122.</p>
FortiFone Call Preference	<p>If this extension is for a FortiFone, you can configure its call preferences.</p>
Direct call	<p>Select to add direct call function to this phone, that is, as soon as you pick up the phone, it dials the number you set automatically.</p>
Direct call number	<p>If you select <i>Direct call</i>, enter the number to call. For example, the number of your paging system.</p>
Direct call timer	<p>Enter the time in seconds to wait before the number dialing starts after the phone is picked up.</p> <p>You can enter a different number to call before the set time expires.</p>
Auto answer	<p>Select to enable this phone to automatically answer phone calls without being picked up.</p>

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 158](#).

To configure follow me settings:

1. Go to *Extensions > Extensions > Preferences > Follow Me*.

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

Repeat steps 4 to 7 of this procedure to add more numbers if you want to transfer a follow me call to multiple numbers in a sequence. The numbers will be dialed according to the sequence in the follow me setting.

Handling calls

Extensions > Extensions > Preferences > 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.

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 call

1. Go to *Extensions > Extensions > Preferences > Call Handling*.
2. Click *Configure call handling*.

Figure 49: Call management configuration

3. Select a call status at the top of the page.
Each status can only be used for one call management configuration.
If you select *Black List*, the call management configuration will apply to the numbers added in the *Black List* configuration. See [“Black list” on page 156](#).
4. For *Call Process*, select *System default action* or *User defined* action.
The *System default action* changes depending on the status selection.

5. If you select *User defined*, click *New* to define a call process according to a schedule.
 - Select a pre-configured *Schedule* for the call action. You can click *View* to display the schedule details. For information on configuring schedules, see [“Scheduling the FortiVoice unit” on page 121](#).
 - Add an *Action* for the call process. You can add multiple actions to process a call in sequence. For example, you can add *Play announcement* and then *Auto attendant*. In this case, an incoming call will be transferred to the auto attendant after an announcement is played.

Default action is equal to the action when you select *System default action* under *Call Process*.

 - If you select *Follow me*, select a follow me profile. For information on configuring follow me, see [“Follow Me” on page 156](#).

This option is available only if call forwarding is enabled in the extension’s user privilege. See [“Configuring user privileges” on page 213](#).
 - If you select *Play announcement*, select a sound file. For information on configuring sound files, see [“Managing sound files and music on hold” on page 116](#).
 - If you select *Auto attendant*, select an auto attendant profile. For information on configuring auto attendant, see [“Configuring auto attendants” on page 206](#).
 - 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 213](#).
 - Click *Create*.
6. Click *OK*.

Resetting voice messages

Extensions > Extensions > Voice Messages lets you view the voice message count in each extension. You can also delete the voice messages for an extension by selecting the extension and click *Maintenance > Reset*. This action only deletes the messages, not the extension itself.

Creating extension groups

Extensions > Groups lets you configure extension groups including extension departments, ring groups, page groups, and pickup groups.

This section contains the following topics:

- [Creating user groups](#)
- [Creating extension departments](#)
- [Creating ring groups](#)
- [Creating page groups](#)
- [Creating pickup groups](#)

Creating user groups

You can create a user group and use it to simplify the configuration of an IP extension voice mailbox, a general voice mailbox, a ring group, a page group, or a pickup group. For example, when creating a ring group, you can select the name of a user group rather than entering each user name individually.

For information on creating IP extension voice mailboxes, see [“Configuring IP extensions” on page 133](#).

For information on creating general voice mailboxes, see [“Setting up general voice mailboxes” on page 164](#).

To create a user group

1. Go to *Extension > Groups > User Group*.
2. Click *New*.
3. Enter a name for the group.
4. Select the available users or user groups that you want to include in the group and click -> to move them into the *Selected* field.
5. Click *Create*.

Creating extension departments

You can create department profiles for applying to the extensions. For example, you can create a department profile called HR and apply it to extension 1111 to indicate that this extension belongs to the HR department.

For information on applying department profiles, see [“Setting up local extensions” on page 133](#).

To create an extension department

1. Go to *Extension > Groups > 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. Click *Create*.

Creating ring groups

A ring group is a group of local extensions and external numbers that can be called using one number. Local extensions and auto attendants can dial a ring group.

A ring group can reach a group of extensions. For example, ring group 301 can ring the sales group at extensions 111, 112, 113, and 114. When a customer calls the sales group, the first available salesperson answers for the group.

To create a ring group

1. Go to *Extension > Groups > Ring Group*.
2. Click *New*.
3. Configure the following:

Figure 50: Creating a ring group

Ring Group

Name:

Number:

Show suggested numbers

Display name:

Enabled:

☒

Ring mode:

☒ All ☐ Sequential

Members:

Available : (9/9)

290 (870i_290) (sip)

7701 (new user) (sip)

7702 (sip)

7711 (sip)

7816 (test 7816) (sip)

7820 (test 7820) (sip)

7821 (TLS_S RTP 7821) (sip)

7822 (QA Ysun) (sip)

1390 (office_public) (virtual number)

->

<-

Selected : (0/9)

External numbers:

New...

Delete

Number

Call Handling

[Configure call handling]

Advanced setting

Create

Cancel

GUI field	Description
Name	Enter the name for the ring group.
Number	<p>Enter the ring group number following the extension number pattern. See “Configuring PBX options” on page 102.</p> <p>Clicking in the field displays a list of crossed-out extensions. These numbers are already used and cannot be used as ring group numbers.</p> <p>The ring group number, once dialed, will ring all the extensions in the group.</p>
Show suggested numbers	<p>Select and click in the <i>Number</i> field to display the extension numbers available for use. If it is deselected, clicking in the <i>Number</i> field displays the extension numbers already in use.</p> <p>This option also serves as a diagnostic tool for finding and fixing duplicate or missing numbers. Missing numbers are the extensions that have user IDs but not numbers.</p> <p>When there are duplicate or missing numbers, an orange exclamation mark icon appears beside this option. You can click the icon and fix the numbers. For more information, see “Fixing duplicate or missing numbers” on page 140.</p>
Display Name	Enter the name displaying on the extensions of the ring group, such as “HR”.
Enabled	Select to activate the ring group.

Ring mode	<p>Select how you want the ring group to be called.</p> <ul style="list-style-type: none"> • <i>All</i>: All extensions in the group will ring when the ring group number is dialed. • <i>Sequential</i>: 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.
Members	<p>Select the available extensions or user groups that you want to include in the ring group and click -> to move them into the <i>Selected</i> field.</p> <p>For information on creating extensions and user groups, see “Setting up local extensions” on page 133 and “Creating extension groups” on page 159.</p>
External numbers	<p>Click <i>New</i> 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.</p>
Call Handling	<p>Use this option to configure the call handling for the ring group. For more information, see “Configuring ring group call handling” on page 162.</p>
Advanced setting	<ul style="list-style-type: none"> • <i>Ring Pattern</i>: Select a ring pattern for the group. • <i>Ring duration</i>: Set the amount of time in seconds allowing all extensions or each one to ring before going to voicemail. • <i>Caller ID option</i>: Select how you want the caller ID to display. • <i>Emergency call option</i>: Select <i>Display emergency caller ID</i> to show the emergency caller’s ID, or <i>Disconnect ongoing call</i> to stop a call that uses the line for emergency call.

4. Click *Create*.

Configuring ring group 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.

If the ring group with configured call handling action is part of another FortiVoice function that also has configured call handling action (for example, a member of another ring group or the ring group extension is used for a virtual number), then the call handling action of the other FortiVoice function overrides the ring group call handling action.

For information on the *Call Handling* option, see [“Call Handling” on page 162](#).

To configure the call process

1. On the *Ring Group* page, click *Configure call handling* under *Call Handling*.
2. Select a call status at the top of the page.

Each status can only be used for one call management configuration.

For the *Busy* status, if you set the ring group’s ring mode to *All*, the FortiVoice unit will declare the ring group busy only if all extensions in the group are busy; if you set the ring group’s ring mode to *Sequential*, the FortiVoice unit will declare the ring group busy only if the last extension in the group is busy after ringing the extensions sequentially and each one is busy at the time of being rung.

3. For *Call Process*, select *System default action* or *User defined action*.
The *System default action* changes depending on the status selection.
4. If you select *User defined*, click *New* to define a call process according to a schedule.
 - Select a pre-configured *Schedule* for the call action. You can click *View* to display the schedule details. For information on configuring schedules, see [“Scheduling the FortiVoice unit” on page 121](#).
 - Add an *Action* for the call process. You can add multiple actions to process a call in sequence. For example, you can add *Play announcement* and then *Auto attendant*. In this case, an incoming call will be transferred to the auto attendant after an announcement is played.
Default action is equal to the action when you select *System default action* under *Call Process*.
 - If you select *Voicemail*, enter the extension number of the voice mail.
 - If you select *Play announcement*, select a sound file. For information on configuring sound files, see [“Managing sound files and music on hold” on page 116](#).
 - If you select *Auto attendant*, select an auto attendant profile. For information on configuring auto attendant, see [“Configuring auto attendants” on page 206](#).
 - 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 213](#).
 - Click *Create*.

Creating page groups

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

A page group can reach a group of extensions. For example, page group 301 can ring the sales group at extensions 111, 112, 113, and 114. When a call reaches 301, all extensions in the group can pick up and answer the call.

To create a page group

1. Go to *Extensions > Groups > Paging Group*.
2. Click *New*.
3. Enter a name for the group.
4. Enter the page group number following the extension number pattern. See [“Configuring PBX options” on page 102](#).
This is the number that, once paged, will ring all the extensions in the group.
5. For *Show suggested numbers*, select and click in the *Number* field to display the extension numbers available for use. If it is deselected, clicking in the *Number* field displays the extension numbers already in use.
This option also serves as a diagnostic tool for finding and fixing duplicate or missing numbers. Missing numbers are the extensions that have user IDs but not numbers.
When there are duplicate or missing numbers, an orange exclamation mark icon appears beside this option. You can click the icon and fix the numbers. For more information, see [“Fixing duplicate or missing numbers” on page 140](#).
6. Enter the name displaying on the extensions of the group, such as “HR”.

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.
8. Select *Enabled* to activate this group.
9. Select the available extensions or extension groups that you want to include in the page group and click -> to move them into the *Selected* field.
10. 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 241](#).

To create a pickup group

1. Go to *Extensions > Groups > Pickup Group*.
2. Click *New*.
3. Enter a name for the group.
4. Select *Enabled* to activate this group.
5. For *Members*, select the *Available* extensions or user groups that you want to include in the pickup group and click -> to move them into the *Selected* field.

For information on creating extensions and user groups, see [“Setting up local extensions” on page 133](#) and [“Creating extension groups” on page 159](#).
6. For *Pickup by members*, select the *Available* extensions or user groups that are allowed to answer incoming calls that ring on other extensions and click -> to move them into the *Selected* field.
7. Click *Create*.

Setting up general voice mailboxes

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

To view the group voice mailbox, go to *Extensions > General Voicemail > General Voicemail*.

Figure 51: Viewing general voice mails



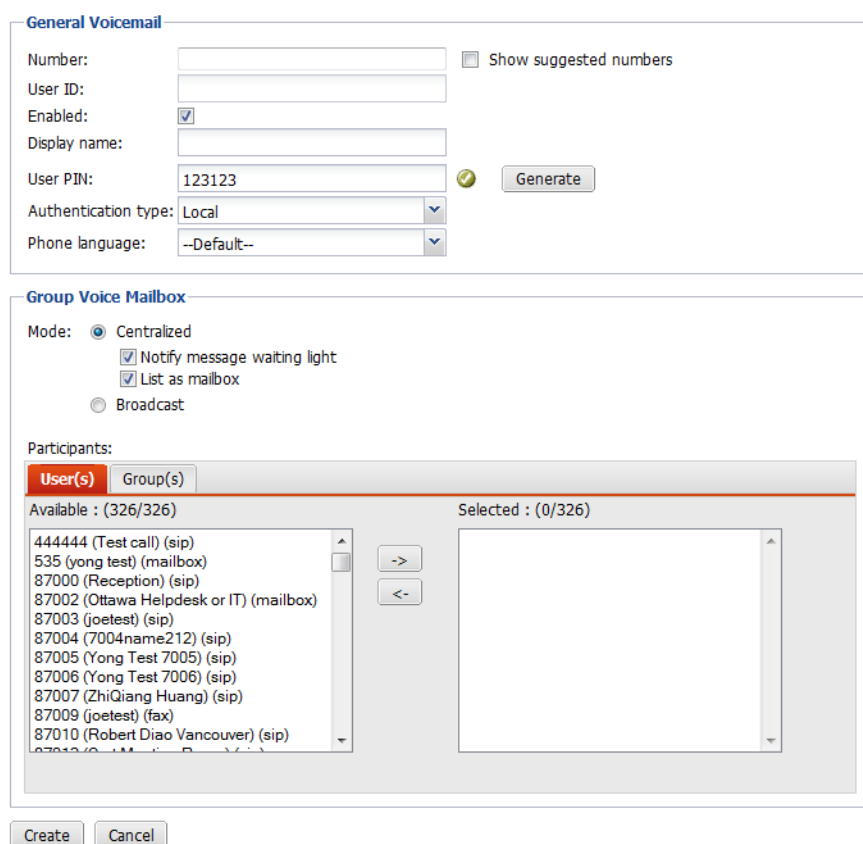
Enabled	Number	Display Name	Disk Usage (KB)
<input checked="" type="checkbox"/>	111		16

GUI field	Description
Enabled	Select to activate the mailbox.
Number	The extension number for the mailbox. This number is for the mailbox only and not associated with any phone.
Display Name	The name displaying on the extension.
Disk Usage (KB)	Displays the size of disk space used by the general voice mails in kilobytes (KB).

To set up a general voice mailbox

1. Go to *Extensions > General Voicemail > General Voicemail*.
2. Click *New* or double-click an existing record.
3. Configure the following:

Figure 52: Adding a general voice mailbox



General Voicemail

Number: ☐ Show suggested numbers

User ID:

Enabled: ☒

Display name:

User PIN:

Authentication type:

Phone language:

Group Voice Mailbox

Mode: ☒ Centralized

☒ Notify message waiting light

☒ List as mailbox

☐ Broadcast

Participants:

Available : (326/326)

Selected : (0/326)

444444 (Test call) (sip)

535 (yong test) (mailbox)

87000 (Reception) (sip)

87002 (Ottawa Helpdesk or IT) (mailbox)

87003 (joetest) (sip)

87004 (7004name212) (sip)

87005 (Yong Test 7005) (sip)

87006 (Yong Test 7006) (sip)

87007 (ZhiQiang Huang) (sip)

87009 (joetest) (fax)

87010 (Robert Diao Vancouver) (sip)

GUI field	Description
-----------	-------------

General Voicemail	
User ID	<p>This is the system-generated ID based on the mailbox extension number.</p> <p>This option is view only. You can add a new user ID through the CLI. For more information, see the FortiVoice CLI Reference.</p>
Number	Enter the mailbox extension number following the extension number pattern. See “ Configuring PBX options ” on page 102.
Show suggested numbers	<p>Select and click in the <i>Number</i> field to display the extension numbers available for use. If it is deselected, clicking in the <i>Number</i> field displays the extension numbers already in use.</p> <p>This option also serves as a diagnostic tool for finding and fixing duplicate or missing numbers. Missing numbers are the extensions that have user IDs but not numbers.</p> <p>When there are duplicate or missing numbers, an orange exclamation mark icon appears beside this option. You can click the icon and fix the numbers. For more information, see “Fixing duplicate or missing numbers” on page 140.</p>
Enabled	Select to activate the mailbox extension.
Display name	Enter the name of the mailbox extension.
User PIN	<p>Password policy warning icon may appear beside this field depending on your password/PIN policy configuration. You can click the warning icon to configure the policy. For details, see “Configuring system options” on page 78.</p> <p>Enter the password for the user to access voicemail (by dialing *98 or the customized code. See “Modifying feature access codes” on page 241) and the user web portal.</p> <p>Click <i>Generate</i> to generate a strong password automatically. Select <i>View PIN</i> to display the password. This option is only available when you edit an extension.</p> <p>If you have configured the default user PIN (see “Default user PIN” on page 104), the password appears here. However, you can change it.</p>
Authentication type	Select the mailbox extension’s authentication type: <i>Local</i> or <i>LDAP</i> .
LDAP profile	<p>If you select <i>LDAP</i> for <i>Authentication type</i>, select an LDAP profile to apply to this extension. For information on LDAP profile, see “Configuring LDAP profiles” on page 125.</p> <p>You can click <i>New</i> to create a new profile or <i>Edit</i> to modify the selected one.</p>

Authentication ID	<p>If you select <i>Try common name with base DN as bind DN</i> as the user authentication option in the authentication profile you select, enter the authentication ID based on the user objects' common name attribute you entered in the <i>Common name ID</i> field of the profile, such as <code>jdoe</code>.</p> <p>If you select <i>Search user and try bind DN</i> as the user authentication option in the authentication profile you select, leave this field blank.</p> <p>This option is only available if you select <i>LDAP</i> for <i>Authentication type</i>.</p>
Phone language	<p>Select the voice prompts for the mailbox extension, such as auto attendant and voicemail. The default is English.</p> <p>For information on adding prompt languages, see “Adding prompt languages” on page 113.</p>
Group Voice Mailbox	Configure the users for sharing this extension's mailbox.
Mode	<p>Select the way to deliver the voicemail from this mailbox extension to the users sharing this mailbox.</p> <ul style="list-style-type: none"> • 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 voice mailbox. • List as mailbox: Users can listen to a centralized voicemail by dialing *97 or the customized code (see “Modifying feature access codes” on page 241) from their own extensions and enter the user PIN for this general voicemail box. • Broadcast: If you select this option, the voicemail is sent to the voicemail boxes of the users. Users can access the voicemail by dialing *98 or the customized code (see “Modifying feature access codes” on page 241) from any extensions and enter the personal user PIN.
Participants	<p>Select the users or groups to notify when a voicemail is left in this mailbox extension.</p> <p>To select the users to share this mailbox, click <i>User(s)</i> and from the <i>Available</i> field, select the users and click -> to move them to the <i>Selected</i> field.</p> <p>To select the groups to share this mailbox, click <i>Group(s)</i> and from the <i>Available</i> field, select the groups and click -> to move them to the <i>Selected</i> field.</p> <p>For information on creating user groups, see “Creating extension groups” on page 159.</p>

4. Click *Create* or *OK*.

Working with virtual numbers

A virtual number is an extension that is not assigned to a phone. Unlike auto attendants, when a call goes to a virtual number, the caller does not need to manually select any options by pressing the phone keys. The call process is automated based on time schedules. For example, for after business hour phone calls, you can configure a virtual number to play an announcement, then transfer the call to the voice mailbox. You can also transfer the calls to the auto attendant where the callers can manually select the options based on the auto attendant configuration.

If the virtual number with configured call handling action is part of another FortiVoice function that also has configured call handling action (for example, a member of a ring group), then the call handling action of the other FortiVoice function overrides the virtual number call handling action.

To configure a virtual number

- 1. Go to *Extensions > Virtual Number > Virtual Number* and click *New*.
- 2. Configure the following:

Figure 53: Configuring virtual numbers

Virtual Number

Name:

Number:

☐ Show suggested numbers

Display name:

Enabled:

☒

Comment:

Call Handling

New...

Edit...

Move

Delete

Schedule

Action

Target

Create

Cancel

GUI field	Description
Name	Enter a name for the virtual number.
Number	Enter the virtual number which is not assigned to any phone.
Show suggested numbers	<p>Select and click in the <i>Number</i> field to display the virtual numbers available for use. If it is deselected, clicking in the <i>Number</i> field displays the virtual numbers already in use.</p> <p>This option also serves as a diagnostic tool for finding and fixing duplicate or missing numbers. Missing numbers are the extensions that have user IDs but not numbers.</p> <p>When there are duplicate or missing numbers, an orange exclamation mark icon appears beside this option. You can click the icon and fix the numbers. For more information, see “Fixing duplicate or missing numbers” on page 140.</p>
Display name	Enter the name displaying on the extension. This is usually the name of the extension user.

Enabled	Select to activate 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 169 .

Configuring virtual number call handling

Use the *Call Handling* option to configure the call automation. For example, you can configure the process to forward a call to another number on a specific schedule.

For information on the *Call Handling* option, see [“Call Handling” on page 169](#).

To configure the call process

1. On the *Virtual Number* page, click *New* under *Call Handling*.

The *Call Handling Setting* page displays.

