



# FortiVoice™ Phone System 5.3.0 Administration Guide



## FortiVoice Phone System 5.3.0 Administration Guide

May 30, 2017

3rd Edition

Copyright© 2017 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	<a href="https://docs.fortinet.com">docs.fortinet.com</a>
Knowledge Base	<a href="https://kb.fortinet.com">kb.fortinet.com</a>
Customer Service & Support	<a href="https://support.fortinet.com">support.fortinet.com</a>
Training Services	<a href="https://training.fortinet.com">training.fortinet.com</a>
FortiGuard	<a href="https://fortiguard.com">fortiguard.com</a>
Document Feedback	<a href="mailto:techdocs@fortinet.com">techdocs@fortinet.com</a>

# Table of Contents

<b>Introduction.....</b>	<b>9</b>
Registering your Fortinet product.....	9
Customer service & technical support.....	9
Training.....	9
Documentation.....	10
Fortinet Tools & Documentation CD.....	10
Fortinet Knowledge Base.....	10
Comments on Fortinet technical documentation.....	10
Scope.....	10
Conventions.....	10
IP addresses.....	10
Cautions and notes.....	11
Typographical conventions.....	11
Command syntax conventions.....	12
<b>Connecting to the FortiVoice System.....</b>	<b>15</b>
Connecting to the web-based manager or CLI.....	15
Connecting to the web-based manager.....	16
Connecting to the CLI.....	17
Setting up the system using the wizard.....	19
Testing the setup.....	19
Configuring setups for phone users.....	20
Accessing the user web portal.....	20
Changing the user PIN.....	21
Receiving and sending fax.....	21
Using the operator console.....	21
Setting user privileges and preferences.....	21
Setting the feature codes.....	21
<b>Monitoring the FortiVoice System.....</b>	<b>22</b>
Viewing overall system status.....	22
Viewing the dashboard.....	22
Viewing the Call Statistics.....	25
Using the CLI Console.....	25
Viewing phone system status.....	25
Viewing active calls.....	25
Viewing parked calls.....	26
Viewing conference calls.....	26
Viewing extension status.....	26
Viewing hot desking configurations.....	27
Viewing trunk status.....	27
Viewing unassigned phones.....	28
Viewing DHCP client list.....	30

Viewing call/fax storage .....	31
Playing recorded calls.....	31
Viewing current fax accounts.....	31
Viewing archived faxes .....	31
Viewing fax queues .....	32
Viewing call records.....	32
Viewing generated reports.....	32
Viewing log messages .....	33
Displaying and arranging log columns.....	35
Using the right-click pop-up menus .....	36
Searching log messages.....	37
Viewing phone directories .....	38
<b>Configuring System Settings.....</b>	<b>40</b>
Configuring network settings.....	40
About IPv6 Support .....	40
About the management IP .....	41
About FortiVoice logical interfaces .....	41
Configuring the network interfaces.....	42
Configuring static routes.....	47
Configuring DNS .....	48
Configuring DHCP server.....	48
Capturing voice and fax packets .....	50
Configuring administrator accounts and access profiles .....	52
Configuring administrator accounts.....	52
Configuring administrator profiles.....	55
Using high availability .....	55
About high availability .....	56
About the heartbeat and synchronization.....	57
How to use HA.....	58
Monitoring the HA status .....	59
Configuring the HA mode and group.....	62
Example: Failover scenarios .....	69
Configuring system time, system options, SNMP, email setting, GUI appearance, and call data storage .....	75
Configuring the time and date .....	76
Configuring system options .....	80
Configuring SNMP queries and traps .....	83
Configuring email settings .....	89
Customizing the GUI appearance.....	91
Selecting the call data storage location.....	93

Managing certificates.....	96
Managing local certificates .....	96
Obtaining and installing a local certificate .....	97
Managing certificate authority certificates.....	102
Managing the certificate revocation list.....	103
Maintaining the system.....	103
Maintaining the system configuration.....	103
Downloading a trace file .....	104
<b>Configuring Phone System.....</b>	<b>105</b>
Configuring phone system settings .....	105
Setting PBX location and contact information.....	105
Configuring PBX options.....	106
Customizing call report and notification email templates.....	109
Configuring advanced phone system settings .....	110
Configuring SIP settings .....	110
Configuring SIP phone auto-provisioning.....	112
Adding prompt languages .....	113
Managing phone configurations .....	115
Configuring system capacity .....	116
Managing sound files and music on hold.....	117
Working with FortiVoice profiles .....	118
Configuring SIP profiles .....	119
Modifying caller IDs .....	120
Configuring phone profiles.....	122
Configuring LDAP profiles.....	125
Configuring user privileges .....	130
Configuring location profile.....	130
Scheduling the FortiVoice unit.....	131
Configuring FortiFone 870i .....	131
Reviewing system configuration.....	133
<b>Configuring Extensions.....</b>	<b>134</b>
Setting up local extensions.....	134
Configuring IP extensions .....	134
Modifying analog extension (200D-T, 1000E-T, and 20E2 models only).....	145
Setting up remote extensions .....	148
Configuring fax extensions .....	151
Setting extension user preferences .....	154
Resetting voice messages .....	163