Figure 54: Call handling setting

2. Select a pre-configured *Schedule* for the call action. You can also click *New* to create a schedule or *Edit* to modify the selected one. For information on configuring schedules, see [“Scheduling the FortiVoice unit” on page 121](#).
3. Select an *Action* for the call handling. You can select multiple actions to process a call in sequence. For example, you can select *Play announcement* and then *Auto attendant*. In this case, an incoming call will be transferred to the auto attendant after an announcement is played.
Some actions require that you enter further information to complete the call process, such as *Dial extension* and *General mailbox*.
4. Click *Create*.
5. Click *OK*.

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 133](#) and [“Configuring Call Routing” on page 189](#).

This topic includes:

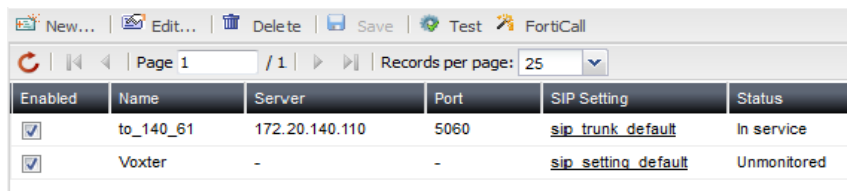
- [Setting up VoIP trunks](#)
- [Modifying PSTN/PRI trunks \(200D-T and 2000E-T2 only\)](#)
- [Configuring office peers](#)

Setting up VoIP trunks

You can add one or more VoIP service providers to the FortiVoice unit trunk configuration. The VoIP service providers deliver your telephone services to customers equipped with SIP-based PBX (IP-PBX).

To view the list of VoIP service providers, go to *Trunks > VoIP > SIP*.

Figure 55: SIP trunks



Enabled	Name	Server	Port	SIP Setting	Status
<input checked="" type="checkbox"/>	to_140_61	172.20.140.110	5060	sip_trunk_default	In service
<input checked="" type="checkbox"/>	Voxter	-	-	sip_setting_default	Unmonitored

GUI field	Description
Test	Select to test if the trunk is created successfully. For more information, see “Testing SIP trunks” on page 175 .
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 176 .
Enabled	Select to activate this trunk.
Name	The name of the VoIP service provider.
Server	The VoIP provider’s domain name or IP address. For example, 172.20.120.11 or voip.example.com.

Port	The port for SIP sessions.
SIP Setting	The SIP profile applied to this trunk.
Status	<p>The status of the SIP trunk.</p> <ul style="list-style-type: none"> • <i>Not registered</i>: The trunk is not registered with the VoIP service provider and is not in service. • <i>In service</i>: The trunk is registered with the VoIP service provider and is in service. • <i>Unavailable</i>: The trunk is not reachable. • <i>Alarm detected</i>: There is a problem with the phone line. • <i>Admin down</i>: The trunk is disabled. • <i>Unmonitored</i>: The trunk is unknown.

To create a VoIP trunk

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

Figure 56: New VoIP trunk

SIP

Name:

Display name:

Main number:

Enabled: ☒

SIP Setting

SIP server:

SIP port:

Using SRV record: ☐

User name:

Password:

Auth. user name:

Realm/domain:

SIP setting:

Max channel: ☐ Overflow check

Caller ID modification: ☐

Inband ringtone: ☐

► Registration

► Outbound Proxy

Phone Number

Phone Number

GUI field	Description
-----------	-------------

SIP	
------------	--

Name	Enter the name of the VoIP service provider.
Display name	Enter your caller ID that will appear on the called phone, such as Example Company.
Main number	Enter the phone number that will appear on the called phone. If you entered the external caller ID in “External caller ID” on page 136 or “External caller ID” on page 154 , this trunk phone number will be overridden by the external caller ID.
Enabled	Select to activate the SIP trunk.
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 <i>Using DNS record</i> option, this field is greyed out.
Using SRV record	If you entered the VoIP provider’s domain name in the <i>SIP server</i> 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.
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 setting	Select the SIP profile to apply the supported phone features and codecs for the trunk. To match the information of the VoIP service provider, you can edit the existing profile or click <i>New</i> to add a new one. For more information, see “Configuring SIP profiles” on page 118 .

Max channel	<p>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 122.</p> <p>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.</p>
Overflow check	<p>If selected, the phone calls exceeding the <i>Max channel</i> limit will be handled according to the call handling actions set in the dialplan applied to this trunk. For information on dialplans, see “Configuring Call Routing” on page 189.</p> <p>If unselected, the phone calls exceeding the <i>Max channel</i> limit will be disconnected.</p>
Caller ID modification	<p>Select if you want the trunk main number to appear on the called phone. See “Main number” on page 172.</p> <p>Otherwise, the user name provided by the VoIP service provider for the FortiVoice unit to register with the SIP server will appear on the called phone. See “User name” on page 172.</p>
Inband ringtone	<p>Select to enable the FortiVoice unit to send ring tone to the caller of an incoming call before the establishment of a call connection.</p> <p>This option is only editable if you enable early media in “Advanced Setting” on page 111.</p>

Registration	<p>Enter the SIP registration information from the VoIP service provider by selecting a registration method. You can receive calls after registering with the SIP server of the VoIP service provider.</p> <ul style="list-style-type: none"> • <i>Enable registration</i>: Select to activate the registration with the VoIP service provider. This trunk is ready to use. • <i>Standard</i>: Select to use the standard registration method which automatically registers with the SIP server of the VoIP service provider. • <i>Registrar</i>: Select to enter the registration information from the VoIP service provider: <ul style="list-style-type: none"> • <i>Registrar host/IP</i>: Enter the VoIP service provider's SIP registration server domain name or IP address. For example, 172.20.120.11 or voip.example.com. • <i>Registrar port</i>: 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. • <i>Transport protocol</i>: Select the transport protocol used for the registration. • <i>Registration URI</i>: Enter the registration string provided by the VoIP service provider in the <i>Registration URI</i> field. The string usually has the following formats: <pre>register => user[:secret[:authuser]]@host[:port][:/extension]</pre> or <pre>register => fromuser@fromdomain:secret@host</pre> or <pre>register => fromuser@fromdomain:secret:authuser@host:port/extension</pre> For example, a string could be: <code>register => 2345:password@mysipprovider.com/1234</code>
Outbound Proxy	<p>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:</p> <ul style="list-style-type: none"> • <i>Enable proxy</i>: Select to activate the proxy server settings. • <i>Proxy host/IP</i>: Enter the proxy server's domain name or IP address. For example, 172.20.120.11 or voip.example.com. • <i>Proxy port</i>: Enter the port number of the proxy server. • <i>Transport protocol</i>: Select the transport protocol used for the registration.
Fax	<p>Configure fax and phone signal automatic detection and fax handling.</p>
Automatic fax detection	<p>Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically.</p>

Forward fax to DID mapping extension	Some extensions have DID mappings. See “Mapping DIDs” on page 194 . When an incoming fax reaches an extension with DID mapping, selecting this option will send the fax to the DID mapping extension. This option is only selectable if <i>Automatic fax detection</i> is selected.
eFax account	Select the fax receiving account for the detected faxes. This does not include the faxes sent to DID mapping extensions if you selected <i>Forward fax to DID mapping extension</i> .
Phone Number	Click <i>New</i> to add the phone number provided by your VoIP service provider. The VoIP service provider SIP server will direct calls from external callers directly to this number. You can add multiple numbers.

4. Click *Create*.

Testing SIP trunks

After you create a SIP trunk, you can select the trunk and click *Test* to see if the trunk works. For more information, see [“Test” on page 170](#).

To test a SIP trunk

1. Go to *Trunks > VoIP > SIP*.
2. Select the trunk that you want to test and click *Test*.
The *System Configuration Test* page appears.
3. Configure the following:

Figure 57: Testing SIP trunk

The screenshot shows the 'System Configuration Test' interface. It features a tabbed interface with 'Test Call - Dry Run' selected. The form includes input fields for 'Destination number' and 'From number', a large text area for 'Test result', and 'Test' and 'Reset' buttons at the bottom.

GUI field	Description
Test 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 <i>Test result</i> .
Reset	Click to remove the test result in order to start a new test.
Test Call	Test the SIP trunk by making a real phone call.
Destination number	Enter a destination number to call.
After call is established	<p>Select the FortiVoice action once it calls the destination number:</p> <ul style="list-style-type: none"> • <i>Play welcome message</i>: The FortiVoice unit will play a message to the destination number. • <i>Connect test call to number</i>: In the <i>Number</i> 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 <i>Test result</i> .
Reset	Click to remove the test result in order to start a new test.

See also

- [Creating a SIP trunk with FortiCall service](#)

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 *Trunks > VoIP > SIP*.
2. Click *FortiCall*.

The *Create SIP Trunk* dialog box displays.

Figure 58: Creating a SIP trunk with FortiCall service

Create SIP Trunk

Would you like to create SIP trunk utilizing our FortiCall service?

☒ FortiCall

MAC Address: 50E549E8DAFC
System ID: FO2HDT00RD000001

Enjoy our reliable enterprise service tailor-made for your FortiVoice systems
Follow this link for more information: [More...](#)

Internet access is required to create FortiCall account. Please make sure the default gateway and DNS are correctly configured.

☒ Create dialplans for this trunk

3. Note down the *MAC Address* and *System ID* for use if you decide to sign up for the service later. See [“To sign up for the FortiCall service”](#) on page 177.

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 *Yes*.
6. Enter your name and email address and click *Create*.
7. Click *OK*.

The FortiCall trunk is created.

To sign up for the FortiCall service

1. Go to *Trunks > VoIP > SIP*.
2. Double-click the trunk named *FortiCall*.
3. Under *Account*, click *Sign Up*.
4. On the FortiCall sign up page, fill out the sign-up form and click *Submit*.

For the *System ID* and *MAC Address* fields, use the noted-down information when you created the FortiCall trunk. See [“To create a SIP trunk with FortiCall service” on page 176](#).

You will receive an email containing your SIP user name and password for logging into and manage your FortiCall account.

To log into the FortiCall account

1. Go to *Trunks > VoIP > SIP*.
2. Double-click the trunk named *FortiCall*.
3. Under *Account*, click *Login*.
4. Enter the login information you received after signing up for the service. See [“To sign up for the FortiCall service” on page 177](#).
5. Click *Login*.

Modifying PSTN/PRI trunks (200D-T and 2000E-T2 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.

This option is only available on the FortiVoice 200D-T and 2000E-T2 models.

The FortiVoice 200D-T supports four FXO (Foreign eXchange Office) analog ports and one FXS (Foreign eXchange Subscriber) digital port.

The FortiVoice 200D-T supports the following default PSTN/PRI trunks:

- T1/E1 voice circuit trunk - *pri1* and *pri2* that use ISDN PRI
- analog CO (Central Office) trunk - *line1* that uses four FXO ports

The FortiVoice 2000E-T2 has two PRI ports and supports two T1/E1 voice circuit trunks - *pri1* and *pri2* that use ISDN PRI.

You can modify the default trunks or create new ones.

To view the PSTN trunks, go to *Trunks > PRI > PRI*.

Figure 59: PRI trunks (200D-T)

Enabled	Name	Status	Type
<input checked="" type="checkbox"/>	pri1	In service	Digital

GUI field	Description
Enabled	Select to activate the trunk.
Name	The name of the trunk.
Status	The trunk statuses, including: <ul style="list-style-type: none"> <i>In service</i>: The trunk is currently in use. <i>Not activated</i>: The trunk is not enabled. <i>Idle</i>: The trunk is not in use. <i>Unavailable</i>: The trunk is not reachable. <i>Conflict</i>: The trunk conflicts with another one. <i>Alarm detected</i>: There is a problem with the trunk. <i>Admin down</i>: The trunk is disabled.
Type	The trunk type: digital or analog.

To add a T1/E1 voice circuit trunk

1. Go to *Trunks > PRI > PRI*.
2. Click *New*.
3. Configure the following:

Figure 60: Adding a T1/E1 trunk

PRI Setting

Name:

Display name:

Number:

Enabled: ☒

Hardware Property

Span: [span1 >>](#)

Fax

☒ Automatic fax detection

☒ Forward fax to DID mapping extension

eFax account:

Phone Number

OK Cancel

GUI field	Description
PRI Setting	
Name	The name of this trunk. This is view only.

Display name	Enter your caller ID that will appear on the called phone, such as Example Company.
Number	Enter the phone number that will appear on the called phone. If you entered the external caller ID in “External caller ID” on page 136 or “External caller ID” on page 154 , this trunk phone number will be overridden by the external caller ID.
Enabled	Select to activate the 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. Click a span name to configure the settings of the T1/E1 span to match the same settings of your PSTN service provider. Click <i>OK</i> after finishing the configuration. For more information, see “Configuring the T1/E1 span” on page 181 .
Fax	Configure fax and phone signal automatic detection and fax handling.
Automatic fax detection	Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically.
Forward fax to DID mapping extension	Some extensions have DID mappings. See “Mapping DIDs” on page 194 . When an incoming fax reaches an extension with DID mapping, selecting this option will send the fax to the DID mapping extension. This option is only selectable if <i>Automatic fax detection</i> is selected.
eFax account	Select the fax receiving account for the detected faxes. This does not include the faxes sent to DID mapping extensions if you selected <i>Forward fax to DID mapping extension</i> .
Phone Number	Click <i>New</i> to add the phone number provided by your PSTN service provider. This is your DID number. Your PSTN service provider will direct calls from external callers directly to this number. You can add multiple numbers, including numbers from full or fractional PRI (T1/E1).

4. Click *Create*.

To add a analog CO trunk for 200D-T

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

Figure 61: Adding an analog CO trunk

Analog Setting

Name:line1

Display name:Fortinet Technologies

Number:6136881230

Enabled:☒

Hardware Property

analog1Edit...

Port: Available ports: (0/4)

->

<-

Done

Selected ports: (4/4)

fxo1

fxo2

fxo3

fxo4

Fax

☒ Automatica fax detection

eFax account:

Phone Number

New...Edit...Delete

Phone Number

OK

Cancel

GUI field	Description
Analog Setting	
Name	The name of this trunk. This is view only.
Display name	Enter your caller ID that will appear on the called phone, such as Example Company.
Number	Enter the phone number that will appear on the called phone. If you entered the external caller ID in “External caller ID” on page 136 or “External caller ID” on page 154 , this trunk phone number will be overridden by the external caller ID.
Enabled	Select to activate the trunk.
Hardware Property	
analog1	Use this option to configure the analog trunk. Click <i>Edit</i> to configure the PSTN analog settings to match the same settings of your PSTN service provider. Click <i>OK</i> after finishing the configuration. For more information, see “Configuring the analog voice trunk” on page 185 .
Port	Select the FXO ports you want for this trunk and click -> to move them into the <i>Selected ports</i> field. Each FXO port provides an analog phone line for a FXO device, such as a phone or fax.

Fax	Configure fax and phone signal automatic detection and fax handling.
Automatic fax detection	Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically.
eFax account	Select the fax receiving account for the detected faxes.
Phone Number	Click <i>New</i> to add the phone number provided by your PSTN service provider. Your PSTN service provider will direct calls from external callers directly to this number. You can add multiple numbers.

4. Click *Create*.

Configuring the T1/E1 span

You can configure the settings of the T1/E1 span, including full or fractional PRI (T1/E1), to match the same settings of your PSTN service provider.



For 2000E-T2, if a PRI trunk includes two spans, the configuration of the second span is much simpler as the spans share many configurations.

For more information, see [“Hardware Property” on page 179](#).

To configure the T1/E1 span

1. On the *PRI* page, click a span name under *Hardware Property*.
2. Configure the following:

Figure 62: Editing T1/E1 card

Standard Options

Name:

span1

Type:

PRI T1

Signalling:

PRI R2 signalling

Advanced Options

Framing and coding option:

ESF/B8ZS

Clocking options:

Clock sourcing from PSTN network

Receive sensitivity:

36dB

D-channel signalling format:

National ISDN 2

Line build out:

0dB(CSU)

D-channel:

24

B-channel:

1-23

PRI R2 Settings

Country:

ITU

Max ANI digits:

20

Max DNIS digits:

7

Caller category:

National-subscriber

Incoming digits mode:

DNIS

DTMF dialing:

☐

DTMF answering:

☐

Allow collect calls:

☐

OK

Cancel

GUI field	Description
Standard Options	
Name	The name of this span. This is view-only.
Type	<p>Select the span type: <i>PRI T1</i> or <i>PRI E1</i>.</p> <p>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.</p>
Signalling	<p>Select the signaling type of the ISDN PRI:</p> <ul style="list-style-type: none"><i>PRI signalling, CPE (Customer Premises Equipment) side</i><i>PRI signalling, Network Side</i><i>PRI R2 signalling</i>
Hardware echo cancellation	Select to enable the FortiVoice echo cancellation function to improve the quality of voice communications.
Hardware DTMF detection	<p>Select to enable the FortiVoice unit to detect dual-tone multi-frequency signals, such as touch-tone signals, from the incoming calls.</p> <p>This option does not need to match that of your PSTN service provider.</p>

Advanced Options

Framing and coding option	<p>Specify the type of framing and coding to provision the PRI with your PSTN service provider.</p>
Clocking options	<p>Select the FortiVoice unit's clock synchronization:</p> <ul style="list-style-type: none">• Clock sourcing from PSTN network• Internal clocking source <p>This option does not need to match that of your PSTN service provider.</p>
Receive sensitivity	<p>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.</p> <p>This option does not need to match that of your PSTN service provider.</p>
D-channel signalling format	<p>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.</p>
Line build out	<p>Select the line build out (LBO).</p> <p>LBO settings are an inherent part of T1 and T3 network element transmission circuitry.</p> <p>Since cable lengths between network elements and digital signal cross-connect (DSX) vary in the central office, LBO settings are used to adjust the output power of the transmission signal to achieve equal level point (ELP) at the DSX.</p>
D-channel	<p>By default, depending on your selection of “Type” on page 182, the typical channel numbers are:</p> <ul style="list-style-type: none">• Full T1: 24• Full E1: 16 <p>You can also set the channel numbers to others such as 1.</p> <p>The settings you configure must match the same settings of your PSTN service provider.</p>

B-channel	<p>By default, depending on your selection of “Type” on page 182, the typical channel settings are:</p> <ul style="list-style-type: none"> • Full T1: 1-23 • Full E1: 1-15, 17-31 <p>You can also configure the fractional channel numbers. For example, for T1/E1, the channels can be:</p> <ul style="list-style-type: none"> • 1-12 • 2, 3, 4, 9-15 • 2-4, 9-15 <p>The settings you configure must match the same settings of your PSTN service provider.</p>
PRI R2 Settings	<p>Since there is no single signaling standard for R2, the FortiVoice unit addresses this challenge by supporting many localized implementations of R2 signaling.</p> <p>This option is active only if you select PRI R2 signalling for “Signalling” on page 182.</p>
Country	Select the country for PRI R2 settings.
Max ANI digits	<p>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.</p> <p>Enter the number of digits of a caller’s phone number to be captured.</p>
Max DNIS digits	<p>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.</p> <p>Enter the number of digits of a dialed call to be sent by the telephone company.</p>
Caller category	Select the caller type.
Incoming digits mode	Select the incoming digits mode by consulting your telephone company.
DTMF dialing	Select to enable dual-tone multi-frequency signaling (DTMF) dialing.
DTMF answering	Select to enable dual-tone multi-frequency signaling (DTMF) answering.
Allow collect calls	Select to allow collect calls.

3. Click **OK**.

Configuring the analog voice trunk

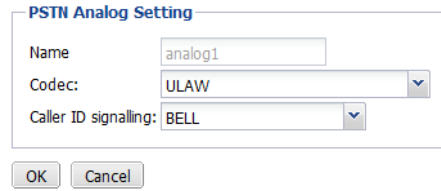
You can configure the settings of the analog CO trunk to match the same settings of your PSTN service provider except the TX/RX gain settings.

For more information, see “[Hardware Property](#)” on page 179.

To configure the analog CO trunk

1. On the *Analog* page, click *Edit* under *Hardware Property*.
2. Configure the following:

Figure 63: Editing analog CO trunk



PSTN Analog Setting

Name:

Codec:

Caller ID signalling:

GUI field	Description
PSTN Analog Setting	
Name	The name of this configuration. This is view-only.
Codec	Select the Codec for the trunk.
Caller ID signalling	Select the caller ID signalling standard per your phone company's request.

3. Click *OK*.

Configuring office peers

If you have remote offices equipped with VoIP network, you can set up office peer trunks so that offices can call each other as if they are local extensions.



For the office peers to call each other, make sure that your FortiVoice unit and the peer office PBX are mutually registered with each other's IP address and SIP port number.

To view the list of office peer trunks, go to *Trunks > Office Peers > Office Peers*.

Figure 64: Office peer trunks

New...

Edit...

Delete

Save

Fetch Office Directory

Page 1

/ 1

Records per page: 25

Enabled	Name	Display name	Type	Server	Port	SIP Setting	Status
<input type="checkbox"/>	OttAsterisk		SIP	172.20.190.254	5060		Admin down
<input checked="" type="checkbox"/>	Off140_60		SIP	172.20.140.64	5060	sip_setting_default	Unmonitored
<input checked="" type="checkbox"/>	Ott2Van	Vancouver	IAX2	172.16.100.95	4569	sip_trunk_default	Unmonitored

GUI field	Description
Fetch Office Directory	<p>Select a trunk and click this button to obtain the phone directory from this office peer.</p> <p>This option only works if the PBX of the remote office is a FortiVoice unit and <i>Fetch directory</i> (see “Fetch Directory” on page 187) is selected on the remote unit.</p> <p>You can view the directory by going to <i>Status > Directory</i> and selecting this office in the <i>Office</i> field. For more information, see “Viewing phone directories” on page 37.</p>
Enabled	Select to activate this trunk.
Name	The name of the office peer.
Display name	The caller ID that will appear on the called phone, such as Example Company.
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	<p>The status of the SIP trunk.</p> <ul style="list-style-type: none">• <i>Not registered</i>: The trunk is not registered with the VoIP service provider and is not in service.• <i>In service</i>: The trunk is registered with the VoIP service provider and is in service.• <i>Unavailable</i>: The trunk is not reachable.• <i>Alarm detected</i>: There is a problem with the phone line.• <i>Admin down</i>: The trunk is disabled.• <i>Unmonitored</i>: The trunk is unknown.

To set up an office peer

1. Go to *Trunks > Office Peers > Office Peers*.
2. Click *New*.
3. Configure the following:

Figure 65: Office peer trunk

Office Peer

Name:

Enabled:

☒

Display name:

Type:

SIP

Remote server:

Remote port:

5060

SIP setting

--None--

New...

Edit...

☐ Fetch directory

Authentication Settings

☐ Incoming authentication

☐ Outgoing authentication

Create

Cancel

GUI field	Description
Office Peer	
Name	Enter a name for the trunk.
Enabled	Select to activate the trunk.
Display name	Enter the caller ID that will appear on the called phone, such as Example Company.
Type	Select the trunk type: <i>SIP</i> or <i>IAX2</i> .
Remote server	Enter the domain name or IP address of the remote office’s PBX.
Remote port	Enter the port number for VoIP network on the remote office’s PBX.
SIP setting	Select the SIP profile for the trunk. You can edit the existing profile or click <i>New</i> to add a new one. For more information, see “Configuring SIP profiles” on page 118 .
Fetch Directory	<p>Select this option and click <i>Fetch now</i> to obtain the phone directory from this office peer.</p> <p>This option only works if the PBX of the remote office is a FortiVoice unit and the same option is selected on the remote unit.</p> <p>You can view the directory by going to <i>Monitor > Directory</i> and selecting this office in the <i>Office</i> field. For more information, see “Viewing phone directories” on page 37.</p>
Authentication Settings	<p>If you want to authenticate incoming and outgoing calls, enable <i>Incoming authentication</i> and <i>Outgoing authentication</i> and enter the <i>Inbound name</i>, <i>Outbound name</i>, and <i>Shared password</i>. These settings must be the same on both PBXs forming the office peer trunk.</p> <p>The PBX on each end will use the settings to authenticate incoming and outgoing calls.</p>

4. Click *Create*.

After setting up the peer office, create outgoing and incoming dial plans for the local and peer offices. For more information, see [“Configuring Call Routing” on page 189](#).

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](#)
- [Configuring outbound dial plans](#)
- [Configuring direct inward dialing](#)

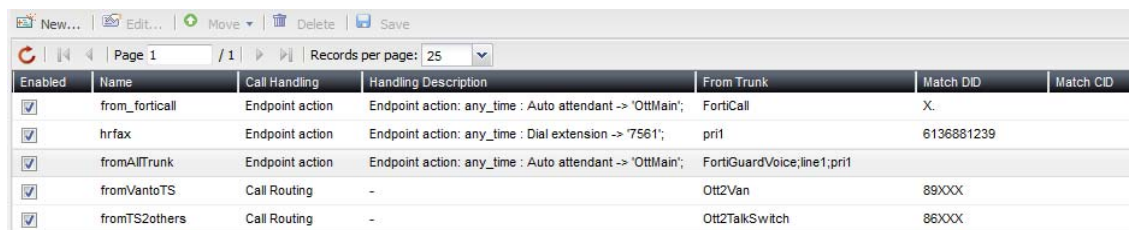
Configuring inbound dial plans

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*.

Figure 66: Viewing inbound dial plans



Enabled	Name	Call Handling	Handling Description	From Trunk	Match DID	Match CID
<input checked="" type="checkbox"/>	from_forticall	Endpoint action	Endpoint action: any_time : Auto attendant -> 'OttMain';	FortiCall	X.	
<input checked="" type="checkbox"/>	hrfax	Endpoint action	Endpoint action: any_time : Dial extension -> '7561';	pri1	6136881239	
<input checked="" type="checkbox"/>	fromAllTrunk	Endpoint action	Endpoint action: any_time : Auto attendant -> 'OttMain';	FortiGuardVoice;line1;pri1		
<input checked="" type="checkbox"/>	fromVantoTS	Call Routing	-	Ott2Van	89XXX	
<input checked="" type="checkbox"/>	fromTS2others	Call Routing	-	Ott2TalkSwitch	86XXX	

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 191 .
Handling Description	The specific call handling actions. For details, see “Action” on page 192 .
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 190 .
Match CID	The caller ID pattern for this dial plan. For details, see “Caller ID Match” on page 191 .

To set up an inbound dial plan

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

Figure 67: Inbound dial plan

Name:

Enabled: ☒

From Trunk

Available : (22/22)

Selected : (0/22)

Babytel
FortiCall
FortiGuardVoice
Ken_YYZ
NexVortex
Of140_60
Ot2BJ
Ot2Sun
Ot2SunFortiVoice
Ot2TalkSwitch
Ot2Van

Dialed Number Match

Caller ID Match

New... Edit... Delete

Caller ID pattern

Caller ID Modification

Apply modification profile: --None-- New... Edit...

Call Handling

Action type: Endpoint action

Action

New... Edit... Move Delete

Schedule	Action	Target
----------	--------	--------

Create Cancel

GUI field	Description
Name	Enter a name for this plan.
Enabled	Select to activate this dial plan.
From Trunk	Select the trunks of the incoming calls that are subject to this dial plan. Select the trunks in the <i>Available</i> field and click -> to move them into the <i>Selected</i> field.
Dialed Number Match	With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers. The called numbers matching this pattern will follow this dial plan rule. Create the number match following “Pattern-matching syntax” on page 199 and “Pattern-matching examples” on page 199 .

Caller ID Match	<p>Click <i>New</i> to set the caller ID pattern following “Pattern-matching syntax” on page 199 and “Pattern-matching examples” on page 199 for this dial plan, and click <i>Create</i>.</p> <p>You can enter an incoming call’s display name string or the caller’s phone number string as the pattern.</p> <p>Caller IDs under this pattern are subject to this plan.</p>
Caller ID modification	<p>Select the caller ID modification configuration. Click <i>Edit</i> to modify the selected configuration or click <i>New</i> to configure a new one. For more information on caller ID modification, see “Modifying caller IDs” on page 120.</p>
Call Handling	<p>Select the actions to process the incoming calls with matched dialed numbers and/or caller IDs.</p>
Action type	<p>Select the type of action for the plan and configure the actions accordingly. See “Action” on page 192.</p> <ul style="list-style-type: none"> • <i>Endpoint action</i>: 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. • <i>Dial local number</i>: Select if you want to send incoming calls to the local destinations at any time. For example, you can enter 222xxxx as a pattern and strip 222. The FortiVoice unit will only dial the last four digits for all called numbers matching the pattern. • <i>Call routing</i>: Select if you want to route incoming calls (to the FortiVoice unit) to an external phone system using an outbound dial plan.

Action

Depending on the selected *Action type*, click *New* to configure the actions:

- If you select the *Endpoint action type*:
 - a. Select the FortiVoice operation schedule for the action. Click *Edit* to modify the selected schedule or click *New* to configure a new one. For more information on PBX schedule, see [“Scheduling the FortiVoice unit” on page 121](#).
 - b. Select an action for the incoming calls under this plan.
For some actions, you need to enter the extension (such as *Go voicemail*) or select a profile (such as *Play announcement*).
 - c. Click *Create*.
 - d. Repeat this procedure if you need more actions for this action type.

Do not use the same schedule for more than one action to avoid schedule conflict.
 - If you select the *Dial local number type*:
 - a. Click *New* to add the number pattern in the *Value* field following [“Pattern-matching syntax” on page 199](#) and [“Pattern-matching examples” on page 199](#) for this dial plan. Repeat to add more patterns.
 - b. For *Strip*, enter a number to omit dialing the starting part of a pattern. 0 means no action.

For example, if your *Match Pattern* is 222XXXX and *Strip* is 3, the FortiVoice unit will only dial the last four digits for all called numbers matching the pattern.
 - c. For *Prefix*, add a number before a pattern.

For example, if your *Match Pattern* is 9XXX and the numbers under this pattern have been upgraded to have an additional digit 5 at the beginning, you can enter 5 for the *Prefix*. When an incoming call matches the pattern, the FortiVoice unit will add a 5 before the number.
 - d. For *Postfix*, add a number after a pattern.

For example, if your *Match Pattern* is 9XXX and the numbers under this pattern have been upgraded to have an additional digit 5 at the end, you can enter 5 for the *Postfix*. When an incoming call matches the pattern, the FortiVoice unit will add a 5 after the number.
 - e. Click *Create*.
 - If you select the *Call routing type*, select the available outbound dial plans and click -> to move them into the *Selected member* field. This means that the FortiVoice unit will route incoming calls to an external phone system using the selected outbound dial plans.
-

4. Click *Create*.

Configuring direct inward dialing

The *Call Routing > Inbound > DID Mapping* submenu lets you configure how to map Direct Inward Dialing (DID) numbers.

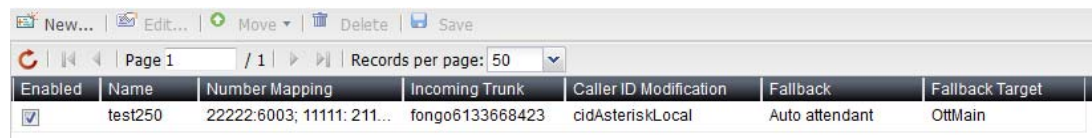
Local phone companies offer DID service to provide a block of telephone numbers for calling into a company's PBX system over limited rented physical lines (also called "trunk lines"). The phone numbers you rent may not be enough to provide a DID number for each workstation, because each DID can only be mapped to one extension. With the FortiVoice unit, you have 2 options to address this issue:

- only map the DID numbers to the extensions you want.
- map a DID number to one or more extensions based on the callers' phone numbers.

For more information, see ["Mapping DIDs" on page 194](#).

To view the DIDs, go to *Call Routing > Inbound > DID Mapping*.

Figure 68: Viewing DID mappings



Enabled	Name	Number Mapping	Incoming Trunk	Caller ID Modification	Fallback	Fallback Target
<input checked="" type="checkbox"/>	test250	22222:6003; 11111: 211...	fongo6133668423	cidAsteriskLocal	Auto attendant	OttMain

GUI field	Description
Enabled	Select to activate this DID.
Name	The name of the DID.
Number Mapping	The DID number and the extension it is mapped to. For details, see "Mapping DIDs" on page 194 .
Incoming Trunk	The trunk used for dialing the DIDs.
Caller ID modification	The caller ID modification configuration. For more information, see "Inbound caller ID modification" on page 194 .
Fall back	The action to take if a caller not in the caller list dialed the DID number mapped to the extensions.
Fallback Target	The extension to dial for the <i>Action</i> you choose. For details, see "Inbound fallback action" on page 194 .

To configure a DID

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

Figure 69: DID setting

Direct Inward Dial Setting

Name:

Enabled:

☒

Trunk:

--None--

Inbound caller ID modification:

--None--

Inbound fallback action:

Hang up

Number Mapping

New... Edit... Delete Export Import

Page 1 / 1 Records per page: 25

DID Number Extension Inbound Outbound Caller ...

Create Cancel

GUI field	Description
Direct Inward Dial Setting	
Name	Enter a name for this DID setting.
Enabled	Select to activate this DID setting.
Trunk	Select the trunk used for dialing the DIDs.
Inbound caller ID modification	Select the caller ID modification configuration. For more information on caller ID modification, see “Modifying caller IDs” on page 120 .
Inbound fallback action	Select the action to take if a caller not in the caller list dialed the DID number mapped to an extension. For some actions, you need to enter the extension, such as <i>Dial voicemail</i> . For information on filtering callers, see “Mapping DIDs” on page 194 .
Number Mapping	For adding a number mapping, see “Mapping DIDs” on page 194 . Click <i>Export</i> to open or save the number mapping file and <i>Import</i> to browse for a number mapping file.

4. Click *Create*.

Mapping DIDs

You can map a DID number to one extension. You can also map a DID to multiple extensions based on the callers’ phone numbers. For example, calling numbers 123-4567, 123-4568, and 123-4569 can call the DID number 222-1000 to reach extension 1234. Calling numbers 234-4567, 234-4568, and 234-4569 can call the same DID number 222-1000 to reach extension 1265. In both cases, the calling numbers will display on the extension.

If a caller outside the configured caller list dialed the mapped DID number, the FortiVoice unit will react according to the selected fall back action. For details, see [“Inbound fallback action” on page 194](#).

To map DIDs

1. Go to *Call Routing > Inbound > DID Mapping*.

2. Click *New*.
3. In *Number Mapping*, click *New*.
4. Configure the following:

Figure 70: DID mapping

The screenshot shows a 'Map Settings' dialog box. It has two input fields: 'DID number' and 'Extension'. Below these are two checkboxes: 'Inbound' (checked) and 'Outbound' (checked). There is an 'Advanced Setting' section with a 'Caller number' field and a 'Pattern String' field. At the bottom are 'Create' and 'Cancel' buttons.

GUI field	Description
Map Setting	This option allows you to map a DID number to an extension.
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 (see “Advanced Setting” on page 196). Otherwise, an error message about duplicate entry appears and the DID mapping configuration cannot be saved.
Extension	Enter the extension that you want to map to the DID number.
Option	<p>Select <i>Inbound</i> to direct incoming calls to the extension through the mapped DID. If this option is not selected, incoming calls to this extension through the mapped DID will follow the inbound fallback action configured in “Inbound fallback action” on page 194. By default, this option is selected.</p> <p>Select <i>Outbound</i> to send the DID numbers of the extensions mapped to the DID with outgoing calls so that the DID numbers can display on the called phones. If this option is not selected, the extension’s DID number is not sent with outgoing calls and the phone number displayed on the called phone could be the FortiVoice main number (see “Main number” on page 102) or the trunk phone number (see “Phone Number” on page 175) associated with the extension. Alternatively, you can choose the caller ID to display on the called phone when configuring an extension (see “External caller ID” on page 136).</p> <p>By default, both <i>Inbound</i> and <i>Outbound</i> are selected.</p>

Advanced Setting	This option allows you to bundle caller numbers to a DID number which can be mapped to any extension.
Caller number	<p>Click <i>New</i> to add the caller's phone number or pattern in the <i>Pattern String</i> field and click <i>Create</i>.</p> <p>Repeat to add more calling numbers or patterns.</p> <p>Only the caller numbers matching the numbers or patterns you set will reach the mapped extension when they dial the DID number.</p> <p>For information on phone number patterns, see “Pattern-matching syntax” on page 199 and “Pattern-matching examples” on page 199.</p>

5. Click *Create*.

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*.

Figure 71: Viewing outbound dial plans

Enabled	Name	Pattern	Match CID	Call Handling
<input checked="" type="checkbox"/>	Vancouver_auth	4X;		any_time : Ott2Van
<input type="checkbox"/>	Beijing_auth	86XXX; 8610X;		any_time : Ott2BJ
<input checked="" type="checkbox"/>	Van2	55X;		any_time : Ott2Van
<input checked="" type="checkbox"/>	Emergency	911;		- : line1

GUI field	Description
Test	<p>Select to test if the dial plan is created successfully.</p> <p>For more information, see “Testing outbound dial plans” on page 198.</p>
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 197 .
Match CID	The caller ID pattern for this dial plan. For details, see “Caller ID Match” on page 198 .
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 198 .

To set up an outbound dial plan

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

Figure 72: Outbound dial plan

GUI field	Description
Name	Enter a name for this plan.
Enable	Select to activate this dial plan.
Emergency call	Select to allow emergency call with this plan. By default, this is selected. For information on setting emergency number, see “Setting PBX location and contact information” on page 101 .
Dialed Number Match	With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers. The dialed numbers matching this pattern will follow this dial plan rule. For information on adding a dialed number match, see “Creating dialed number match” on page 199 .

Caller ID Match	<p>Click <i>New</i> to set the caller ID pattern following “Pattern-matching syntax” on page 199 and “Pattern-matching examples” on page 199 for this dial plan, and click <i>Create</i>.</p> <p>You can enter a caller’s display name string or the caller’s phone number string as the pattern.</p> <p>Callers with IDs under this pattern are subject to this plan.</p>
Call Handling	<p>Click <i>New</i> 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 201.</p>

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 196.

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*.
The call test page appears.
3. Configure the following:

Figure 73: Testing dial plans

The screenshot shows a web interface titled "System Configuration Test". There are two tabs: "Test Call - Dry Run" (which is active and highlighted in orange) and "Test Call". Below the tabs, there are two input fields: "Destination number:" and "From number:". Below these fields is a large, empty text area labeled "Test result:". At the bottom left of the form, there are two buttons: "Test" and "Reset".

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 <i>Test result</i> .
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: <ul style="list-style-type: none"> • <i>Play welcome message</i>: The FortiVoice unit will play a message to the destination number. • <i>Connect test call to number</i>: In the <i>Number</i> 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 <i>Test result</i> .
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:

Table 25:Pattern-matching syntax

Syntax	Description
X	Matches any single digit from 0 to 9.
Z	Matches any single digit from 1 to 9.
N	Matches any single digit from 2 to 9.
[15-7]	Matches a single character from the range of digits specified. In this case, the pattern matches a single 1, as well as any number in the range 5, 6, 7.
.	Wildcard match; matches one or more characters, no matter what they are.
!	Wildcard match; matches zero or more characters, no matter what they are.

Table 26:Pattern-matching examples

Pattern	Description
NXXXXXX	Matches any seven-digit number, as long as the first digit is 2 or higher.
NXXNXXXXXX	This pattern matches with areas with 10-digit dialing.

Table 26:Pattern-matching examples

Pattern	Description
1NXXNXXXXXX	Matches the number 1, followed by an area code between 200 and 999, then any seven-digit number. In the North American Numbering Plan calling area, you can use this pattern to match any long-distance number.
011.	Matches any number that starts with 011 and has at least one more digit.

To create a dialed number match

1. Go to *Call Routing > Outbound > Outbound*.
2. Click *New*.
3. In *Dialed Number Match*, click *New*.
4. Configure the following:

Figure 74: Creating a number match

GUI field	Description
Match Pattern	
New	Click to add the number pattern in the <i>Value</i> field following “ Pattern-matching syntax ” on page 199 and “ Pattern-matching examples ” on page 199 for this dial plan. Repeat to add more patterns.
Modification	You can manipulate the number patterns you entered.
Strip	<p>Enter a number to omit dialing the starting part of a pattern. 0 means no action.</p> <p>For example, if your <i>Match Pattern</i> is 9XXX and <i>Strip</i> is 1, you only need to dial the last three digits for this pattern.</p>

Prefix	<p>Add a number before a pattern, such as area code.</p> <p>For example, if your <i>Match Pattern</i> is 123XXXX and its area code is 555, you can enter 555 for the <i>Prefix</i>. When you dial a number under this pattern, you do not need to dial the area code 555.</p>
Postfix	<p>Add a number after a pattern.</p> <p>For example, if your <i>Match Pattern</i> 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 <i>Postfix</i>. When you dial a number under this pattern, you do not need to dial the last digit 5.</p>

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 <i>Edit</i> to modify the selected schedule or click <i>New</i> to configure a new one. For more information on PBX schedule, see “Scheduling the FortiVoice unit” on page 121 .
Action	Select the call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern.
Outgoing trunk	Select the trunk for the outbound calls. Click <i>Edit</i> to modify the selected trunk or click <i>New</i> to configure a new one. For more information on trunks, see “Configuring Trunks” on page 170 .
Caller ID modification	Select the caller ID modification configuration. Click <i>Edit</i> to modify the selected configuration or click <i>New</i> to configure a new one. For more information on caller ID modification, see “Modifying caller IDs” on page 120 .