Creating extension groups.....	163
Creating user groups .....	163
Creating extension departments.....	164
Creating ring groups .....	164
Creating page groups .....	166
Creating pickup groups .....	167
Setting up general voice mailboxes.....	167
Working with virtual numbers .....	171
<b>Configuring Trunks.....</b>	<b>173</b>
Setting up VoIP trunks .....	173
Testing SIP trunks.....	177
Creating a SIP trunk with FortiCall service .....	178
Modifying PSTN/PRI trunks .....	179
Configuring the T1/E1 span .....	182
Configuring the analog voice trunk.....	184
Configuring office peers.....	185
<b>Configuring Call Routing .....</b>	<b>187</b>
Configuring inbound dial plans .....	187
Configuring direct inward dialing .....	190
Mapping DIDs .....	191
Configuring outbound dial plans.....	192
Testing outbound dial plans.....	194
Creating dialed number match .....	194
Configuring call handling actions.....	196
<b>Setting up a Call Center.....</b>	<b>198</b>
Creating call queues .....	198
Configuring agents.....	207
Configuring IVRs .....	208
Setting up an IVR .....	208
Configuring restful service .....	214
Configuring surveys .....	214
Setting up queue view .....	216
Configuring other agent information.....	216
Adding agent skill sets .....	216
Creating agent skill levels .....	217
Modifying agent reason code descriptions.....	217
Configuring data service .....	217
Setting caller priorities .....	217
Configuring agent profiles.....	218
Working with call queue statistics .....	219

Configuring call center report profiles and generating reports.....	220
Configuring the report query selection .....	221
Configuring the report time period.....	222
Configuring report email notifications.....	222
Configuring the report schedule .....	222
Generating a report manually.....	223
<b>Working with Property Management System .....</b>	<b>224</b>
Configuring hotel management settings.....	224
Configuring hotel room status .....	226
<b>Configuring phone auto dialer .....</b>	<b>228</b>
Setting up an auto dialer campaign.....	228
Creating a recorded broadcast message .....	229
Adding contacts and contact groups .....	229
Configuring auto dialer settings.....	229
Viewing auto dialer reports .....	230
<b>Configuring Call Features .....</b>	<b>231</b>
Configuring auto attendants .....	231
Viewing auto attendant hierarchies.....	233
Configuring key actions .....	235
Configuring user privileges .....	237
Configuring account codes.....	241
Mapping speed dials .....	242
Configuring conference calls .....	242
Recording calls .....	245
Configuring call recordings.....	245
Setting the recorded file format .....	246
Archiving recorded calls .....	247
Creating call queues .....	248
Configuring call parking .....	252
Configuring fax.....	253
Receiving Faxes.....	253
Sending faxes .....	255
Configuring other fax settings.....	259
Archiving faxes.....	260
Setting calendar reminder.....	261
Modifying feature access codes.....	262
<b>Configuring Logs and Reports .....</b>	<b>268</b>
About FortiVoice logging .....	268
FortiVoice log types .....	268
Log message severity levels .....	269

Configuring logging.....	270
Configuring logging to the hard disk.....	270
Choosing which events to log.....	271
Configuring logging to a Syslog server or FortiAnalyzer unit.....	272
Configuring report profiles and generating call reports .....	274
Configuring the report query selection .....	275
Configuring the report time period.....	277
Configuring report email notifications.....	277
Configuring the report schedule .....	278
Choosing call rate .....	278
Generating a report manually.....	278
Setting call rates .....	279
Submitting CDRs to a database .....	279
Configuring CDR submission.....	279
Modifying CDR templates.....	280
Creating CDR filters .....	281
Configuring Station Messaging Detail Record (SMDR) .....	281
Configuring SMDR settings .....	281
Setting SMDR formats .....	282
Configuring alert email .....	282
Configuring alert recipients .....	283
Configuring alert categories.....	283
<b>Installing firmware.....</b>	<b>285</b>
Testing firmware before installing it .....	285
Installing firmware.....	287
Reconnecting to the FortiVoice unit.....	289
Restoring the configuration.....	290
Verifying the configuration .....	291
Upgrading .....	291
Clean installing firmware.....	292
<b>Appendix A: Installing Click-to-Dial software.....</b>	<b>294</b>
<b>Index .....</b>	<b>295</b>



# Introduction

Welcome, and thank you for selecting Fortinet products.

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

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

This document describes how to configure and use the FortiVoice phone system. Only the configuration procedures through the web-based manager are provided. 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](mailto: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](mailto: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
<b>Button, menu, text box, field, or check box label</b>	From <i>Minimum log level</i> , select <i>Notification</i> .
<b>CLI input</b>	<pre>config system dns   set primary &lt;address_ipv4&gt; end</pre>
<b>CLI output</b>	<pre>FGT-602803030703 # get system settings comments           : (null) opmode              : nat</pre>
<b>Emphasis</b>	HTTP connections are <b><i>not</i></b> secure and can be intercepted by a third party.
<b>File content</b>	<pre>&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;Firewall Authentication&lt;/TITLE&gt;&lt;/HEAD&gt; &lt;BODY&gt;&lt;H4&gt;You must authenticate to use this service.&lt;/H4&gt;</pre>
<b>Hyperlink</b>	Visit the Fortinet Technical Support web site, <a href="https://support.fortinet.com">https://support.fortinet.com</a> .
<b>Keyboard entry</b>	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

<b>Navigation</b>	Go to <i>Monitor &gt; Status &gt; DHCP</i> .
<b>Publication</b>	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

<b>Convention</b>	<b>Description</b>
<b>Square brackets [ ]</b>	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

<p><b>Angle brackets &lt; &gt;</b></p>	<p>A word constrained by data type.</p> <p>To define acceptable input, the angled brackets contain a descriptive name followed by an underscore ( _ ) and suffix that indicates the valid data type. For example:</p> <pre>&lt;retries_int&gt;</pre> <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"><li>• <b>&lt;xxx_name&gt;</b>: A name referring to another part of the configuration, such as <code>policy_A</code>.</li><li>• <b>&lt;xxx_index&gt;</b>: An index number referring to another part of the configuration, such as 0 for the first static route.</li><li>• <b>&lt;xxx_pattern&gt;</b>: 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>.</li><li>• <b>&lt;xxx_fqdn&gt;</b>: A fully qualified domain name (FQDN), such as <code>mail.example.com</code>.</li><li>• <b>&lt;xxx_email&gt;</b>: An email address, such as <code>admin@mail.example.com</code>.</li><li>• <b>&lt;xxx_url&gt;</b>: 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>.</li><li>• <b>&lt;xxx_ipv4&gt;</b>: An IPv4 address, such as <code>192.168.1.99</code>.</li><li>• <b>&lt;xxx_v4mask&gt;</b>: A dotted decimal IPv4 netmask, such as <code>255.255.255.0</code>.</li><li>• <b>&lt;xxx_ipv4mask&gt;</b>: A dotted decimal IPv4 address and netmask separated by a space, such as <code>192.168.1.99 255.255.255.0</code>.</li><li>• <b>&lt;xxx_ipv4/mask&gt;</b>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as <code>192.168.1.99/24</code>.</li><li>• <b>&lt;xxx_ipv6&gt;</b>: A colon ( : )-delimited hexadecimal IPv6 address, such as <code>3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234</code>.</li><li>• <b>&lt;xxx_v6mask&gt;</b>: An IPv6 netmask, such as <code>/96</code>.</li><li>• <b>&lt;xxx_ipv6mask&gt;</b>: An IPv6 address and netmask separated by a space.</li><li>• <b>&lt;xxx_str&gt;</b>: A string of characters that is <b>not</b> another data type, such as <code>P@ssw0rd</code>. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences.</li><li>• <b>&lt;xxx_int&gt;</b>: An integer number that is <b>not</b> another data type, such as 15 for the number of minutes.</li></ul>
--	--

**Table 2:** Command syntax notation

<b>Curly braces { }</b>	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces.  You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].
<b>Options delimited by vertical bars  </b>	Mutually exclusive options. For example:  <code>{enable   disable}</code>  indicates that you must enter either <code>enable</code> or <code>disable</code> , but must not enter both.
<b>Options delimited by spaces</b>	Non-mutually exclusive options. For example:  <code>{http https ping snmp ssh telnet}</code>  indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:  <code>ping https ssh</code>  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:  <code>ping https snmp ssh</code>  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.

# 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 23.



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

<b>Network Interface</b>	port1
<b>URL</b>	<a href="https://192.168.1.99/admin">https://192.168.1.99/admin</a>
<b>Administrator Account</b>	admin
<b>Password</b>	(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 23](#). 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

<b>Network Interface</b>	port1
<b>IP Address</b>	192.168.1.99
<b>SSH Port Number</b>	22
<b>Administrator Account</b>	admin
<b>Password</b>	(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*.

<b>Bits per second</b>	9600
<b>Data bits</b>	8
<b>Parity</b>	None
<b>Stop bits</b>	1
<b>Flow control</b>	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 server 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 134](#). 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 134](#).