Warning message	If you select <i>Allow with warning</i> or <i>Deny with warning</i> in the <i>Action</i> field, select the sound file for the warning. Click <i>Edit</i> to modify the selected file or click <i>New</i> to configure a new one. For more information on sound files, see “Managing sound files and music on hold” on page 116 .
Delay	Optionally, if you want to discourage certain users for making outbound calls, enter the call delay time in seconds.

5. Click *Create*.

Working with Property Management System

Businesses such as hotels use Property Management System (PMS) to manage their services. The PMS can be connected to a PBX such as the FortiVoice unit to configure a customer's room phone by displaying the customer's name on the phone, emptying voicemails when a new customer checks in, logging phone calls, setting wake-up calls, and other services. You can also set the room condition codes for room maids to record the room cleaning status using the room phone.

This option is only available if you have purchased license.

This topic includes:

- [Configuring hotel management settings](#)
- [Configuring hotel room status](#)

Configuring hotel management settings

Hotel Management > Setting lets you configure the settings for the FortiVoice unit to interoperate with your PMS, set the room condition codes, such as setting 1 to represent that maid is present and 4 to represent out of service, and configure guest check in and check out actions.

Configure your PMS settings accordingly.

To configure hotel management settings

1. Go to *Hotel Management > Setting > PMS*.
2. Select to enable the PMS.
3. For *PMS protocol*, select the protocol used by the FortiVoice unit to communicate with the PMS.
4. For *Port*, enter the port number that connects to the PMS.

Note that you need to use an adaptor for the FortiVoice-PMS connection. Fortinet recommends using iPocket232 by Precidia. From the ports you configured, connect the PMS serial cable to the adaptor and then connect the RJ45 cable from the FortiVoice unit to the adaptor.

5. For *Trusted hosts*, enter the IP address and netmask of the PMS. If the PMS uses serial connection to an adaptor, enter the IP address and netmask of the adaptor.

If you have multiple PMSes, you may enter multiple trusted hosts.

6. Click *OK*.

To set room condition codes

1. Go to *Hotel Management > Setting > Condition Code*.
2. Click *New* to add a code or select an existing code and click *Edit* to modify it.
3. Select the protocol for connecting to your PMS.
4. Enter a code number.
5. Enter the code description.
6. Click *Create*.

To configure check in and check out actions

1. Go to *Hotel Management > Setting > Option*.
2. Configure the following:

<i>GUI field</i>	<i>Description</i>
Check in action	
Reset	<p>Set the guest information and room condition to make a room check-in ready.</p> <ul style="list-style-type: none">• <i>Privilege</i>: 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 <i>Privilege</i> for the room user. For information on setting user privileges, see “Configuring user privileges” on page 132• <i>Guest name</i>: Select to display room number or guest name on the room extension. In the <i>Name</i> field, enter %%NUMBER%% or %%NAME%%.• <i>Room condition</i>: Select to clear any condition set for the room.
Check out action	
Reset	<p>Set the guest information and room condition to make a room check-out ready.</p> <ul style="list-style-type: none">• <i>Privilege</i>: 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 <i>Privilege</i> for the room user. For information on setting user privileges, see “Configuring user privileges” on page 132• <i>Guest name</i>: Select to display room number or guest name on the room extension. In the <i>Name</i> field, enter %%NUMBER%% or %%NAME%%.• <i>Room condition</i>: Select to clear any condition set for the room.• <i>Voice mail</i>: Select to clear all voicemails for the room extension.• <i>Wakeup call</i>: Select to clear all wakeup call setups for the room extension.

3. Click *Apply*.

Configuring hotel room status

Hotel Management > Room Status lets you set hotel room statuses.

Once the PMS and the FortiVoice unit is properly connected and the PMS is enabled on the FortiVoice unit, all hotel room extensions appear on the FortiVoice unit.

To batch-configure hotel room statuses

1. Go to *Hotel Management > Room Status*.
2. Select more than one room in the list.

Depending on the situations of the rooms you select, the *Check in*, *Check out*, *Privilege*, *Condition code*, and *Guest status* buttons become active.

3. Click a button to batch-configure the room status and apply it to all rooms.

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:

Figure 75:Hotel room status

Room status

Number: 7701 ☒ Guest phone
Room: 7701
Location: [Click to edit...](#)

Checkin status: ☐ Checked-out ☒ Checked-in
Guest name:
Privilege:
DND: ☐
Room condition:

GUI field	Description
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 133.
Guest phone	Select to bind the extension with the room and make the room a guest room.
Room	The hotel room number. You can click the number and modify it if required.
Location	Click to enter the room location.
If you have selected <i>Guest phone</i> , configure the following:	
Checkin status	Choose the room status to configure: <i>Checked-out</i> or <i>Checked-in</i> .
Guest name	Enter the name of the guest for this room. This option is available only if the <i>Checkin status</i> is <i>Checked-in</i> .
Privilege	Select phone call restriction (internal, local, or long distance) and user privilege (option 1, 2, 3) for the room. For information on setting user privileges, see “Configuring user privileges” on page 132. This option is available only if the <i>Checkin status</i> is <i>Checked-in</i> .
DND	Select if the guest of the room does not want to be disturbed. This option is available only if the <i>Checkin status</i> is <i>Checked-in</i> .
Room condition	Select the cleaning status of the room. You can add a new code or edit the current one. For more information, see “To set room condition codes” on page 203.

4. Click *OK*.

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](#)
- [Configuring user privileges](#)
- [Configuring account codes](#)
- [Mapping speed dials](#)
- [Configuring conference calls](#)
- [Recording calls](#)
- [Creating call queues](#)
- [Configuring call parking](#)
- [Configuring fax](#)
- [Modifying feature access codes](#)

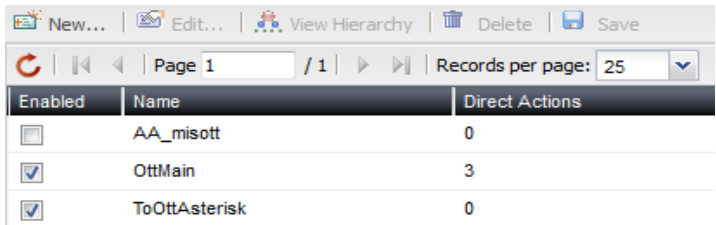
Configuring auto attendants

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.

To view the list of auto attendants, go to *Call Features > Auto Attendant > Auto Attendant*.

Figure 76: Auto attendants list



Enabled	Name	Direct Actions
<input type="checkbox"/>	AA_misott	0
<input checked="" type="checkbox"/>	OttMain	3
<input checked="" type="checkbox"/>	ToOttAsterisk	0

<i>GUI field</i>	<i>Description</i>
View Hierarchy	Click to view the hierarchical structure of the selected auto attendant. For more information, see “Viewing auto attendant hierarchies” on page 209 .
Delete	Removes a selected auto attendant. You cannot remove an auto attendant that is used in another auto attendant configuration.
Enabled	Select to activate this auto attendant.

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. For more information, see “Viewing auto attendant hierarchies” on page 209 .

To create an auto attendant

1. Go to *Call Features > Auto Attendant > Auto Attendant* and click *New*.
2. Configure the following:

Figure 77: New auto attendant

Auto Attendant

Name:

Enabled: ☒

Default language: --Default--

Greeting mode: ☒ Simple ☐ Scheduled

Greeting: --None--

Ringing for: 0 seconds before answer

Time out after: 20 seconds if no response

Timeout action: Start over Maximum number of times: 3

Invalid input action: Dial operator

Dial Pad Key Action

New... Edit... Delete

Key	Action	Target
-----	--------	--------

Advanced

☐ Enable voicemail access

☒ Dial local number

☐ Call Bridge(DISA) Account code: --None--

Outbound dialplans allowed for access:

Available : (43/43)

Selected : (0/43)

Beijing
Beijing_auth
Emergency
FXOOut
FortiCall_service
FortiGUardService
MIS
MIS2
OttAsteriskLocal
PrimusSIPOut
PrimusT1

GUI field Description

Auto Attendant

Name	Enter a name for the auto attendant.
Enabled	Select to activate the auto attendant.

Default language	<p>Select the language for the auto attendant greeting message (sound file). If you select <i>Default</i>, the greeting message will be the same as what you set for the FortiVoice unit. For more information, see “Setting PBX location and contact information” on page 101.</p> <p>You can also select other languages. The language files are created in “Adding prompt languages” on page 113.</p>
Greeting mode	<p>If you select <i>Simple</i>, select a greeting message (sound file) for the auto attendant. See “Greeting” on page 208.</p> <p>If you select <i>Scheduled</i> to add a scheduled greeting, do the following:</p> <ul style="list-style-type: none"> • In <i>Scheduled Greeting Setting</i>, click <i>New</i>. • In the <i>Schedule</i> field, select a schedule for the greeting. Scheduled are created in “Scheduling the FortiVoice unit” on page 121. • In the <i>Greeting</i> field, select a sound file. You can click <i>New</i> to add a new file or <i>Edit</i> to modify the selected one. For more information, see “Managing sound files and music on hold” on page 116. • Click <i>Create</i>.
Greeting	<p>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 sound files and music on hold” on page 116.</p> <p>This option is only available if you select the <i>Simple</i> greeting mode.</p>
Ring for	Enter the number of seconds for the phone to ring before the auto attendant answers with the greeting message.
Timeout 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.
Timeout action	<p>Select the action when the auto attendant timeout is reached.</p> <ul style="list-style-type: none"> • <i>Dial operator</i>: The call is transferred to an operator. • <i>Dial extension</i>: 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 133. • <i>Start over</i>: The auto attendant will repeat the instructions for the caller. Also enter the maximum times to repeat. • <i>Hang up</i>: The call will be terminated.
Invalid input action	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 211 .
Key	The key that transfers a call to a resource, for example, voicemail, if pressed.
Action	The resource to which a call is transferred by pressing a key.

Target	The resource target if applicable. For example, an extension number, sound file, or external phone number that leads to a resource.
Advanced	<p>Upon finishing configuring these functions, you need to inform the users on how to use them after they reach the auto attendant.</p> <ul style="list-style-type: none"> • <i>Enable voicemail access</i>: 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 241. • <i>Dial local number</i>: Select to enable an external caller to dial local extensions. • <i>Call Bridge (DISA)</i>: Select an account code for external users to dial into the FortiVoice unit and use the FortiVoice service just like the local extensions. Callers must dial the DISA code followed by the account code before making the calls. You can edit a selected account code or create a new one. For more information on DISA code, see “Modifying feature access codes” on page 241. For more information on account code, see “Configuring account codes” on page 218. • <i>Outbound dialplans allowed for access</i>: Select the outbound dial plan for users to call the FortiVoice unit and through it to make outbound calls. For details, see “Configuring outbound dial plans” on page 196.

3. Click *Create*.

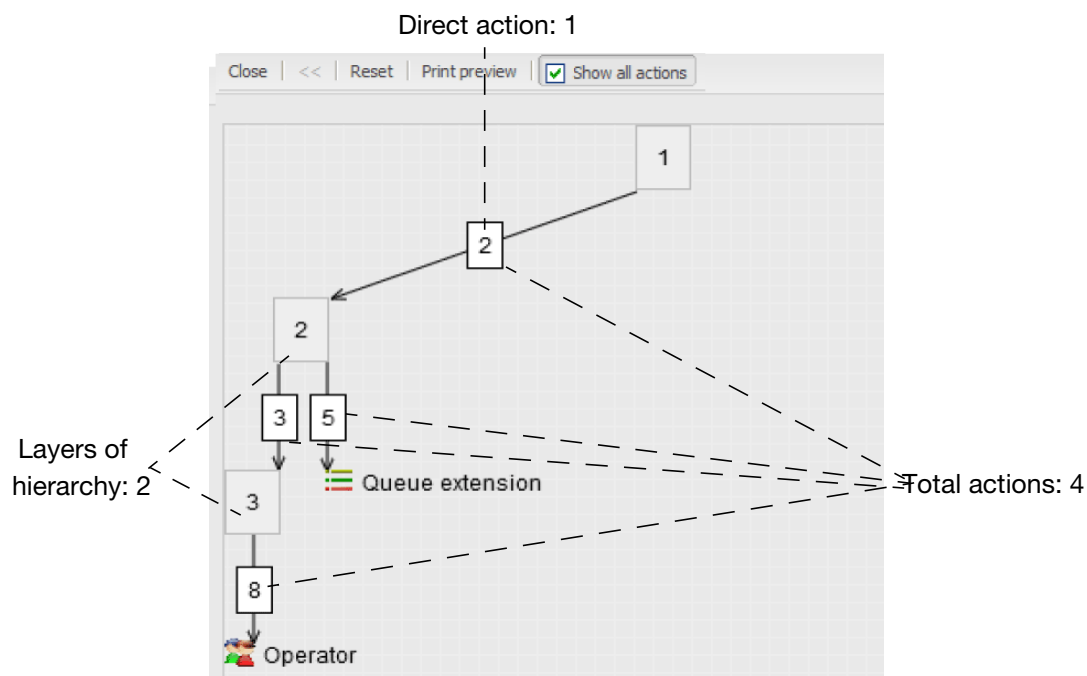
Viewing auto attendant hierarchies

The FortiVoice unit provides a chart based on your auto attendant configurations to display the layers of auto attendant hierarchy and the key actions. You can save the chart and load it later. You can also drag the chart into the shape you want.

To view the auto attendant hierarchy

1. Go to *Call Features > Auto Attendant > Auto Attendant*.
2. From the auto attendant list, select the one of which you want to view its hierarchy chart.
3. Click *View Hierarchy*.

Figure 78: Sample auto attendant hierarchy



This example shows the hierarchy of auto attendant 1.

- Based on the configuration, press 2 transfers the call to auto attendant 2.
- Auto attendant 2 configuration allows you to go to auto attendant 3 by pressing 3 and places you on a call queue if you press 5.
- Auto attendant 3 configuration allows you to go to the operator by pressing 8.

You can right-click an auto attendant node and select *Edit* to modify it or view the snapshot of an auto attendant (other than the main one) by right-clicking it and selecting *Drill down*.

Table 27: Sample auto attendant hierarchy

Close	Closes the chart.
<<	If you selected viewing the snapshot of an auto attendant (other than the main one) by right-clicking it and selecting <i>Drill down</i> on the chart, clicking << restores the full chart.
Reset	Sets the chart to its default view. All the saved and unsaved views will be lost.
Print preview	Click to preview the chart before printing it.
Show all actions	Select to display the total actions. Deselect to hide the end resources to which a call is transferred by pressing a key. In this sample, the end resources are Operator (8) and Queue extension (5).

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 208](#).

To configure a key action

1. While configuring an auto attendant, click *New* under *Dial Pad Key Action*.
2. Enter the key number that transfers a call to a resource, if pressed.
3. Select an action:

GUI field	Description
No action	The call is not transferred to any resource.
Play announcement	<p>Play an announcement with directions, business hours, etc.</p> <ul style="list-style-type: none"> • Select an action to follow the announcement: <ul style="list-style-type: none"> • <i>No action</i>: The auto attendant takes no action. • <i>Start over</i>: The auto attendant will repeat the announcement. • <i>Hang up</i>: The call will be terminated. • Select the sound file for the announcement. You can click <i>Edit</i> to modify an existing one or <i>New</i> to add a new one. For information on sound files, see “Managing sound files and music on hold” on page 116.
Dial operator	The call is transferred to the operator.
Dial extension	<p>The call is transferred to a specified local extension.</p> <p>Select the extension. You can click <i>Edit</i> to modify an existing one or <i>New</i> to add a new one. For more information, see “Configuring Extensions” on page 133.</p>

Go voicemail	<p>The call is transferred to a voice mailbox, allowing the caller to leave a message.</p> <p>Select the voice mailbox. You can click <i>Edit</i> to modify an existing one or <i>New</i> to add a new one. For more information, see “Configuring IP extensions” on page 133.</p>
Ring group	<p>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.</p> <p>Select the ring group. You can click <i>Edit</i> to modify an existing one or <i>New</i> to add a new one. For more information, see “Creating extension groups” on page 159.</p>
Dial number	<p>The call is transferred to a specified remote extension number.</p> <p>Enter the remote extension number. For more information, see “Setting up remote extensions” on page 145.</p>
Call queue	<p>The call is transferred to a call queue.</p> <p>Enter the call queue configuration. For more information, see “Creating call queues” on page 224.</p>
Lookup name directory	<p>Access the dial-by-name directory so the caller can find a user’s extension number by entering the user’s name.</p>
Change language	<p>Change the auto attendant greeting language. Select the language and a follow-up action. If you choose <i>Auto attendant</i> for the follow-up action, select the auto attendant.</p> <p>For <i>Language</i>, if you select <i>Default</i>, the greeting message will be the same as what you set for the FortiVoice unit. For more information, see “Setting PBX location and contact information” on page 101.</p> <p>You can also select other languages. The language files are created in “Adding prompt languages” on page 113.</p>
Auto attendant	<p>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.</p> <p>Select an auto attendant. For information on creating auto attendants, see “Configuring auto attendants” on page 206.</p>
Start over	<p>The auto attendant will repeat the announcement.</p>
Go back	<p>The auto attendant will repeat the previous level announcement.</p>
Hang up	<p>The call is terminated.</p>

4. Optionally, enter any comments about this key action.
5. 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 not be deleted.

For information on extensions, see “Configuring Extensions” on page 133.

To configure a user privilege

- 1. Go to *Call Features > User Privileges > User Privileges* and click *New*.
- 2. Configure the following:

Figure 79: User privilege configuration

Name:

Basic Settings

☒ Auto provisioning

☒ List in directory

☒ Configure programmable phone key/PPK

☒ Lookup directory

☒ Lookup directory in remote office(s)

Role Settings

☐ Operator role

Voice Mail

☒ Enabled

Maximum messages:

Voice mail retention days:

Music

Fax

Call Restriction

Monitor/Recording

Hot-desking

Advanced

Create

Cancel

GUI field	Description
Name	Enter a name for this class of service.
Basic Settings	

Auto provisioning	<p>Select to enable auto-provisioning for the extension. For more information, see “Configuring SIP phone auto-provisioning” on page 111.</p> <p>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.</p>
List in directory	<p>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.</p>
Configure programmable phone feature key/PFK	<p>Select to enable configuring the feature access codes. For more information, see “Modifying feature access codes” on page 241.</p>
Lookup directory	<p>Select to enable a user to view the phone directory of the local office. For more information, see “Viewing phone directories” on page 37.</p>
Lookup directory in remote offices)	<p>Select to enable a user to view the phone directories of remote offices. For more information, see “Viewing phone directories” on page 37.</p>
Role Settings	
Operator role	<p>Select to enable an extension user to process phone calls using the FortiVoice user web portal.</p> <p>When the user privilege with this option selected is applied to an extension, an <i>Operator Console</i> button will appear on the top of the extension user’s FortiVoice web portal. Clicking the button lets the user to process phone calls on the Web.</p> <p>For more information, see the online help of the user web portal.</p>
Voice Mail	
Enabled	<p>Select to enable the voicemail service.</p>
Maximum messages	<p>Enter the number of voice mails allowed.</p>
Voicemail retention days	<p>Enter the number of days to keep the voicemails.</p>
Music	
Music on hold	<p>Select a music on hold file. For details, see “Managing sound files and music on hold” on page 116.</p>

Early media	Early media is the exchange of information between the PBXes before the establishment of a phone connection, such as the ring tone. You can select a music file for early media. For details, see “Managing sound files and music on hold” on page 116 .
Fax	Set the user rules for faxing. For information on fax, see “Configuring fax” on page 230 .
Enabled	Select to set the fax rules for users.
Max incoming messages	Enter the number of incoming faxes allowed.
Max incoming fax retention days	Enter the number of days to keep the incoming faxes.
Max outgoing messages	Enter the number of outgoing faxes allowed.
Max outgoing fax retention days	Enter the number of days to keep the outgoing faxes.
Call Restriction	
Allow long distance call	Select to allow long-distance direct dialing. If required, select the account code that needs to be dialed before making a long-distance call. For information on account code, see “Configuring account codes” on page 218 .
Allow international call	<p>Select to allow international direct dialing. If required, select the account code that needs to be dialed before making a long distance call. For information on account code, see “Configuring account codes” on page 218.</p> <p>There are phone numbers with certain calling services and likely higher calling rates such as 900 number in North America and 0990-5 number in Japan. These numbers do not belong to international calls or long-distance calls and can be banned on a system-wide basis (see “Configuring PBX options” on page 102). However, if you want to allow calling to some of these numbers, click <i>New</i> and configure the following:</p> <ol style="list-style-type: none"> 1. Enter a name for this setting. 2. Select <i>Enabled</i> to activate this exemption. 3. Enter the area code/prefix of the number to be called, such as 900. 4. Select the account/exempt code that needs to be dialed before making a call with this prefix. For information on account code, see “Configuring account codes” on page 218. 5. Click <i>Create</i>.