## 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 253](#).

## 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 238](#).

## 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 237](#) and [“Setting extension user preferences” on page 154](#).

## 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 262](#).

# 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

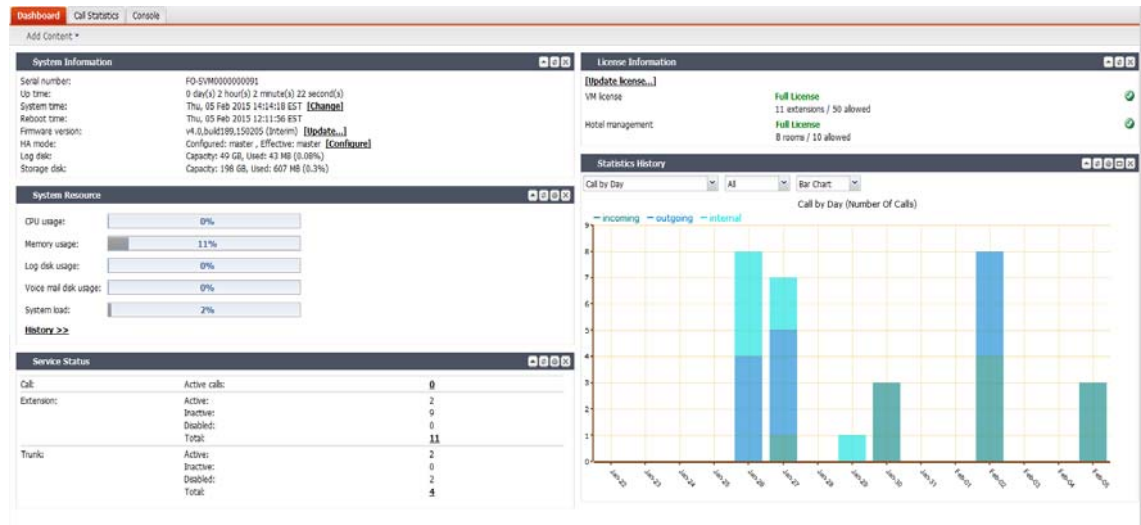
## Viewing the dashboard

*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, license information, 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 285.

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

### License Information widget

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

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

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



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

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

### 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 25.

### 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 252.

## 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 242.

## 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, phone information, and if it has any auxiliary devices.

For more information, see “[Configuring Extensions](#)” on page 134.

<b>GUI field</b>	<b>Description</b>
<b>Category/Status</b>	Select to view the extensions by categories. Each category has its corresponding statuses. <ul style="list-style-type: none"><li>• <i>All</i>: Displays extensions in all statuses.</li><li>• <i>Active</i>: Can display extensions in each of the following statuses once selected:<ul style="list-style-type: none"><li>• <i>Idle</i>: The extension is not in use.</li><li>• <i>In Use</i>: The extension is in use.</li><li>• <i>Busy</i>: The extension is busy.</li><li>• <i>Ringing</i>: The extension is ringing.</li><li>• <i>On Hold</i>: The extension has an on-hold call.</li><li>• <i>Other</i>: The status other than the above.</li></ul></li><li>• <i>Inactive</i>: Can display extensions in each of the following statuses once selected:<ul style="list-style-type: none"><li>• <i>Not registered</i>: The extension is not registered with the FortiVoice unit and is not in service.</li><li>• <i>Unavailable</i>: The extension is not reachable.</li></ul></li><li>• <i>Disable</i>: Displays all disabled extensions.</li></ul>

<b>Deregister</b>	Select an extension and click this icon to remove the extension assigned to the phone.
<b>Status</b>	The status of the extension. See <a href="#">“Category/Status” on page 26.</a>
<b>User ID</b>	This is the system-generated ID based on the extension number.
<b>Number</b>	The extension number.
<b>Display Name</b>	The name displaying on the extension. This is usually the name of the extension user.
<b>Type</b>	The type for this extension, such as SIP or analog (for the FortiVoice 200D-T and 2000E-T2 models).
<b>IP</b>	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 <a href="#">“IP” on page 141.</a>
<b>Phone type</b>	The phone brand and model.
<b>Phone Info</b>	The phone brand and model and its MAC address.
<b>Auxiliary device</b>	Devices added to the extension. This is known as SIP forking. For more information, see <a href="#">“Configuring IP extensions” on page 134.</a>

## 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.

If the two phones use different programmable phone keys, the host phone will reboot. For information on programmable phone keys, see [“Configuring phone profiles” on page 122.](#)

For information on configuring hot desking, see [“Hot-desking” on page 240.](#)

## Viewing trunk status

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

The trunk statuses include:

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

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 173](#).