Other restricted area code	<p>You can specify area codes to which an extension is allowed or denied to make phone calls.</p> <ol style="list-style-type: none"> 1. Click <i>New</i>. 2. Enter a name for this call restriction. 3. Select <i>Enable</i> to activate this restriction. 4. Enter the area code that you want to set restriction. 5. If you do not want an extension to call the area code you set, select <i>None</i> for <i>Exempt code</i>; otherwise, select a code. For information on exempt code, see “Configuring account codes” on page 218. 6. Click <i>Create</i>.
Misc	<ul style="list-style-type: none"> • <i>Internal numbers</i>: Select to allow an extension to dial internal extensions. • <i>Local/city numbers</i>: Select to allow an extension to make local calls. • <i>The max number of concurrent calls</i>: Set the maximum number of concurrent incoming and outgoing calls on the extension. The range is 1-10.
Monitor/Recording	Configure monitoring and recording outgoing and incoming calls of an extension to which this user privilege is applied.
Personal recording	Select to allow users to configure personal recording of their incoming and outgoing calls on the user web interface.
Allow being barged	Select to allow monitoring an extension to which this user privilege is applied.
Allow barging	<p>Select to allow the extension to which this user privilege is applied to monitor other extensions.</p> <p>To barge a call, you need to enter your user PIN. For information on user PIN, see “User PIN” on page 137.</p>
Call barge option	If you select <i>Allow barging</i> , choose a barging method.

Hot-desking

Hot desking enables users to log into another phone. However, unlike using Follow Me or Call Forwarding which simply redirect a user's calls to another user's phone, hot desking takes total control of another phone by applying all of the user's own phone 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 and enter his extension number and user PIN.

You can view hot desking configurations by going to [“Viewing hot desking configurations” on page 26](#).

- *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 doing so, the regular phone keeps its configuration and extension number. However, outgoing calls display the hot-desking number.
The regular phone logs out of hot-desking when the time set in *Automatic logout hours* expires.

Advanced

Conference number Select the permission for conference calls:

- *Allow all*: Select to allow all extensions to join conference calls.
- *Disallow all*: Select to prohibit all extensions from joining conference calls.
- *Allow all with exempt*: If you select this option, click *New* to enter the number(s) banned for joining conference calls.
- *Disallow all with exempt*: If you select this option, click *New* to enter the number(s) allowed for joining conference calls.

For more information, see [“Configuring auto attendants” on page 206](#).

Paging number

Select the permission for paging:

- *Allow all*: Select to allow all paging numbers to page.
- *Disallow all*: Select to prohibit all paging numbers from paging.
- *Allow all with exempt*: If you select this option, click *New* to enter the number(s) disallowed to page.
- *Disallow all with exempt*: If you select this option, click *New* to enter the number(s) allowed to page.

For more information on paging, see [“Configuring auto attendants” on page 206](#).

Trusted hosts	Click <i>New</i> to enter the IP address and netmask of the subnet that can register with the SIP server. Only extensions on the specified subnet can register with the SIP server.
Permit outgoing rules	Select the available outbound calling rules in the <i>Available rules</i> field and click -> to move them to the <i>Selected rules</i> field. You can apply the rules to a user later. For more information on calling rules, see “Configuring outbound dial plans” on page 196 .

7. Click *Create*.

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 213](#).

To set an account code

1. Go to *Call Features > User Privileges > Account Code*.
2. Click *New*.
3. Enter a name for the account code.
4. Enter the access code, such as 69.
5. Select *Shared* to use this code on any extension.
6. Enter any notes about this code as required.
7. Click *Create*.

Mapping speed dials

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

For information on setting speed dial number pattern, see [“Configuring PBX options” on page 102](#).

To map speed dials

1. Go to *Call Features > Speed Dials*.
2. Enter a name for the speed dial mapping.
3. For *Code*, enter the number based on the speed dial number pattern you set. For example, 333.
4. Enter the phone *Number* to map to the speed dial code.

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 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.

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

Configuring conference calls

The *Call Features > Conferencing > Conferencing* tab lets you configure and enable conference call settings.

To configure a conference call

1. Go to *Call Features > Conferencing > Conferencing* and click *New*.
2. Configure the following:

Figure 80: Configuring conference calls

Conference

Name:

Number: ☐ Show suggested numbers

Display name:

User PIN:

Admin PIN: (Admin/moderator PIN to start/manage conference)

Enabled: ☒

Description:

Music on hold: ☐

Quiet mode: ☐ (Don't record/announce participate's name)

Recursive Schedules

Enabled: ☐

Schedule

One Time Schedules

Enabled: ☐

Start date	Start time	End date	End time

GUI field	Description
Name	Enter the name for the conference call.
Number	Select an extension number that callers can call and enter the user PIN to join a conference call.
Display name	Enter the name displaying on the conference call extension, such as “HR”.

Show suggested numbers	<p>Select and click in the <i>Number</i> field to display the extension numbers available for use. If it is deselected, clicking in the <i>Number</i> field displays the extension numbers already in use.</p> <p>This option also serves as a diagnostic tool for finding and fixing duplicate or missing numbers. Missing numbers are the extensions that have user IDs but not numbers.</p> <p>When there are duplicate or missing numbers, an orange exclamation mark icon appears beside this option. You can click the icon and fix the numbers. For more information, see “Fixing duplicate or missing numbers” on page 140.</p>
User PIN	<p>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.</p> <p>This password is always valid and should only be sent to the people who need it.</p>
Admin PIN	<p>Enter the PIN number to be entered by the conference host to be able to host a conference call. The default is 123123.</p> <p>This password is always valid and should only be sent to the people who need it.</p>
Enabled	Select to activate this conference call.
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.
Quiet mode	Select to mute the background sound that callers hear after the joining message and leaving message are played.
Recursive Schedules	<p>If you want conference calls on repeating schedules, select <i>Enabled</i> and click <i>New</i> to select a schedule. Enter a password for joining the conference call and click <i>Create</i>.</p> <p>This option is useful if you want to limit the participants to a particular recursive conference call only provided that they do not have the <i>User PIN</i> or <i>Admin PIN</i> for the conference call. They can only join the conference call during the scheduled time period and by entering the password you set.</p> <p>For information on setting up a schedule, see “Scheduling the FortiVoice unit” on page 121.</p>
One Time Schedules	<p>If you want to set up a one time conference call, select <i>Enabled</i> and click <i>New</i> to enter the start and end time. Enter a password for joining the conference call and click <i>Create</i>.</p> <p>This option is useful if you want to limit the participants to a particular one time conference call only provided that they do not have the <i>User PIN</i> or <i>Admin PIN</i> for the conference call. They can only join the conference call during the scheduled time period and by entering the password you set.</p> <p>If the one time schedule conflicts with the recursive schedule, the one time schedule has priority.</p>

3. Click *Create*.

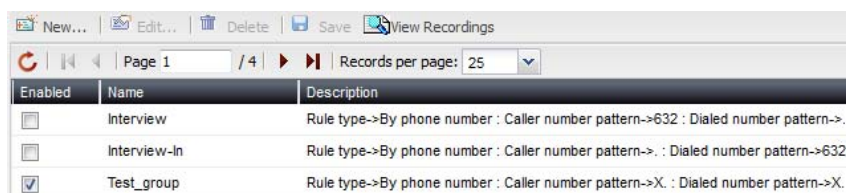
Recording calls

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.

Configuring call recordings

Call Features > Call Recording > Policy allows you to configure call recordings by creating, editing, removing, saving, or viewing a recording.

Figure 81: Call recording list

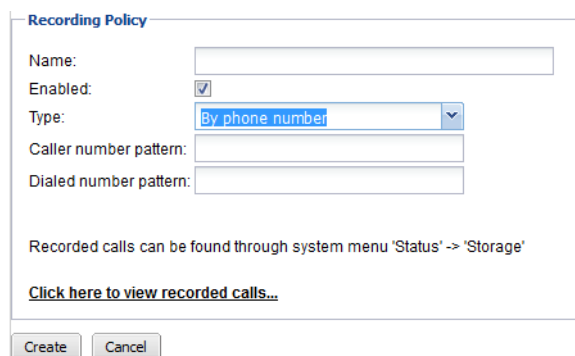


Enabled	Name	Description
<input type="checkbox"/>	Interview	Rule type->By phone number : Caller number pattern->632 : Dialed number pattern->
<input type="checkbox"/>	Interview-In	Rule type->By phone number : Caller number pattern-> : Dialed number pattern->632
<input checked="" type="checkbox"/>	Test_group	Rule type->By phone number : Caller number pattern->X. : Dialed number pattern->X.

GUI field	Description
View Recordings	Click to view, listen, search, or save the recordings. You can also do so by going to <i>Status > Storage > Recorded Calls</i> . For details, see “Playing recorded calls” on page 30 .
Enabled	Select to activate this call recording service.
Name	The name of the call recording service.
Description	Information of call recording configuration.

To configure call recording

1. Go to *Call Features > Call Recording > Policy*.
2. Click *New*.



Recording Policy

Name:

Enabled: ☒

Type:

Caller number pattern:

Dialed number pattern:

Recorded calls can be found through system menu 'Status' -> 'Storage'

[Click here to view recorded calls...](#)

Create Cancel

GUI field	Description
Recording Policy	

Name	Enter a name for this configuration.
Enabled	Select to activate this configuration.
Type	Select the category of calls you want to record: by phone number, department, group, or trunk.

If you select *By phone number* for *Type*, configure the following:

Caller number pattern	<p>Enter the number pattern to match the callers' phone numbers following the pattern:</p> <p><code>^[0-9XNZ]*[^\.]*\$</code> where X=(0-9), Z=(1-9), and N=(2-9).</p> <p>For more information, see “Configuring PBX options” on page 102.</p> <p>The phone calls from the numbers matching the pattern will be recorded.</p>
Dialed number pattern	<p>Enter the number pattern to match the dialed phone numbers following the pattern:</p> <p><code>^[^_][0-9XNZ\.]*\$</code> where X=(0-9), Z=(1-9), and N=(2-9).</p> <p>For more information, see “Configuring PBX options” on page 102.</p> <p>The phone calls to the numbers matching the pattern will be recorded.</p>

If you select *By department* for *Type*, configure the following:

Department	<p>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 160.</p>
-------------------	---

If you select *By group* for *Type*, configure the following:

Group	<p>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 159.</p>
--------------	--

If you select *By trunk* for *Type*, configure the following:

Trunk	<p>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 170.</p>
Direction	<p>Select the direction of which you want to record the calls.</p>

3. Click *Create*.

Setting the recorded file format

Select the format for recording calls.

To set the recorded file format

1. Go to *Call Features > Call Recording > Setting*.
2. Select the format: *Standard* or *Low rate*.
3. Click *Apply*.

Archiving recorded calls

Configure the settings to archive the recorded calls.

To configure the recording archive settings

1. Go to *Call Features > Call Recording > Archive*.

Figure 82: Recording archive settings

Recording Archive Settings

Rotation Settings

The archived recording will rotate when either the file size or rotation time is reached.

Recording rotation size: 500 (MB)

Recording rotation time: 7 (day) At hour: 0

Archiving options when disk quota is full: Overwrite

Destination Settings

Destination: Local

Local disk quota: 100 (GB)

Protocol: SFTP

IP address: 0.0.0.0

User name:

Password:

Remote directory:

Remote cache quota: 5 (GB)

Apply Cancel

2. Configure the following:

GUI field	Description
Rotation Settings	
Recording rotation size/time	Enter the recorded file rotation size and time. When the file reaches either the rotation size or time specified, whichever comes first, the archiving file is automatically renamed. The FortiVoice unit generates a new file, where it continues saving recording archives. You can access all rotated files through search.
Archiving options when disk quota is full	Specify what the FortiVoice unit should do if it runs out of disk space. Select <i>Overwrite</i> to remove the oldest archived folder in order to make space for the new archive, or select <i>Do not archive</i> to stop archiving more recorded calls.
Destination Settings	
Destination	Select an archiving destination: <ul style="list-style-type: none">• <i>Local</i>: the FortiVoice unit's local hard drive or a NAS server.• <i>Remote</i>: a remote FTP or SFTP storage server.

Local disk quota	<p>If <i>Local</i> is the archiving destination, enter the disk space quota.</p> <p>The total disk quota for archiving calls cannot exceed 50% 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 call archiving.</p> <p>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 settings you specify under “Rotation Settings” on page 223.</p>
If <i>Remote</i> 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 <code>/home/fortivoice/call-archives</code> .
Remote cache quota	Enter the FortiVoice cache quota that is allowed to be used for remote host archiving. The above statement regarding the <i>Local disk quota</i> also applied to the cache quota.

3. Click *Apply*.

Creating call queues

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.

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 189.

Call queues consist of:

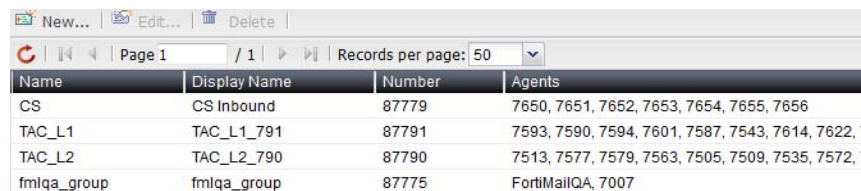
- Incoming calls waiting in the queue
- Agents who answer the calls in the queues
- A plan for how to handle the queue and assign calls to agents
- Music played while waiting in the queue
- Announcements for agents and callers

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 view the call queues, go to *Call Features > Call Queue*.

Figure 83:Call queues



The screenshot shows a web interface for managing call queues. At the top, there are buttons for 'New...', 'Edit...', and 'Delete'. Below these is a navigation bar with 'Page 1' and 'Records per page: 50'. The main content is a table with four columns: Name, Display Name, Number, and Agents. The table contains four rows of data.

Name	Display Name	Number	Agents
CS	CS Inbound	87779	7650, 7651, 7652, 7653, 7654, 7655, 7656
TAC_L1	TAC_L1_791	87791	7593, 7590, 7594, 7601, 7587, 7543, 7614, 7622
TAC_L2	TAC_L2_790	87790	7513, 7577, 7579, 7563, 7505, 7509, 7535, 7572
fmlqa_group	fmlqa_group	87775	FortiMailQA, 7007

GUI field	Description
Name	The name of the call queue.
Display Name	The queue name displaying on the queue extension.
Number	The extension number for the call queue.
Agents	The extensions of the agents enrolled in the queue.

To create a call queue

1. Go to *Call Features > Call Queue*.
2. Click *New*.
3. Configure the following:

Figure 84:Creating a call queue

Queue

Name:

Number:

☐ Show suggested numbers

Display name:

Caller ID option:

No change

Description:

Status

☒

Queue Setting

Music:

Maximum waiting caller:

20

Maximum waiting time:

30

(Minutes)

Non member agent login:

☐

Distribution:

Round robin

Ring duration:

20

(Seconds)

Business schedule

>>

Announcement Setting

Announce to agent

Queue name:

--None--

New...

Edit...

Announce to caller

Interval:

180

(Seconds)

Holdtime:

☒ No ☐ Yes ☐ Once

Position:

No

Mark position:

20

☐ Custom announcement to caller

Agent

[Configure Agents...]

Create

Cancel

GUI field	Description
Queue	
Name	Enter a name for the queue.

Number	<p>Enter an extension for callers to dial and enter into a call queue following the extension number pattern. See “Configuring PBX options” on page 102.</p> <p>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.</p> <p>Even if you enter an extension, you can still add the call queue configuration 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.</p>
Show suggested numbers	<p>Select and click in the <i>Number</i> field to display the extension numbers available for use. If it is deselected, clicking in the <i>Number</i> field displays the extension numbers already in use.</p> <p>This option also serves as a diagnostic tool for finding and fixing duplicate or missing numbers. Missing numbers are the extensions that have user IDs but not numbers.</p> <p>When there are duplicate or missing numbers, an orange exclamation mark icon appears beside this option. You can click the icon and fix the numbers. For more information, see “Fixing duplicate or missing numbers” on page 140.</p>
Display name	Enter the queue name displaying on the queue extension, such as Support.
Caller ID option	<p>Select how you want to display the ID of a caller to the queue.</p> <ul style="list-style-type: none"> • <i>No change</i>: the caller ID will display as is. • <i>Replace</i>: the caller ID will be replaced by the <i>Display name</i> you set. • <i>Prefix</i>: the caller ID will be prefixed with the <i>Display name</i> you set.
Description	Enter any notes about this queue.
Queue Setting	
Music	Select a sound file or music on hold file to play when a caller is waiting. For more information, see “Managing sound files and music on hold” on page 116 .
Maximum waiting caller	<p>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 call handling action you set after the call queue action (<i>Action</i>) for this call queue configuration (<i>Target</i>) in your default inbound dial plan. If there is no action after the call queue action (<i>Action</i>) for this call queue configuration (<i>Target</i>) in your default inbound dial plan, the call will hang up. For more information, see “Configuring inbound dial plans” on page 189.</p> <p>The maximum is 100.</p>

Maximum waiting time	<p>Enter the maximum call queue waiting time in minutes. When the call waiting time is due, the callers in the queue will be dealt with according to the call handling action you set after the call queue action (<i>Action</i>) for this call queue configuration (<i>Target</i>) in your default inbound dial plan. If there is no action after the call queue action (<i>Action</i>) for this call queue configuration (<i>Target</i>) in your default inbound dial plan, the call will hang up. For more information, see “Configuring inbound dial plans” on page 189.</p> <p>The maximum is 720 minutes.</p>
Non member agent login	<p>Select to allow non-enrolled agents to log into this queue. Non-enrolled agents are those that are not included in this queue when you configure the queue agents. For more information, see “Configure Agents” on page 229.</p>
Distribution	<p>Select the method for calls in the queue to be delivered to the agents.</p>
Ring duration	<p>Enter the time in seconds to ring each agent. If a call is not answered when the ring duration is due, the call is transferred to the next agent. The range is between 5 to 120 seconds.</p>
Business schedule	<p>Select a 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.</p>
Announcement Setting	
Announce to agent	<p>Select a sound file to announce this call queue configuration name to the agent so that the agent knows that this is the right call for his/her agent group.</p> <p>For example, a caller calls company ABC and presses 3 for technical support. The call is routed to this call queue named Tech Support. When the call is picked up, the agent will hear an announcement such as “This call is for the technical support department”.</p> <p>You can edit a selected sound file or create a new one. For more information on sound files, see “Managing sound files and music on hold” on page 116.</p>
Announce to caller	<p>Set the basic announcement settings to callers.</p> <p><i>Interval:</i> Enter the time in seconds for the interval of announcement hold time and position. The default is 180 and the range is between 60-1800.</p> <p><i>Holdtime:</i> Select <i>No</i> to cancel announcement, <i>Yes</i> to announce according to the time interval you set, and <i>Once</i> to announce only once during a call.</p>

	<p>Position: Select to announce a caller's waiting position in the queue, such as "You are caller No. 5 in the call queue".</p> <ul style="list-style-type: none"> • <i>No</i>: Caller position in the queue is not announced. • <i>Always</i>: Always announce caller position in the queue. • <i>Abbreviated</i>: The caller's position is only announced once if caller is over the <i>Mark position</i> and always announced when caller is within the <i>Mark position</i>. For example, if you set 5 for <i>Mark position</i>, and if the caller is number 8 in the queue, the caller's position is only announced once before he/she becomes number 5. After that, the caller's position is announced according to time <i>Interval</i> you set. • <i>Minimal</i>: The caller's position is only announced according to time <i>Interval</i> you set if caller is within the <i>Mark position</i>. • <i>Mark position</i>: If you select <i>Abbreviated</i> or <i>Minimal</i> for <i>Position</i>, enter the value to mark the queue position.
Custom announcement to caller	<p>Select the method of greeting announcement to the caller and a sound file for the announcement/greeting.</p> <p><i>Mode</i>:</p> <ul style="list-style-type: none"> • <i>Disable</i>: No greeting announcement to the caller. • <i>Periodic</i>: The greeting is announced periodically at the interval you set. If you select this option, also configure <i>Interval</i> and <i>Audio</i>. • <i>Random</i>: The greeting is announced periodically at the interval set by the system. Also configure <i>Audio</i>, although the order of the sound files you set will be randomly arranged by the system. • <i>Interval</i>: Enter the time in seconds for the interval of greeting announcement. The default is 120 and the range is between 60-3600. • <i>Audio</i>: If you select <i>Periodic</i> or <i>Random</i> announcement method, select a sound file for the announcement/greeting. You can edit a selected sound file or create a new one. For more information on sound files, see "Managing sound files and music on hold" on page 116.
Agent	
Configure Agents	<p>Click to enroll agents into the queue.</p> <ul style="list-style-type: none"> • Click <i>Configure Agents</i>. • Click <i>New</i>. • In the <i>Name</i> field, select the agents for this queue. • Click <i>Create</i>. • Click <i>OK</i>.

4. Click *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, 301–320.

To view the parked calls, see [“Viewing parked calls” on page 25](#).

To configure call parking

1. Go to *Call Features > Call Parking > Call Parking*.
2. For *Park call number*, enter the number to dial to park a call. The default is 300.
For example, if you enter 300, depending on the phone, when a user receives a call and wants to park it, the user may:
 - Press *1300.
The FortiVoice unit selects the first available park orbit (301–320). The user hears a confirmation indicating the caller has been parked successfully and into which park orbit.
By default, dialing *1 and then 300 parks a call.
 - Provide the park orbit to the person with the parked call through paging or other means (e.g. “Mary, there is a call parked for you in 301”. Mary can then pick up any phone and dial 301 to retrieve the parked call.).
3. For *Park line start*, enter the starting park orbit. The default is 301.
4. For *Park line end*, enter the ending park orbit. The default is 320.
5. For *Parking time out*, enter the time, in seconds, to time out the parked call. The default is 60 seconds.
6. For *Music on hold*, select the music on hold file to play while the call is place on hold. Click *Edit* to modify the selected file or click *New* to configure a new one. For more information on music on hold, see [“Managing sound files and music on hold” on page 116](#).
7. Click *Apply*.

Configuring fax

The FortiVoice unit supports fax in the following ways:

- Use the FortiVoice unit to send and receive faxes. The FortiVoice unit contains a full featured fax server that is able to receive faxes and forward them in PDF format to an extension’s user web portal or a user’s email. End users can log into their web portal to view the faxes and upload PDF or JPEG files to send faxes. For configuration information, see [“Receiving Faxes” on page 231](#) and [“Sending faxes” on page 232](#).
- If you want to continue using your fax machine with the VoIP phone system, connect the fax machine to an adapter (such as OBIHAI OBi 200, Cisco SPA 112, or Grandstream HT 702) that supports T.38 first before connecting to the FortiVoice unit. T.38 is a protocol designed to allow fax to travel over a VoIP network.

In this case, the fax machine is treated like an extension. The FortiVoice unit receives faxes and relays them to the fax machine. Faxes sent from the fax machine will follow the fax sending dial plans.

To use this option, you need to create and enable the fax extensions first. You then need to configure the FortiVoice unit to receive and relay the faxes to the fax machine. See [“Configuring fax extensions” on page 148](#), [“Receiving Faxes” on page 231](#) and [“Sending faxes” on page 232](#).

- With FortiVoice 200D-T, if you want to use your existing analog phone line, connect the fax machine directly to the FXS port. Make sure that the fax function is enabled when

configuring the analog extension. See [“Modifying analog extension \(200D-T model only\)”](#) on page 142.

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 Features > Fax > eFax Account* and click *New*.
- 2. Configure the following:

Table 28: Fax receiving configuration

Name:

Number:

Show suggested numbers

Display name:

Enabled:

☒

External Numbers

New...

Edit...

Delete

Enabled

Incoming trunk

DID numbers

Select Fax Monitors

Fax to Email

Relay to Fax Machine

Archive

Description:

Create

Cancel

GUI field	Description
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.
Show suggested numbers	<p>Select and click in the <i>Number</i> field to display the extension numbers available for use. If it is deselected, clicking in the <i>Number</i> field displays the extension numbers already in use.</p> <p>This option also serves as a diagnostic tool for finding and fixing duplicate or missing numbers. Missing numbers are the extensions that have user IDs but not numbers.</p> <p>When there are duplicate or missing numbers, an orange exclamation mark icon appears beside this option. You can click the icon and fix the numbers. For more information, see “Fixing duplicate or missing numbers” on page 140.</p>

Enabled	Select to activate this fax.
External Numbers	<p>Map the DID numbers to the extension of the fax. Incoming faxes to the DIDs will all reach the extension. For information on DID, see “Mapping DIDs” on page 194.</p> <p>To map the DID numbers:</p> <ul style="list-style-type: none"> • Click <i>New</i>. • Select <i>Enabled</i> to activate this DID mapping. • Select the trunk used for dialing the DIDs. • Enter the DID number that you want to map to an extension. • Click <i>Create</i>.
Select Fax Monitors	<p>Select the users that can monitor the faxes received on this fax extension in their FortiVoice user web portal and can choose to view, delete, resend, forward, or download the faxes. For more information, see the online help of the web user portal.</p> <p>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 152.</p> <p>This is useful if you have a fax that serves several departments.</p>
Fax to Email	Enter the email addresses to receive the faxes sent to this extension. Users will receive the faxes in PDF format.
Relay to Fax Machine	Select the fax machines connected to the FortiVoice unit via T.38 adapters. Faxes will be relayed to the selected machines.
Archive	<p>Select <i>Fax archive</i> to activate fax archiving. Enter the maximum number of faxes to archive and the maximum number of days to keep them.</p> <p>To view faxes sent and received through the FortiVoice unit, see “Viewing archived faxes” on page 30.</p>
Description	Optionally, you can enter some notes about this configuration.

3. Click *Create*.

Sending faxes

Configure the dial plans for sending faxes. The dialed fax numbers matching the configured number pattern will be subject to the call handling actions.

The fax sending dial plans will not interfere with phone call dial plans since the FortiVoice unit deals with the dial plans separately.

For information on dial plans, see [“Configuring Call Routing” on page 189](#).

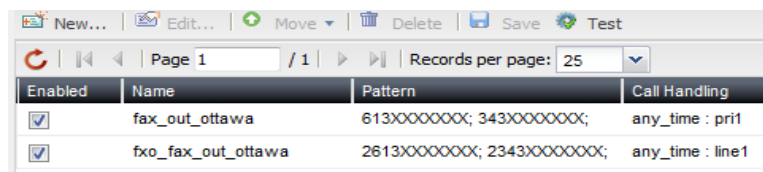
You send faxes in the user web portal. Senders will receive email notifications when a fax is sent if their extensions are linked with email addresses. The notification will inform if the fax has been successfully sent and have a PDF attachment of the fax if their extensions are configured with

email notification attachment option. For more information, see [“Setting extension user preferences” on page 152](#).

In addition, senders can always view the status of the fax sent in their FortiVoice user web portal. For more information, see the online help of the web user portal.

To view the outbound dial plans, go to *Call Features > Fax > Sending Rule*.

Figure 85: Viewing dial plans for sending faxes



Enabled	Name	Pattern	Call Handling
<input checked="" type="checkbox"/>	fax_out_ottawa	613XXXXXXXX; 343XXXXXXXX;	any_time : pri1
<input checked="" type="checkbox"/>	fxo_fax_out_ottawa	2613XXXXXXXX; 2343XXXXXXXX;	any_time : line1

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 234 .
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 234 .
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 234 .

To set up a fax sending dial plan

1. Go to *Call Features > Fax > Sending Rule*.
2. Click *New*.
3. Configure the following:

Figure 86: Dial plan for sending faxes

Name:

Enabled: ☒

Dialed Number Match

New... Edit... Delete | Match... Strip Prefix Postfix

Call Handling

New... Edit... Move Delete | Schedule Trunk Caller... Warning Message Account Code

Create Cancel

GUI field	Description
Name	Enter a name for this plan.
Enabled	Select to activate this dial plan.
Dialed Number Match	<p>With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers.</p> <p>The dialed numbers matching this pattern will follow this dial plan rule.</p> <p>For information on adding a dialed number match, see “Creating dialed number match” on page 235.</p>
Call Handling	Click <i>New</i> to configure the call handling action for the numbers matching the configured number pattern. For details, see “Configuring call handling actions” on page 237 .

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 233](#).

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*.
The call test page appears.
3. Configure the following:

Figure 87: Testing dial plans

System Configuration Test

Test Call - Dry Run

Test Call

Destination number:

From number:

Test result:

Test

Reset

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 <i>Test result</i> .
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: <ul style="list-style-type: none"><i>Play welcome message</i>: The FortiVoice unit will play a message to the destination number.<i>Connect test call to number</i>: In the <i>Number</i> 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 <i>Test result</i> .
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:

Table 29:Pattern-matching syntax

Syntax	Description
X	Matches any single digit from 0 to 9.
Z	Matches any single digit from 1 to 9.
N	Matches any single digit from 2 to 9.
[15-7]	Matches a single character from the range of digits specified. In this case, the pattern matches a single 1, as well as any number in the range 5, 6, 7.
.	Wildcard match; matches one or more characters, no matter what they are.
!	Wildcard match; matches zero or more characters, no matter what they are.

Table 30:Pattern-matching examples

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

To create a dialed number match

1. Go to *Call Features > Fax > Sending Rule*.
2. Click *New*.
3. In *Dialed Number Match*, click *New*.
4. Configure the following:

Figure 88: Creating a number match

GUI field

Description

Match Pattern

New	Click to add the number pattern in the <i>Value</i> field following “ Pattern-matching syntax ” on page 236 and “ Pattern-matching examples ” on page 236 for this dial plan. Repeat 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 <i>Match Pattern</i> is 9XXX and <i>Strip</i> 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 <i>Match Pattern</i> is 123XXXX and its area code is 555, you can enter 555 for the <i>Prefix</i> . 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 <i>Match Pattern</i> 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 <i>Postfix</i> . 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 Features > Fax > Sending Rule*.
2. Click *New*.
3. In *Call Handling*, click *New*.
4. Configure the following:

GUI field	Description
Call Handling Action	
Schedule	Select the FortiVoice operation schedule to implement this plan. Click <i>Edit</i> to modify the selected schedule or click <i>New</i> to configure a new one. For more information on PBX schedule, see “ Scheduling the FortiVoice unit ” on page 121.
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 <i>Edit</i> to modify the selected trunk or click <i>New</i> to configure a new one. For more information on trunks, see “ Configuring Trunks ” on page 170.

Caller ID modification	Select the caller ID modification configuration. Click <i>Edit</i> to modify the selected configuration or click <i>New</i> to configure a new one. For more information on caller ID modification, see “Modifying caller IDs” on page 120 .
Warning message	If you select <i>Allow with warning</i> or <i>Deny with warning</i> in the <i>Action</i> field, select the sound file for the warning. Click <i>Edit</i> to modify the selected file or click <i>New</i> to configure a new one. For more information on sound files, see “Managing sound files and music on hold” on page 116 .
Delay	Optionally, if you want to discourage certain users for sending faxes, enter the call delay time in seconds.

5. Click *Create*.

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 Features > Fax > Setting*.
2. Configure the following:

Figure 89: Fax settings

GUI field	Description
System station ID	Enter a station ID that shows on each fax sent from the FortiVoice unit.
System fax header	Enter a fax subject header that shows on each fax sent from the FortiVoice unit.
T.38 Fax	

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.
Fallback to audio (G.711) mode on T.38 failure	Select to use G.711 mode if T.38 communication fails.
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 <i>Max retry times</i> configuration.

3. Click *Apply*.

Archiving faxes

Configure the settings to archive the faxes.

To configure archiving faxes

1. Go to *Call Features > Fax > Archive*.

Figure 90: Recording archive settings

Fax Archive Settings

Rotation Settings

The archived Fax will rotate when either the file size or rotation time is reached.

Fax rotation size: 10 (MB)

Fax rotation time: 1 (day) At hour: 1

Archiving options when disk quota is full: Overwrite

Destination Settings

Destination: Remote

Local disk quota: 4 (GB)

Protocol: FTP

IP address: 172.20.140.117

User name: chenxhao

Password:

Remote directory: fvc-archive

Remote cache quota: 2 (GB)

Apply Cancel

2. Configure the following:

GUI field	Description
Rotation Settings	

Fax rotation size/time	<p>Enter the archived fax file rotation size and time.</p> <p>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.</p>
Archiving options when disk quota is full	<p>Specify what the FortiVoice unit should do if it runs out of disk space. Select <i>Overwrite</i> to remove the oldest archived folder in order to make space for the new archive, or select <i>Do not archive</i> to stop archiving more recorded calls.</p>
Destination Settings	
Destination	<p>Select an archiving destination:</p> <ul style="list-style-type: none"> • <i>Local</i>: the FortiVoice unit's local hard drive or a NAS server. • <i>Remote</i>: a remote FTP or SFTP storage server.
Local disk quota	<p>If <i>Local</i> is the archiving destination, enter the disk space quota.</p> <p>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.</p> <p>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 settings you specify under "Rotation Settings" on page 223.</p>
If <i>Remote</i> 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 <code>/home/fortivoice/call-archives</code> .
Remote cache quota	Enter the FortiVoice cache quota that is allowed to be used for remote host archiving. The above statement regarding the <i>Local disk quota</i> also applied to the cache quota.

3. Click *Apply*.

Modifying feature access codes

By default, the FortiVoice unit defines the following codes for users to access certain features by dialing the codes. You can go to *Call Features > 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 example, if you change the DISA code from the default ** to 12, dialing 12 still accesses the DISA feature.

Table 31: Feature access codes

GUI field	Description
Call bridge (DISA)	<p>Direct Inward System Access (DISA) service allows external users to dial into PBX and use PBX service just like the local extensions.</p> <p>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 <i>PBX > Class of Service > Account code</i>). Once you pass authorization, you can use PBX service just like a local extension.</p>
Blind transfer	<p>Blind transfer serves 2 purposes:</p> <ul style="list-style-type: none">• During a call, dial *1 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 *1 and then the call parking number (default is 300) to park a call. For details, see “Configuring call parking” on page 230.
Check hot desk login status	<p>Hot-desking refers to the sharing of one phone by multiple users at different time periods.</p> <p>Dial *10 or the code you set to check hot desk login status including login expiry time.</p>
Hot desk user login	<p>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.</p>
Hot desk user logout	<p>To log out hot desking, press *12 or the code you set.</p>
Reset phone to be 'unassigned' by admin	<p>This code is used to remove the extension number of a FortiFone by the administrator.</p> <p>Dial *15 or the code you set on any FortiFone that connects to the FortiVoice unit and enter the phone configuration PIN.</p> <p>For information on setting the phone configuration PIN, see “Configuring SIP phone auto-provisioning” on page 111.</p>
Reset phone to be 'unassigned' by user	<p>This code is used to remove the extension number of a FortiFone by the user.</p> <p>Dial *16 or the code you set on your FortiFone that connects to the FortiVoice unit and enter the phone configuration PIN.</p> <p>For information on setting the phone configuration PIN, see “Configuring SIP phone auto-provisioning” on page 111.</p>

Table 31: Feature access codes

GUI field	Description
Configure phone to extension by administrator	<p>This code is used to set an extension number for a FortiFone by the administrator.</p> <p>Dial *17 or the code you set on any FortiFone that connects to the FortiVoice unit and enter the phone configuration PIN. You can then enter an existing extension to set it as the extension of this phone.</p> <p>For information on setting the phone configuration PIN, see “Configuring SIP phone auto-provisioning” on page 111.</p>
Configure phone to extension by user	<p>This code is used to set an extension number for a FortiFone by a phone user.</p> <p>Dial *18 or the code you set on your FortiFone that connects to the FortiVoice unit and enter the phone configuration PIN provided by the administrator. You can then enter an existing extension to set it as the extension of this phone.</p>
Attended transfer	<p>During a call, dial *2 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.</p>
Personal recording	<p>Dial *3 or the code you set to record a phone conversation.</p> <p>Before doing so, have the agreement of the person you talk with or check your local laws regarding phone recording.</p>
Park	<p>Dial *4 or the code you set to park a call.</p>
Lookup name directory from extension	<p>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.</p>
Barge	<p>Dial *5 or the code you set to monitor a call by listening to it. You also need to enter your voicemail PIN. For details, see “Monitor/Recording” on page 216</p>
Hotel room cleaning status	<p>Dial *75 or the code you set and enter a maid code to show the room cleaning status.</p> <p>For information on maid codes, see “Configuring hotel management settings” on page 203.</p>
Wake-up call	<p>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.</p>
DND on	<p>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.</p>
DND off	<p>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.</p>

Table 31: Feature access codes

GUI field	Description
Pickup any ringing extension in pickup group	As a pickup group member, you can dial *80 or the code you set on your phone to pick up a call from any ringing extension. For information on pickup groups, see “Creating pickup groups” on page 164 .
Pickup group extension	As a pickup group member, you can dial *81 or the code you set on your phone followed by a ringing extension number to pick up a call from that extension. For information on pickup groups, see “Creating pickup groups” on page 164 .
Intercom	Dial *92 or the code you set and an extension to intercom that extension.
Voicemail direct	Dial *97 or the code you set from your own phone and then enter your voicemail password to directly access your voice mailbox.
Voicemail prompt	Dial *98 or the code you set from any extension and then enter your extension number and voicemail password to access your voice mailbox.
Operator	Dial 0 or the code you set to access the operator.
One key DND	This is for supporting the DND key on the FortiFones. Press the DND key on the FortiFone to turn DND on or off.
Unpark	This is for supporting the Unpark key on the FortiFones. Press this key on the FortiFone to unpark a call.

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](#)
- [Configuring logging](#)
- [Configuring report profiles and generating call reports](#)
- [Configuring Station Messaging Detail Record \(SMDR\)](#)
- [Configuring alert email](#)

About FortiVoice logging

FortiVoice units can log:

- system-related events, such as configuration changes and administrator login/logout
- phone call events

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 245](#).

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 246](#). It can also use log messages as the basis for reports. For more information, see [“Configuring report profiles and generating call reports” on page 250](#).

This topic includes:

- [FortiVoice log types](#)
- [Log message severity levels](#)

FortiVoice log types

FortiVoice units can record the following types of log messages. The Event log also contains several subtypes. You can view and download these logs from the *Logs* submenu of the *Status* tab.

Table 32: Log types

Log type	Subtype	Description
Event	config admin system smtp ha dhcp voicemail monitor	Includes system and administration events, such as downloading a backup copy of the configuration.
Voice		Includes phone calls 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.



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.

Table 33: 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 Settings* submenu includes two tabs, *Local Log Settings* and *Remote Log Settings*, that let you:

- set the severity level
- configure which types of log messages to record
- specify where to store the logs

You can configure the FortiVoice unit to store log messages locally (that is, in RAM or to the hard disk), remotely (that is, on a Syslog server or FortiAnalyzer unit), or at both locations.

Your choice of storage location may be affected by several factors, including the following:

- Local logging by itself may not satisfy your requirements for off-site log storage.
- Very frequent logging may cause undue wear when stored on the local hard drive. A low severity threshold is one possible cause of frequent logging. For more information on severity levels, see “[Log message severity levels](#)” on page 245.

For information on viewing locally stored log messages, see “[Viewing log messages](#)” on page 32.

This section includes the following topics:

- [Configuring logging to the hard disk](#)
- [Choosing which events to log](#)
- [Configuring logging to a Syslog server or FortiAnalyzer unit](#)

Configuring logging to the hard disk

You can store log messages locally on the hard disk of the FortiVoice unit.

To ensure that the local hard disk has sufficient disk space to store new log messages and that it does not overwrite existing logs, you should regularly download backup copies of the oldest log files to your management computer or other storage, and then delete them from the FortiVoice unit. (Alternatively, you could configure logging to a remote host.)

You can view and download these logs from the *Log* submenu of the *Monitor* tab. For more information, see “[Viewing log messages](#)” on page 32.

For logging accuracy, you should also verify that the FortiVoice unit’s system time is accurate. For details, see “[Configuring the time and date](#)” on page 74.

To configure logging to the local hard disk

1. Go to *Log & Report > Log Settings > Local Log Settings*.
2. Select the *Enable* option to allow logging to the local hard disk.

3. In *Log file size*, enter the file size limit of the current log file in megabytes (MB). The log file size limit must be between 10 MB and 1000 MB.
4. In *Log time*, enter the time (in days) of file age limit.
5. In *At hour*, enter the hour of the day (24-hour format) when the file rotation should start.

When a log file reaches either the age or size limit, the FortiVoice unit rotates the current log file: that is, it renames the current log file (elog.log) with a file name indicating its sequential relationship to other log files of that type (elog2.log, and so on), then creates a new current log file. For example, if you set the log time to 10 days at hour 23, the log file will be rotated at 23 o'clock of the 10th day.