## 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 134](#) and [“Configuring user privileges” on page 237](#).

**Figure 3: 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
<b>Action</b>	<ul style="list-style-type: none"> <li>• <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 <a href="#">“To assign a new extension user to an unassigned phone”</a> on page 29.</li> <li>• <i>Assign to FortiFone-870i device</i>: Select an unassigned FortiFone 870i 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 <a href="#">“To assign a new extension user to an unassigned phone”</a> on page 29.</li> <li>• <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 <a href="#">“To assign an existing extension user to an unassigned phone”</a> on page 29.</li> </ul>
<b>Export</b>	Select to save the unassigned phone list in <i>csv</i> format.
<b>MAC</b>	The Media Access Control address (MAC address) of the unassigned phone.
<b>IP</b>	The IP address of the unassigned phone assigned by the FortiVoice unit.
<b>Vendor</b>	The brand name of the unassigned phone.
<b>Phone Info</b>	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 134.
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.

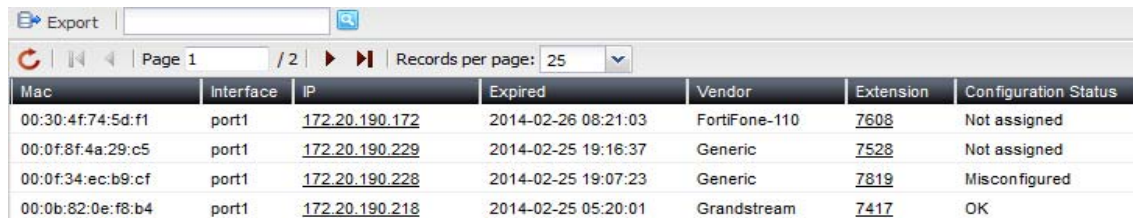
For the supported DHCP-enabled phone to connect to the FortiVoice unit:

- 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 48](#).

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 48](#).
- 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 4:** DHCP client list



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

<b>GUI field</b>	<b>Description</b>
<b>Export</b>	Select to save the DHCP client list in <code>csv</code> format.
<b>MAC</b>	The Media Access Control address (MAC address) of the DHCP client.
<b>Interface</b>	The FortiVoice unit port to which the DHCP client connects. For information on FortiVoice interfaces, see <a href="#">“Configuring network settings” on page 40</a> .
<b>IP</b>	The IP address of the DHCP client assigned by the FortiVoice DHCP server.
<b>Expired</b>	The expiration time of the DHCP client IP address.
<b>Vendor</b>	The brand names of the DHCP clients.

<b>Extension</b>	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 <a href="#">“Viewing unassigned phones” on page 28</a> .
<b>Configuration Status</b>	<ul style="list-style-type: none"> <li>• <i>OK</i>: The DHCP client is assigned to a new or an existing extension user.</li> <li>• <i>Not assigned</i>: The DHCP client is not assigned to a new or an existing extension user.</li> <li>• <i>Misconfigured</i>: The DHCP client’s configuration has errors.</li> </ul>

## 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 245](#).

### 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 253](#).

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 253](#).

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. 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 253.

## 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, call type, and call recordings.

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 274.



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

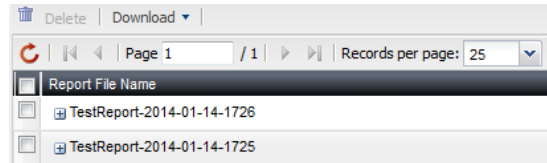
---

### To view call or call center reports

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



**Figure 5:** Reports tab



<b>GUI field</b>	<b>Description</b>
<b>Download</b>	Click to create a PDF or HTML version of the report.
<b>Report File Name</b>	<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>
<b>Last Access Time</b>	Lists the date and time when the FortiVoice unit completed the generated report.
<b>Size</b>	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.
4. To view the report in CSV (comma-separated value) file format that can be viewed in a spreadsheet application such as Microsoft Excel or OpenOffice Calc, mark the check box in the corresponding row and click *Download*. On the pop-up menu, select *Download CSV*.

## 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 268.

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

### To view the list of log files and their contents

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

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

2. To download an event, voice, fax, and call center 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 37.

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 6](#).

**Figure 6:** Log message view

#	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 fe
6	2014-02-20	05:00:01	Expired 2' faxes from 'inbox' folder for extension '6003'
7	Date=2014-02-20, Time=09:55:51, Message=Fax from "" <6132259381>' to 'freephone8423': 'receiving FAX failed.		
8	Extra Info: {Status String = Disconnected after permitted		
9	retriesECM = yesError Code = Disconnected after permitted retr		
10	iesFilenames = /var/spool/fax_queue		
11	/incoming		
12	/1392908125. freephone8423.1392908123.2.tif.local		
13	Station ID=8423Remote'		
14	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 268](#).

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 37](#).

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.