Large log files may decrease display and search performance.

6. From *Log level*, select the severity level that a log message must equal or exceed in order to be recorded to this storage location.
7. From *Log options when disk is full*, select what the FortiVoice unit will do when the local disk is full and a new log message is caused, either:
 - *Do not log*: Discard all new log messages.
 - *Overwrite*: Delete the oldest log file in order to free disk space, and store the new log message.
8. In *Logging Policy Configuration*, click the arrow to review the options and enable the types of logs that you want to record to this storage location. For details, see [“Choosing which events to log” on page 247](#).
9. Click *Apply*.

Choosing which events to log

Both the local and remote server configuration recognize the following events. Select the check boxes of the events you want to log.

Table 34:Events logging options

Event Log	Select this check box and then select specific events. No event types are logged unless you enable this option. <ul style="list-style-type: none">• <i>When configuration has changed:</i> Log configuration changes.• <i>Admin login/logout event:</i> Log all administrative events, such as logins, resets, and configuration updates.• <i>System activity event:</i> Log all system-related events, such as rebooting the FortiVoice unit.• <i>SMTP server event:</i> Log SMTP relay or proxy events. This option is for local log setting only.• <i>HA:</i> Log all high availability (HA) activity.• <i>DHCP event:</i> Log DHCP server events. This option is for local log setting only.• <i>Voice mail event:</i> Log voicemail events. This option is for remote log setting only.• <i>Monitor:</i> Log call recording, call barging, and traffic capture events.
Voice Log	Log phone call events. This option is for local log setting only.
Fax Log	Log fax events.
DTMF Log	DTMF (Dual Tone Multi-Frequency) events.
Hotel Log	Log hotel management events, such as guest check-in and check-out.

Configuring logging to a Syslog server or FortiAnalyzer unit

Instead of or in addition to logging locally, you can store log messages remotely on a Syslog server or a FortiAnalyzer unit.

You can add a maximum of three remote Syslog servers.



Logs stored remotely cannot be viewed from the web-based manager of the FortiVoice unit. If you require the ability to view logs from the web-based manager, also enable local storage. For details, see [“Configuring logging to the hard disk” on page 246](#).

Before you can log to a remote location, you must first enable logging. For details, see [“Choosing which events to log” on page 247](#). For logging accuracy, you should also verify that the FortiVoice unit’s system time is accurate. For details, see [“Configuring the time and date” on page 74](#).

To configure logging to a Syslog server or FortiAnalyzer unit

1. Go to *Log & Report > Log Settings > Remote Log Settings*.

GUI field	Description
Enabled	Select to enable remote storage on the server. Clear to disable storage.

Profile Name	Displays the remote host name.
Server	Displays the IP of the Syslog server or FortiAnalyzer unit.
Port	Displays the port on the Syslog server or FortiAnalyzer unit.
Level	Displays the minimum severity level for logging purposes.
Facility	Displays the facility identifier the FortiVoice unit uses to identify itself.

2. Click *New* to create a new entry or double-click an existing entry to modify it.
A dialog appears.

Figure 91: Remote host configuration dialog

GUI field	Description
Log to Remote Host	
Enable	Select to allow logging to a remote host.
Name	Enter a name for the remote host.
IP	Enter the IP address of the Syslog server or FortiAnalyzer unit where the FortiVoice unit will store the logs.
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 245 .
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).

Facility	<p>Select the facility identifier that the FortiVoice unit will use to identify itself when sending log messages.</p> <p>To easily identify log messages from the FortiVoice unit when they are stored on a remote logging server, enter a unique facility identifier, and verify that no other network devices use the same facility identifier.</p>
CSV format	<p>Enable this option if you want to send log messages in comma-separated value (CSV) format.</p> <p>Do not enable this option if the remote host is a FortiAnalyzer unit. FortiAnalyzer units do not support CSV-formatted log messages.</p>
Logging Policy Configuration	<p>Click the arrow to review the options and enable the types of logs you want to record to this storage location. For details, see “Choosing which events to log” on page 247.</p>

3. Click *Create*.
4. If the remote host is a FortiAnalyzer unit, confirm with the FortiAnalyzer administrator that the FortiVoice unit was added to the FortiAnalyzer unit's device list, allocated sufficient disk space quota, and assigned permission to transmit logs to the FortiAnalyzer unit. For details, see the [FortiAnalyzer Administration Guide](#).
5. To verify logging connectivity, from the FortiVoice unit, trigger a log message that matches the types and severity levels that you have chosen to store on the remote host. Then, on the remote host, confirm that it has received that log message.

For example, if you have chosen to record event log messages to the remote host and if they are more severe than *Information*, you could log in to the web-based manager or download a backup copy of the FortiVoice unit's configuration file in order to trigger an event log message.

If the remote host does not receive the log messages, verify the FortiVoice unit's network interfaces (see [“Configuring the network interfaces” on page 40](#) and [“About the management IP” on page 39](#)) and static routes (see [“Configuring static routes” on page 45](#)), 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. For details, see the [FortiVoice CLI Reference](#).

Configuring report profiles and generating call reports

The *Log & Report > Call Report > Call Report* tab displays a list of 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 log data. The FortiVoice unit presents the information in tabular and graphical format.

You can create one report profile for each type of report that you will generate on demand or on a schedule.

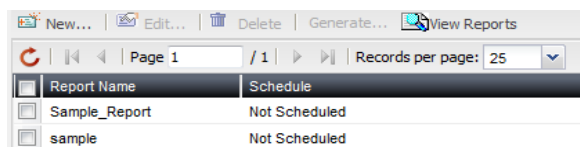


Generating reports can be resource intensive. To avoid phone processing performance impacts, you may want to generate reports during times with low traffic volume, such as at night. For more information on scheduling the generation of reports, see [“Configuring report email notifications” on page 254](#).

To view and configure report profiles

1. Go to *Log & Report > Call Report > Call Report*.

Figure 92: Configuration tab



<i>GUI field</i>	<i>Description</i>
Generate	Select a report and click this button to generate a report immediately. See “Generating a report manually” on page 255 .
View Reports	Click to display the list of reports generated by the FortiVoice unit. You can delete, view, and/or download generated reports. For more information, see “Viewing generated reports” on page 31 .
Report Name	Displays the name of the report profiles.
Schedule	Displays the frequency with which the FortiVoice unit generates a scheduled report. If the report is designed for manual generation, <i>Not Scheduled</i> appears in this column.

2. Click *New* to add a profile or double-click a profile to modify it.
A multisection dialog appears.

Figure 93: New report configuration

3. In *Name*, enter a name for the report profile.
Report names cannot include spaces.
4. Click the arrow next to each option, and configure the following as needed:
 - [Configuring the report query selection](#)
 - [Configuring the report time period](#)
 - [Configuring report email notifications](#)
 - [Configuring the report schedule](#)
 - [Choosing call rate](#)
 - [Generating a report manually](#)
5. Click *Create*.

Configuring the report query selection

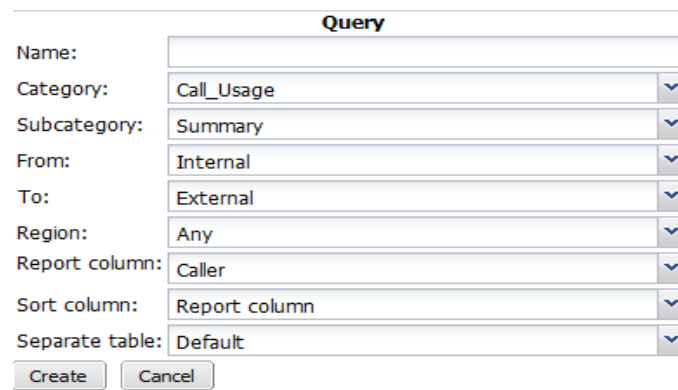
When configuring a report profile, you can select the queries that define the subject matter of the report.

Each report profile corresponds to a chart that will appear in the generated report.

To configure the report query selection

1. Go to *Log & Report > Call Report > Call Report*.
2. Click *New*.
3. Expand *Query List* and click *New*.
4. Configure the following:

Figure 94: Query selection



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. <ul style="list-style-type: none">• <i>Call Usage</i>: The number of calls.• <i>Phone Bill</i>: The cost of making the phone calls.• <i>Trunk Usage</i>: The status of the trunks being used.
Subcategory	Select to have a summary or detailed report on the report category you select.
From	Select to include the source of the incoming calls: <i>Internal</i> , <i>External</i> , or <i>Any</i> .
To	Select to include the source of the outgoing calls: <i>Internal</i> , <i>External</i> , or <i>Any</i> .
Region	Select the call region, such as international or long-distance.
Report column	Select the source of the call statistics: from caller or receiver. For details, see Figure 95 on page 253 .

Sort column	<p>Select the value for filtering the call information. The caller or receiver with the higher value moves to the top of the table.</p> <p>If you select <i>Report column</i>, the sort column value is equal to what you select in the <i>Report column</i> field.</p> <p>For details, see Figure 95 on page 253.</p>
Separate table	<p>Depending on the query values, if a report table is too long, it can be divided into separate tables. Selecting <i>Default</i> keeps the pre-defined table settings of the query values and is recommended.</p> <p>You can select to enable or disable the pre-defined table settings of the query values, although this is not recommended.</p>

5. Click *Create*.

Figure 95: Sample report with *Report column* as *Caller* and *Sort column* as *Duration*

Report column

Sort column

Detailed Calls_by_Duration

Call Usage Detailed [Internal/External, Any Region, by Caller, Sort: Duration]						
Caller	Date	Time	Receiver	Trunk	Duration	Cost(\$)
"80@61" <80>	2012-11-26 / Mon	16:02	6136978752	freephoneline	00:00:10	0.00
	2012-11-27 / Tue	11:16	6136978752	freephoneline	00:00:13	0.00
	Total				00:00:23	0.00
"6819" <6819>	2012-11-26 / Mon	16:14	7817	fvc60	00:00:02	0.00
	2012-11-27 / Tue	10:23	7817	fvc60	00:00:02	0.00
	Total				00:00:04	0.00
Total					00:00:27	0.00

Call duration of caller 80@61 <80>

Call duration of caller 6819 <6819>

Note: Since the sort column is *Duration* and the call time of caller 80@61 <80> is longer, this caller is placed before caller 6819 <6819>.

Configuring the report time period

When configuring a 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 *Log & Report > Call Report > Call Report*.
2. Expand *Period*.
3. Select the time span option you want. This sets the range of log data to include in the report.
 - For *Type*, choose a relative time, such as *Today*, *Yesterday*, *Last N hours*, and so on. If you select an option with an unspecified "N" value, enter the number of hours, days or weeks in the *Value* field, as applicable.
 - Set a specific time range. Set the start date and hour in *From* field and end date and hour in *To* field.

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 email history report and notification email templates” on page 105](#).

To configure an email notification

1. Go to *Log & Report > Call Report > Call Report*.
2. Expand *Email*.
3. Enter the email address of the person who will receive the report notification in the *Mail to* field. Click + to enter more email addresses if necessary, or click - to remove an address.
4. In the *Format* field, select the format of the generated attachment, either *Html* or *Pdf*.

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 255](#).

To configure the report schedule

1. Go to *Log & Report > Call Report > Call Report*.
2. Expand *Schedule*.
3. Configure the following:

<i>GUI field</i>	<i>Description</i>
Type	<ul style="list-style-type: none">• <i>None</i>: 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 255.• <i>Daily</i>: Select to generate the report each day. Also configure <i>Hour</i>.• <i>Weekdays</i>: Select to generate the report on specific days of each week, then select those days in <i>These weekdays</i>. Also configure <i>Hour</i>.• <i>These dates</i>: Select to generate the report on specific date of each month, then enter those date numbers in <i>These days</i>. Also configure <i>Hour</i>.

Choosing call rate

You can choose the call rate for calculating the phone bills. For information on setting the call rates, see [“Setting call rates” on page 255](#).

To choose the call rate

1. Go to *Log & Report > Call Report > Call Report*.
2. Expand *Rate Setting*.
3. Select an available rate and click -> to move it to the *Selected rates* field.
Only one call rate is allowed per report.
4. Click *Create*.

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 *Log & Report > Call Report > Call 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 31.

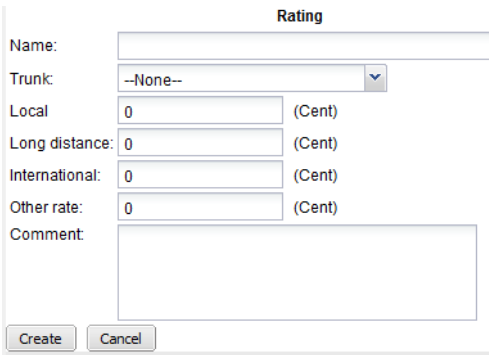
Setting call rates

The *Log & Report > Call Report > Rate* tab lets you set call rates for calculating phone bills.

To set call rates

1. Go to *Log & Report > Call Report > Rate* and click *New*.
2. Configure the following:

Figure 96: Setting call rate



<i>GUI field</i>	<i>Description</i>
Name	Enter a name for the rating profile.
Trunk	Select the trunk that will use the rates.
Local	Enter the rate for local phone calls.
Long distance	Enter the rate for long-distance phone calls.
International	Enter the rate for international phone calls.
Other rate	Enter the rate for other types of phone calls.
Comment	Enter any notes you have for this rating profile.

3. Click *Create*.

Configuring Station Messaging Detail Record (SMDR)

FortiVoice SMDR component provides FortiVoice call detail records to third party devices on certain communication and format protocols based on third party's device requirements. For example, Property Management System (PMS) uses the FortiVoice SMDR to manage hotel guest call charges.



Configuring FortiVoice SMDR requires advanced SMDR knowledge and should be performed by advanced administrative users and field engineers.

This section contains the following topics:

- [Configuring SMDR settings](#)
- [Setting SMDR formats](#)

Configuring SMDR settings

Configure SMDR settings to enable the FortiVoice communications with third party devices.

To configure SMDR settings

1. Go to *Log & Report > SMDR Settings > SMDR*.
2. Select *Enabled* to activate the FortiVoice SMDR function.
3. Select a format protocol for the FortiVoice communications with the third party devices.
For information on format, see [“Setting SMDR formats” on page 256](#).
4. For *Port*, enter the port number that connects to the third party devices.
5. For *Max clients*, enter the number of third party devices to which the FortiVoice unit provides SMDR. The range is 1-10.
6. For *Trusted hosts*, enter the IP address and netmask of the third party device.
If you have multiple third party devices, you may enter up to 10 trusted hosts.
7. Click *OK*.

Setting SMDR formats

To communicate with third party devices, the FortiVoice SMDR format needs to be defined based on the device requirements so that the devices can recognize the FortiVoice SMDR.

The FortiVoice unit provides example XML SMDR format files. You can modify the files to meet with your needs. The following is an example format file:

Figure 97: Example SMDR format file

```
<smdr_type id="Fortivoice">
  <discard_filter>
    <field name="Disposition" value="NO ANSWER"/>
  </discard_filter>
  <formatting>
    <field name="UniqueID" length="20"/>
    <field name="StartTime" length="20"/>
    <field name="EndTime" length="20"/>
    <field name="SourceForti" length="10"/>
    <field name="DestinationForti" length="10"/>
    <field name="Duration" length="8"/>
    <field type="text" value="@"/>
    <field type="line_break"/>
    <field type="line_break"/>
  </formatting>
</smdr_type>
```

An SMDR format is composed of parts as shown in the above example:

- *smdr_type id*: the name of the SMDR format file.
- *discard_filter*: the data you do not want to send to the third party devices.
- *formatting*: the body of the SMDR format file in the form of field values (for example, *<field name="AnswerTime"/>*), plus the field lengths (for example, *length="13"*) required by the third party devices.

To set SMDR format

1. Go to *Log & Report > SMDR Settings > Formats*.
2. Select an example format file and click *Edit*.
3. Click *Available FortiVoice SMDR field names* to display the complete list of FortiVoice SMDR field names.
4. 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.
5. Click *OK*.
6. If errors appear, click *SMDR types XML* 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 258](#)) and which event categories will trigger an alert email message (see [“Configuring alert categories” on page 258](#)).

Alert email messages also require that you supply the FortiVoice unit with the IP address of at least one DNS server. The FortiVoice unit uses the domain name of the SMTP server to send alert email messages. To resolve this domain name into an IP address, the FortiVoice unit must be able to query a DNS server. For information on DNS, see [“Configuring DNS” on page 46](#).

You can customize the alert email. For more information, see [“Customizing email history report and notification email templates” on page 105](#).

This section contains the following topics:

- [Configuring alert recipients](#)
- [Configuring alert categories](#)

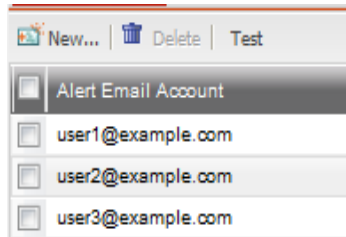
Configuring alert recipients

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 > Alerts > Configuration*.

Figure 98: Alert email configuration



<i>GUI field</i>	<i>Description</i>
Test (button)	Select one or more email accounts and click <i>Test</i> to verify that alert email is configured correctly. This sends a sample alert email to all selected recipients.
Alert Email Account	Displays the names of email accounts receiving email alerts.

2. Click *New* to add the email address of a recipient.
A single-field dialog appears.
3. In *Email to*, enter a recipient email address.
4. Click *Create*.
5. Repeat the previous steps to add more users.

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 258](#)).

To select events that will trigger an alert email message

1. Go to *Log & Report > Alerts > Categories*.
2. Select one or more of the following event categories check boxes:

Table 35: Alert email category choices

<i>GUI field</i>	<i>Description</i>
Critical events	Send an alert email message when the FortiVoice unit detects a system error that may affect its operation.
Disk is full	Send an alert email message when the hard disk of the FortiVoice unit is full.
HA events	Send an alert email message when any high availability (HA) event occurs.
Archive quota is exceeded	Send an alert email message when the recorded call archiving account reaches its quota of hard disk space. For information about recorded call archiving account quota, see “Archiving recorded calls” on page 223 .

Table 35: Alert email category choices

GUI field	Description
Deferred emails # over	Send an alert email message if the deferred email queue contains greater than this number of email messages. Enter a number between 1 and 10 000 to define the alert threshold, then enter the interval of time between each alert email message that the FortiVoice unit will send while the number of email messages in the deferred email queue remains over this limit.
Daily call summary	<p>Send an alert email with a daily call summary including the number of total calls, long distance calls, and international calls.</p> <p>You need to enter the time for generating the summary which is for the 24 hours period prior to the time you set. For example, if you set 9 for <i>Schedule at hour</i>, the summary will be for the period from 9am of the previous day to 9am of the day when you receive the alert email.</p>
PSTN digital line alarm	Send an alert email when the PSTN digital line has a problem. This option is not available for FortiVoice 200D.
PSTN analog line alarm	Send an alert email when the PSTN analog line has a problem. This option is not available for FortiVoice 200D.
Trunk lines are saturated	<p>Send an alert email when the SIP/PSTN/PRI trunk lines are fully occupied.</p> <p>SIP trunk alert only works if you select <i>Overflow check</i> when configuring SIP trunk. See “Setting up VoIP trunks” on page 170.</p>

3. Click *Apply*.

Installing firmware

Fortinet periodically releases FortiVoice firmware updates to include enhancements and address issues. After you have registered your FortiVoice unit, FortiVoice firmware is available for download at <http://support.fortinet.com>.

New firmware can also introduce new features which you must configure for the first time.

For information specific to the firmware release version, see the Release Notes available with that release.



In addition to major releases that contain new features, Fortinet releases patch releases that resolve specific issues without containing new features and/or changes to existing features. It is recommended to download and install patch releases as soon as they are available.



Before you can download firmware updates for your FortiVoice unit, you must first register your FortiVoice unit with Fortinet Technical Support. For details, go to <http://support.fortinet.com/> or contact Fortinet Technical Support.

This section includes:

- [Testing firmware before installing it](#)
- [Installing firmware](#)
- [Clean installing firmware](#)

Testing firmware before installing it

You can test a new firmware image by temporarily running it from memory, without saving it to disk. By keeping your existing firmware on disk, if the evaluation fails, you do not have to re-install your previous firmware. Instead, you can quickly revert to your existing firmware by simply rebooting the FortiVoice unit.

To test a new firmware image

1. Connect your management computer to the FortiVoice console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
2. Initiate a connection from your management computer to the CLI of the FortiVoice unit.
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.