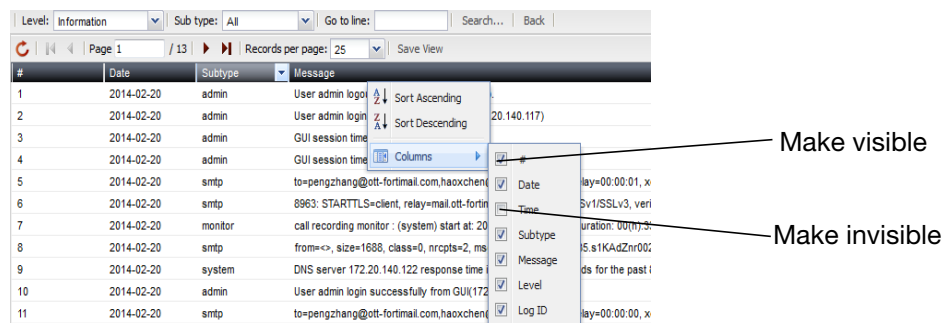
Depending on your currently selected theme:

- 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/Call center*.
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 7: Hiding and showing log columns**



4. Click *Save View*.

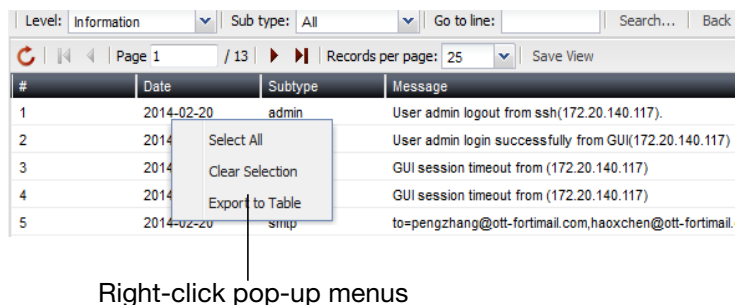
#### To change the order of the columns

1. Go to *Status > Logs > Event/Voice/Queue/Call center*.
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 menu

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

**Figure 8: Using the right-click menus on log reports**



Right-click pop-up menus

**Table 5:** Log report right-click menu options

<b>Select All</b>	Select to select all log messages in the current page, so that you can export all messages to a table.
<b>Clear Selection</b>	Select to deselect one or multiple log messages.
<b>Export to Table</b>	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/Call center*.
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 9:** Log search dialog

FortiVoice  
seconds for the past 9 DNS UDP request

**Event Log Search**

Keyword:

Message:

Log ID:

Time: Zero day and 12 hour(s) before

02/20/14 12

Match condition: Contain

Apply Cancel

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

<b>GUI field</b>	<b>Description</b>
<b>Keyword</b>	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.
<b>Message</b>	Enter all or part of the <i>Message</i> log field.
<b>Log ID</b>	Enter all or part of the log ID in the log message.

<b>Time</b>	Select the time span of log messages to include in the search results.  For example, you might want to search only log messages that were recorded during the two weeks and 8 hours previous to the current date. In that case, you would specify the current date, and also specify the size of the span of time (two weeks and 8 hours) before that date.
<b>Match condition</b>	<ul style="list-style-type: none"> <li>• <i>Contain</i>: searches for the exact match.</li> <li>• <i>Wildcard</i>: supports wildcards in the entered search criteria.</li> </ul>

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 extensions used for the following purposes:

- local
- remote
- ring group
- paging
- virtual number
- conference
- analog
- general voicemail
- fax

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 10:** Viewing directory

Number	Display Name	Location	Department	Type
7701	Operator	Local		Sip
7702	Administrator	Local		Sip
470	470	Local		Sip

<b>GUI field</b>	<b>Description</b>
<b>Download</b>	Select to save all directories or search result.
<b>Number</b>	The extension number. For information on creating extension numbers, see “ <a href="#">Setting up local extensions</a> ” on <a href="#">page 134</a> .

---

<b>Display Name</b>	The name displaying on the extension. This is usually the name of the extension user.
<b>Location</b>	The extension location.
<b>Department</b>	The department to which the extension belongs.
<b>Type</b>	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, GUI appearance, and call data storage
- 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 16.

## 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 42.

### 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 42.

### 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 42.

## 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 41, and “[Editing network interfaces](#)” on page 43.

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

**Figure 11:** Network tab

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

#### GUI field

#### Description

#### Name

Displays the name of the network interface, such as *port1*.

<b>Type</b>	Displays the interface type: physical, VLAN, redundant, or loopback. For details, see <a href="#">“About FortiVoice logical interfaces”</a> on page 41.
<b>IP/Netmask</b>	Displays the IP address and netmask of the network interface.
<b>IPv6/Netmask</b>	Displays the IPv6 address and netmask of the network interface. For more information about IPv6 support, see <a href="#">“About IPv6 Support”</a> on page 40.
<b>Access</b>	Displays the administrative access and phone user access that are enabled on the network interface, such as HTTPS for the web-based manager.
<b>Status</b>	<p>Indicates the <b>up</b> (available) or <b>down</b> (unavailable) administrative status for the network interface.</p> <ul style="list-style-type: none"> <li>• <i>Green up arrow</i>: The network interface is up and can receive traffic.</li> <li>• <i>Red down arrow</i>: The network interface is down and cannot receive traffic.</li> </ul> <p>To change the administrative status (that is, bring up or down a network interface), see <a href="#">“Editing network interfaces”</a> on page 43.</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 52.

#### 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:

**Figure 12: Edit Interface dialog**

**Edit Interface**

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

---

**Addressing Mode**

Manual

IP/Netmask:  /

IPv6/Netmask:  /

DHCP

---

Access  HTTPS  PING  HTTP

SSH  SNMP  TELNET

MTU  Override default MTU value (1500)

(bytes)

Administrative status  Up  Down

---

**Figure 13: Creating logical interfaces**

**Edit Interface**

Interface name:

Type:  ▼

Interface:  ▼

VLAN ID:

---

**Addressing Mode**

Manual

IP/Netmask:  /

IPv6/Netmask:  /

DHCP

---

Access  HTTPS  PING  HTTP

SSH  SNMP  TELNET

MTU  Override default MTU value (1500)

(bytes)

Administrative status  Up  Down

---

**GUI field**

**Description**

**Interface Name**

If you are editing an existing interface, this field displays the name (such as port2) and media access control (MAC) address for this network interface.

If you are creating a logical interface, enter a name for the interface.

---

**Type**

If you are creating a logical interface, select which type of interface you want to create. For information about logical interface types, see [“About FortiVoice logical interfaces” on page 41](#).

- *VLAN*: If you want to create a VLAN subinterface, select the interface for which you want to create the subinterface. Then specify a VLAN ID. Valid VLAN ID numbers are from 1 to 4094, while 0 is used for high priority frames, and 4095 is reserved.
- *Redundant*: If you want to create a redundant interface, select the interface members from the available interfaces. Usually, you need to include two or more interfaces as the redundant interface members.
- *Loopback*: If you want to add a loopback interface, select the Loopback type and the interface name will be automatically reset to “loopback”. You can only add one loopback interface on the FortiVoice unit.

---

**Addressing Mode**

- *Manual*: Select to enter the IP address or IPv6 address and netmask for the network interface in *IP/Netmask* or *IPv6/Netmask*.
  - *DHCP*: Select and click *Update request* to retrieve a dynamic IP address using DHCP.
-

---

**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 124](#).

- **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 42](#).

- **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 52](#).

---

**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:

- *Up*: Enable (that is, bring up) the network interface so that it can send and receive traffic.
  - *Down*: Disable (that is, bring down) the network interface so that it cannot send or receive traffic.
- 

## Configuring static routes

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

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

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

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

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

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

### To view or configure static routes

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

**Figure 14:** 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	

---

**GUI field****Description**

---

**Destination IP/Netmask**

Displays the destination IP address and subnet of packets subject to the static route. A setting of 0.0.0.0/0.0.0 indicates that the route matches all destination IP addresses.

---

**Interface**

The interface that this route applies to.

---

---

<b>Gateway</b>	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 15:**DHCP server configuration

<b>GUI field</b>	<b>Description</b>
<b>Network Interface Setting</b>	
<b>ID</b>	The system will generate an ID for this configuration. This is view only.
<b>Enabled</b>	Select to enable the DHCP server.
<b>Interface</b>	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 55.
<b>Gateway</b>	Enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
<b>DNS options</b>	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 48.
<b>Domain</b>	Enter the domain that the DHCP server assigns to its clients.
<b>Netmask</b>	Enter the netmask of the addresses that the DHCP server assigns.
<b>Advanced Setting</b>	

<b>TFTP server (Opt66)</b>	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 <a href="#">“Configuring SIP phone auto-provisioning” on page 112.</a>
<b>Lease time (Seconds)</b>	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.
<b>Vender Class Identifier option</b>	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 &gt; PBX Status &gt; DHCP &gt; VCI.</i>
<b>VCI string</b>	Enter the phone VCI string supplied by the vendor.
<b>DHCP IP Range</b>	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.
<b>DHCP Excluded IP Range</b>	Click <i>New</i> to enter a range of IP addresses that this server should not assign to the DHCP clients.
<b>Reserved IP Address</b>	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 16:** 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