Enter the following command to restart the FortiVoice unit:

```
execute reboot
```

6. As the FortiVoice unit starts, a series of system startup messages are displayed.
Press any key to display configuration menu.....
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 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:

7. Type G to get the firmware image from the TFTP server.
The following message appears:
Enter TFTP server address [192.168.2.99]:
8. Type the IP address of the TFTP server and press Enter.
The following message appears:
Enter Local Address [192.168.2.99]:
9. 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]:
10. 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]
Type R.
The FortiVoice image is loaded into memory and uses the current configuration, **without** saving the new firmware image to disk.
11. To verify that the new firmware image has been loaded, log in to the CLI and type:
get system status
12. Test the new firmware image.
 - If the new firmware image operates successfully, you can install it to disk, overwriting the existing firmware, using the procedure [“Installing firmware” on page 262](#).
 - If the new firmware image does **not** operate successfully, reboot the FortiVoice unit to discard the temporary firmware and resume operation using the existing firmware.

Installing firmware

You can use either the web-based manager or the CLI to upgrade or downgrade the firmware of the FortiVoice unit.

Administrators whose access profile contains *Read-Write* access in the *Others* category, such as the `admin` administrator, can change the FortiVoice firmware.

Firmware changes are either:

- an upgrade to a newer version
- a reversion to an earlier version

To determine if you are upgrading or reverting your firmware image, examine the firmware version number. For example, if your current firmware version is `FortiVoice-200D 2.00,build0082,120827`, changing to `FortiVoice-200D 2.00,build0081,120801`, an earlier build number and date, indicates that you are reverting.

Reverting to an earlier version may cause the FortiVoice unit to remove parts of the configuration that are not valid for that earlier version. In some cases, you may lose all call data and configurations.

When upgrading, there may also be additional considerations. For details, see [“Upgrading” on page 266](#).

Therefore, no matter if you are upgrading or downgrading, it is always a good practice to back up the configuration and call data. For details, see [“Backing up configuration” on page 99](#).

To install firmware using the web-based manager

1. Log in to the Fortinet Technical Support web site, <https://support.fortinet.com/>.
2. Download the firmware image file to your management computer.
3. Log in to the web-based manager as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
4. Install firmware in one of two ways:
 - Go to *Monitor > System Status > Status*, and in the *System Information* area, in the *Firmware version* row, click *Update*. Click *Browse* to locate the firmware and then click *Upload*.
 - Go to *System > Maintenance > Configuration*, under *Restore Firmware*, click *Browse* to locate the firmware. Then click *Restore*.

Your web browser uploads the firmware file to the FortiVoice unit. The FortiVoice unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.

If you are downgrading the firmware to a previous version, the FortiVoice unit reverts the configuration to default values for that version of the firmware. You must either reconfigure the FortiVoice unit or restore the configuration file.

5. Clear the cache of your web browser and restart it to ensure that it reloads the web-based manager and correctly displays all changes.
6. To verify that the firmware was successfully installed, log in to the web UI and go to *Monitor > System Status > Status*. Text appearing in the *Firmware version* row indicates the currently installed firmware version.

To install firmware using the CLI

1. Log in to the Fortinet Technical Support web site, <https://support.fortinet.com/>.
2. Download the firmware image file to your management computer.

3. Connect your management computer to the FortiVoice console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
4. Initiate a connection from your management computer to the CLI of the FortiVoice unit, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
5. Connect port1 of the FortiVoice unit directly or to the same subnet as a TFTP server.
6. Copy the new firmware image file to the root directory of the TFTP server.
7. Verify that the TFTP server is currently running, and that the FortiVoice unit can reach the TFTP server.

To use the FortiVoice CLI to verify connectivity, enter the following command:

```
execute ping 192.168.2.99
```

where `192.168.2.99` is the IP address of the TFTP server.

8. Enter the following command to download the firmware image from the TFTP server to the FortiVoice unit:

```
execute restore image tftp <name_str> <tftp_ipv4>
```

where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is `192.168.2.99`, enter:

```
execute restore image tftp image.out 192.168.2.99
```

One of the following messages appears:

```
This operation will replace the current firmware version!
```

```
Do you want to continue? (y/n)
```

or:

```
Get image from tftp server OK.
```

```
Check image OK.
```

```
This operation will downgrade the current firmware version!
```

```
Do you want to continue? (y/n)
```

9. Type `y`.

The FortiVoice unit downloads the firmware image file from the TFTP server. The FortiVoice unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.

If you are downgrading the firmware to a previous version, the FortiVoice unit reverts the configuration to default values for that version of the firmware. You must either reconfigure the FortiVoice unit or restore the configuration file.

10. If you also use the web-based manager, clear the cache of your web browser and restart it to ensure that it reloads the web-based manager and correctly displays all tab, button, and other changes.

11. To verify that the firmware was successfully installed, log in to the CLI and type:

```
get system status
```

12. If you have downgraded the firmware version, reconnect to the FortiVoice unit using its default IP address for port1, `192.168.1.99`, and restore the configuration file. For details, see [“Reconnecting to the FortiVoice unit” on page 264](#) and [“Restoring the configuration” on page 265](#).

If you have upgraded the firmware version, to verify the conversion of the configuration file, see [“Verifying the configuration” on page 266](#). If the upgrade is unsuccessful, you can downgrade the firmware to a previous version.

Reconnecting to the FortiVoice unit

After downgrading to a previous firmware version, the FortiVoice unit reverts to default settings for the installed firmware version, including the IP addresses of network interfaces through which you connect to the FortiVoice web-based manager and/or CLI.



If your FortiVoice unit has not been reset to its default configuration, but you cannot connect to the web-based manager or CLI, you can restore the firmware, resetting the FortiVoice unit to its default configuration in order to reconnect using the default network interface IP address. For more information, see [“Clean installing firmware” on page 267](#).

To reconnect using the CLI

1. Connect your management computer to the FortiVoice console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
2. Start HyperTerminal, enter a name for the connection and click *OK*.
3. Configure HyperTerminal to connect directly to the communications (COM) port on your computer and click *OK*.
4. Select the following port settings and click *OK*:

Table 36: Port settings

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

5. Press Enter to connect to the FortiVoice CLI.
The login prompt appears.
6. Type `admin` and press Enter twice.
The following prompt appears:
`Welcome!`

7. Enter the following command:

```
set system interface <interface_str> mode static ip <address_ipv4>
<mask_ipv4>
```

where:

- <interface_str> is the name of the network interface, such as `port1`
- <address_ipv4> is the IP address of the network interface, such as `192.168.1.10`
- <mask_ipv4> is the netmask of the network interface, such as `255.255.255.0`

Enter the following command:

```
set system interface <interface_str> config allowaccess
<accessmethods_str>
```

where:

- <interface_str> is the name of the network interface configured in the previous step, such as `port1`
- <accessmethods_str> is a space-delimited list of the administrative access protocols that you want to allow on that network interface, such as `ping ssh https`

The network interface's IP address and netmask is saved. You can now reconnect to either the web UI or CLI through that network interface. For information on restoring the configuration, see [“Restoring the configuration” on page 265](#).

Restoring the configuration

You can restore a backup copy of the configuration file from your local PC using either the web-based manager or CLI. For information about configuration backup, see [“Backing up configuration” on page 99](#).

If you have just downgraded or restored the firmware of the FortiVoice unit, restoring the configuration file can be used to reconfigure the FortiVoice unit from its default settings.

To restore the configuration file using the web UI

1. Clear your browser's cache. If your browser is currently displaying the web-based manager, also refresh the page.
2. Log in to the web-based manager.
3. Go to *System > Maintenance > Configuration*.
4. Under *Restore Configuration*, click *Browse* to locate and select the configuration file that you want to restore, then click *Restore*.

The FortiVoice unit restores the configuration file and reboots. Time required varies by the size of the file and the speed of your network connection.

5. After restoring the configuration file, verify that the settings have been successfully loaded. For details on verifying the configuration restoration, see [“Verifying the configuration” on page 266](#).

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 settings!
```

```
(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. For details on verifying the configuration restoration, see “[Verifying the configuration](#)” on page 266.

Verifying the configuration

After installing a new firmware file, you should verify that the configuration has been successfully converted to the format required by the new firmware and that no configuration data has been lost.

In addition to verifying successful conversion, verifying the configuration also provides familiarity with new and changed features.

To verify the configuration upgrade

1. Clear your browser’s cache and refresh the login page of the web-based manager.
2. Log in to the web-based manager using the `admin` administrator account.
Other administrator accounts may not have sufficient privileges to completely review the configuration.
3. Review the configuration and compare it with your configuration backup to verify that the configuration has been correctly converted.

Upgrading

If you are upgrading, it is especially important to note that the upgrade process may require a specific path. Very old versions of the firmware may not be supported by the configuration upgrade scripts that are used by the newest firmware. As a result, you may need to upgrade to an intermediate version of the firmware first, **before** upgrading to your intended version. Upgrade paths are described in the Release Notes.

Before upgrading the firmware of the FortiVoice unit, for the most current upgrade information, review the Release Notes for the new firmware version. Release Notes are available from <http://support.fortinet.com> when downloading the firmware image file.

Release Notes may contain late-breaking information that was not available at the time this guide was prepared.

Clean installing firmware

Clean installing the firmware can be useful if:

- you are unable to connect to the FortiVoice unit using the web-based manager or the CLI
- you want to install firmware **without** preserving any existing configuration
- a firmware version that you want to install requires that you format the boot device (see the Release Notes accompanying the firmware)

Unlike upgrading or downgrading firmware, clean installing firmware re-images the boot device. Also, a clean install can only be done during a boot interrupt, before network connectivity is available, and therefore requires a local console connection to the CLI. **A clean install cannot be done through a network connection.**



Back up your configuration before beginning this procedure, if possible. A clean install resets the configuration, including the IP addresses of network interfaces. For information on backups, see “[Backing up configuration](#)” on page 99. For information on reconnecting to a FortiVoice unit whose network interface configuration has been reset, see “[Reconnecting to the FortiVoice unit](#)” on page 264.



If you are reverting to a previous FortiVoice version, you might not be able to restore your previous configuration from the backup configuration file.

To clean install the firmware

1. Download the firmware file from the Fortinet Technical Support web site, <https://support.fortinet.com/>.
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 unit starts, a series of system startup messages are displayed.

```
Press any key to display configuration menu.....
```

9. Immediately press a key to interrupt the system startup.



You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiVoice unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appear:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[I]: Configuration and information.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

Enter G,F,B,I,Q,or H:

10.If the firmware version requires that you first format the boot device before installing firmware, type F. (Format boot device) before continuing.

11.Type G to get the firmware image from the TFTP server.

The following message appears:

Enter TFTP server address [192.168.2.99]:

12.Type the IP address of the TFTP server and press Enter.

The following message appears:

Enter Local Address [192.168.1.188]:

13.Type a temporary IP address that can be used by the FortiVoice unit to connect to the TFTP server.

The following message appears:

Enter File Name [image.out]:

14.Type the firmware image file name and press Enter.

The FortiVoice unit downloads the firmware image file from the TFTP server and displays a message similar to the following:

```
Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]
```

15.Type D.

The FortiVoice unit downloads the firmware image file from the TFTP server. The FortiVoice unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.

The FortiVoice unit reverts the configuration to default values for that version of the firmware.

16.Clear the cache of your web browser and restart it to ensure that it reloads the web-based manager and correctly displays all tab, button, and other changes.

17.To verify that the firmware was successfully installed, log in to the CLI and type:

```
get system status
```

The firmware version number appears.

18.Either reconfigure the FortiVoice unit or restore the configuration file from a backup. For details, see [“Restoring the configuration” on page 265](#).

Appendix A: Installing Click-to-Dial software

If you use MicroSoft Outlook, you can install the FortiVoice Click-to-Dial plugin to dial the phone numbers of your contacts.

For information on installing the software, go to [FortiVoice Click-to-Dial Software Installation](#).



Step 4 in the instructions is specific to FortiVoice 40/70/100 models. For FortiVoice 200D/200D-T, do the following:

- *System IP Address*: Enter the FortiVoice IP address. For details, see “[Configuring the network interfaces](#)” on page 40.
 - *User Extension #*: Enter the user ID of the extension. For details, see “[Configuring IP extensions](#)” on page 133.
 - *Password*: Enter the password used for configuring your SIP phone from the phone or the Web. For details, see “[Configuring IP extensions](#)” on page 133.
-

Index

A

- active-passive HA 56
- address bar 20
- administrative access 41
- administrator
 - "admin" account 15, 16, 262, 263, 265, 266, 267
 - log messages 248
- alert email 57, 257
 - recipients 258
- appearance, web-based manager 89
- authentication 15
 - LDAP 125

B

- backup unit 54
- bandwidth 23
- Base64 96, 97
- bind DN 128, 129, 130
- boot interrupt 267
- browser 14, 15, 19
 - warnings 15

C

- cable
 - null modem 16
- call statistics 24
- certificate
 - backup 98
 - default 15
 - mismatch 15
 - options 94
 - self-signed 15
 - server 92
 - warning 15
- certificate authority (CA) 15, 93, 94, 96, 97, 98, 99
- certificate request
 - downloading and submitting 96
- certificate revocation list (CRL) 99
- certification 8
- CIDR 12
- clean install firmware 267
- CLI 44
 - connecting to 16
- column view
 - logs 34
- command line interface (CLI) 9, 11, 14
- comma-separated value (CSV) 250
- common name (CN) field 15
- communications (COM) port 16
- configuration, verifying the 266
- configured operating mode 58
- connecting
 - web UI 15
- conventions 9

- CPU 23, 82
- CSV import 141

D

- dashboard 21
- date 74
- daylight savings time (DST) 74, 75
- default
 - administrator account
 - 15, 16, 262, 263, 265, 266, 267
 - bridge configuration 39
 - certificate 15
 - gateway 45
 - password 15, 16, 17, 18
 - route 45
 - settings 16
- default variables 106, 107, 108
- DHCP 43
- DNS server 46, 257
- documentation 9
 - conventions 9
 - Release Notes 267
- domain name
 - certificate 15
- DOS 14
- dotted decimal 12
- downgrade 262
- download
 - report 31
- dynamic DNS (DDNS) 95
- dynamic IP address 43

E

- effective operating mode 60
 - HA 58
- _email 12
- end-user guide 19
- Ethernet 15, 16
- expected input 11

F

- factory default settings 16
- failover 61, 63, 64, 81
 - HA 67
- FAQ 9
- firmware 262
 - change 22
 - clean install 267
 - downgrade 262
 - upgrade 262
 - version 21
- formatted view
 - logs 34
- formatting the boot device 267
- FortiAnalyzer 246, 248

- Fortinet
 - Knowledge Base 9
 - MIB 85, 86
 - Technical Documentation 9
 - conventions 9
 - Technical Support 8
 - Technical Support, registering with 8
 - Technical Support, web site 8
 - Training Services 8
- _fqdn 12
- frame size 44
- fully qualified domain name (FQDN) 12, 95
- fully-qualified domain name (FQDN) 95
- G**
- gateway 45
- glossary 9
- graphical user interface (GUI) 14
- H**
- HA
 - active-passive 56
 - alert email 57
 - backup unit 54
 - configuration not synchronized 55
 - configuration options 56, 60
 - configured operating mode 58
 - effective operating mode 58, 60
 - failover 61, 63, 64, 67, 81
 - forcing configuration synchronization 59
 - forcing data synchronization 59
 - heartbeat 55, 57
 - interface configuration synchronization 56
 - log messages 57
 - mail queue sync after a failover 56
 - master 54
 - monitoring 55, 66
 - MTA spool directory sync after a failover 56
 - network interface 56
 - primary unit 54
 - service monitoring 56, 57
 - slave 54
 - synchronization 55, 57
 - virtual IP 66
 - wait for recovery then assume slave role 62, 69
 - wait for recovery then restore original role 62, 69
- halt 23
- hard disk
 - logging to 246
- heartbeat 57
 - HA 55
- high availability (HA) 53
 - log messages 248
- host name 15
 - in HA 55
- how-to 9
 - HA 56
- HTTP
 - web-based manager 44
- HTTPS 15, 44, 92, 95

- HyperTerminal 16
- I**
- ICMP ECHO 44
- idle timeout 79
- import
 - user in CSV 141
- _index 12
- index number 12
- InetOrgPerson 130
- input constraints 11
- _int 12
- Internet service provider (ISP) 46
- IP address 15, 16, 20
 - private network 9
- _ipv4 12
- _ipv4/mask 12
- _ipv4mask 12
- _ipv6 12
- _ipv6mask 12

- K**
- Knowledge Base 9

- L**
- language
 - web-based manager 90
- LDAP
 - bind 128
 - bind DN 129, 130
 - cache 131
 - password 128
 - profile 125
 - query 130
 - schema 130
 - timeout 131
 - TTL 131
- LDAPS 127, 128
- local certificate
 - options 94
- location 20
- log
 - column view 34
 - formatted view 34
 - FortiAnalyzer 248
 - rotate 247
 - search 36
 - severity level 245
 - storage 246
 - storing 246
 - Syslog 248
 - to the hard disk 246

- M**
- management IP 39
- master 54
- master, HA mode 62
- maximum transmission unit (MTU) 44
- media access control (MAC) 42

- memory usage 23
- MIB 86
 - Fortinet 85
 - RFC 1213 85
 - RFC 2665 85
- Microsoft
 - Internet Explorer 15
- Microsoft Active Directory 130
- mode
 - HA 53
- monitor
 - HA 55
- monitoring services
 - for HA 56
- Mozilla Firefox 15

N

- _name 12
- network
 - interface 16
- network interface
 - in HA 56
- network time protocol (NTP) 74, 75
- next-hop router 45, 46
- null modem cable 16

O

- objectClass 130
- on HA failure
 - wait for recovery then assume slave role 62, 69
 - wait for recovery then restore original role 62, 69

P

- password 15, 16, 17, 18
 - administrator 51
 - certificate 98
 - LDAP bind 128
- _pattern 12
- pattern 12
- PDF report 254
- ping 44
- PKCS #10 96
- PKCS #12 97, 98
- port1 16
- primary unit 54
- privacy-enhanced email (PEM) 97
- product registration 8
- profile
 - administrator access 52
 - LDAP 125
- protocol 131
 - administrative access 52
- public key 97

Q

- query
 - cache 131
 - filter 130
 - LDAP 130
 - report 252
 - SNMP 84, 85

R

- reachable 45
- read & write
 - administrator 52
- reconnecting to the FortiMail unit 264
- registering
 - with Fortinet Technical Support 8
- regular expression 12
- Release Notes 267
- report
 - configure 250
 - download 31
 - HTML format 254
 - on demand 250
 - PDF format 254
 - periodically generated 250
 - query 252
 - subject matter 252
 - time span 253
 - view 31
- reset
 - effective operating mode for HA 59
- restart 23
- restore
 - factory defaults 38
 - previous configuration 265
- RFC
 - 1213 81, 85
 - 1918 10
 - 2665 81, 85
- RJ-45 15, 16
- route
 - default 45
 - static 45

S

- secure (S/MIME) 98
- Secure Shell (SSH) 14
- secure shell (SSH) 44
- security certificate 15
- self-signed 15
- services
 - monitoring for HA 56
- severity level 245
- shut down 23
- slave 54
- slave, HA mode 62

- SNMP 44
 - community 83, 84
 - event 84, 85
 - manager 83, 84, 85, 86
 - MIB 86
 - MIBs 85
 - query 84, 85
 - RFC 12123 85
 - RFC 2665 85
 - traps 86
- SSL 127, 128
- static route 45
- static routing 45
- storing logs 246
- _str 12
- string 12
- subject matter 252
- synchronization 55
- syntax 11
- Syslog 246, 248
- system options
 - changing 78
 - data and time 74
- system resource usage 21
- system time 21

T

- technical
 - documentation 9
 - notes 9
- Telnet 14
- telnet 44
- terminal 14, 16
- time 74
- time to live (TTL)
 - cache 131
 - LDAP 131
- time zone 75
- timeout 131
- Training Services 8
- transport layer security (TLS) 98
- traps, SNMP 86

- troubleshooting 131
 - Syslog 250
- trust certificate 15
- trusted host 52

U

- UNIX 14
- update 262
 - verify 266
- uptime 21
- URL 15, 20
- _url 12
- Use secure connection 127
- user
 - group 126
 - query 130
- user guide 19

V

- _v4mask 12
- _v6mask 12
- value parse error 12
- variable
 - Predefined 105
- variables
 - predefined list 106, 107, 108
- virtual IP
 - HA 66

W

- wait for recovery then assume slave role
 - on HA failure 62, 69
- wait for recovery then restore original role
 - on HA failure 62, 69
- web browser 14, 15, 19
 - warnings 15
- web UI 15
- web-based manager
 - customizing appearance 89
 - HTTP 44
 - HTTPS 44
 - language 90
- widget 21
- wild cards 12