<b>GUI field</b>	<b>Description</b>
<b>Stop</b>	Click to stop the packet capture.
<b>Download</b>	When the capture is complete, click <i>Download</i> to save the packet capture file to your hard disk for further analysis.
<b>Name</b>	The name of the packet capture file.
<b>Status</b>	The status of the packet capture process, <i>Complete</i> or <i>Running</i> .
<b>Size</b>	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 17:** 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	<a href="#">super_admin_prof</a>
<input checked="" type="checkbox"/>	admin_temp	-	Local		0.0.0.0/0::/0	<a href="#">super_admin_prof</a>
<input checked="" type="checkbox"/>	akaye	-	LDAP	<a href="#">corp_ldap_ottawa</a>	0.0.0.0/0::/0	<a href="#">read_only</a>
<input checked="" type="checkbox"/>	dbodnariuc	-	LDAP	<a href="#">corp_ldap_ottawa</a>	0.0.0.0/0::/0	<a href="#">super_admin_prof</a>

GUI field	Description
<b>Name</b>	Displays the name of the administrator account.
<b>Extension</b>	Displays the extension associated with the administrator account.
<b>Authentication Type</b>	The administrator authentication type: <i>Local</i> or <i>LDAP</i> .
<b>Authentication Profile</b>	The LDAP authentication profile. For more information, see “Configuring LDAP profiles” on page 125.
<b>Trusted Hosts</b>	Displays the IP address and netmask from which the administrator can log in.
<b>Admin Profile</b>	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 18:** New Administrator dialog

The screenshot shows the 'New Administrator' dialog box with the following fields and controls:

- Administrator:** A text input field.
- Single sign-on manager:** A dropdown menu showing '470 (470) (sip)', with 'New...', 'Edit...', and an information icon.
- Managed departments:** A '>>' button.
- Authentication type:** A dropdown menu showing 'Local'.
- Create password:** A checked checkbox with a right-pointing arrow.
- Trusted hosts:** A text input field containing '0.0.0.0 / 0', with '+' and '-' buttons.
- Admin profile:** A dropdown menu showing 'monitor\_prof', with 'New...' and 'Edit...' buttons.
- Select language:** A dropdown menu showing '--Default--'.
- Select theme:** A dropdown menu showing 'Red Grey', with a 'Use Current' button.
- Buttons:** 'Create' and 'Cancel' buttons at the bottom.

<b>GUI field</b>	<b>Description</b>
<b>Administrator</b>	<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>
<b>Single sign-on manager</b>	<p>Select 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 <a href="#">“Configuring IP extensions” on page 134</a>.</p>
<b>Managed departments</b>	<p>This option appears after you select an extension for the administrator account.</p> <p>If you want to configure an administrator to manage call center departments, click &gt;&gt; and select the departments for the administrator. Click <i>Done</i> when you are finished.</p> <p>For information on setting up call center departments, see <a href="#">“Configuring agents” on page 207</a>.</p> <p>With this configuration, an administrator can log into the FortiVoice unit and view the following information of the managed departments:</p> <ul style="list-style-type: none"><li>• recorded calls</li><li>• call center reports</li><li>• call queues</li><li>• call queue reports</li></ul> <p>The administrator can also click <i>User Portal</i> to go to the user web portal and click <i>Administrator</i> to return to the administration page.</p> <p>Note that in the administrator’s <i>Admin profile</i>, <i>Call center management</i> and <i>Storage recorded calls</i> must be <i>Read Only</i> or <i>Read-Write</i>. For details, see <a href="#">“Configuring administrator profiles” on page 55</a>.</p>

<b>Authentication type</b>	Select an administrator authentication type: <i>Local</i> or <i>LDAP</i> .
<b>Create password</b>	<p>Click to configure account login information.</p> <ul style="list-style-type: none"> <li><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>. <b>Caution:</b> 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.</li> <li><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>.</li> </ul>
<b>LDAP profile</b>	If you select <i>LDAP</i> for <i>Authentication type</i> , select an LDAP authentication profile. For more information, see <a href="#">“Configuring LDAP profiles” on page 125</a> .
<b>Trusted Hosts</b>	<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 <code>0.0.0.0/0.0.0.0</code>.</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 <code>192.168.1.0/255.255.255.0</code>.</p> <p><b>Note:</b> 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><b>Note:</b> For information on restricting administrative access protocols that can be used by these hosts, see <a href="#">“Editing network interfaces” on page 43</a>.</p> <p>Click the + sign to add additional IP addresses or subnets from which the administrator can log in.</p>
<b>Admin profile</b>	<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 <a href="#">“Configuring administrator profiles” on page 55</a>.</p>
<b>Select language</b>	Select this administrator account's preference for the display language of the web-based manager.

---

<b>Select theme</b>	Select this administrator account's preference for the display theme or click <i>Use Current</i> to choose the theme currently in effect.  The administrator may switch the theme at any time during a session by clicking <i>Next Theme</i> .
---------------------	--

---

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 58](#).

This section contains the following topics:

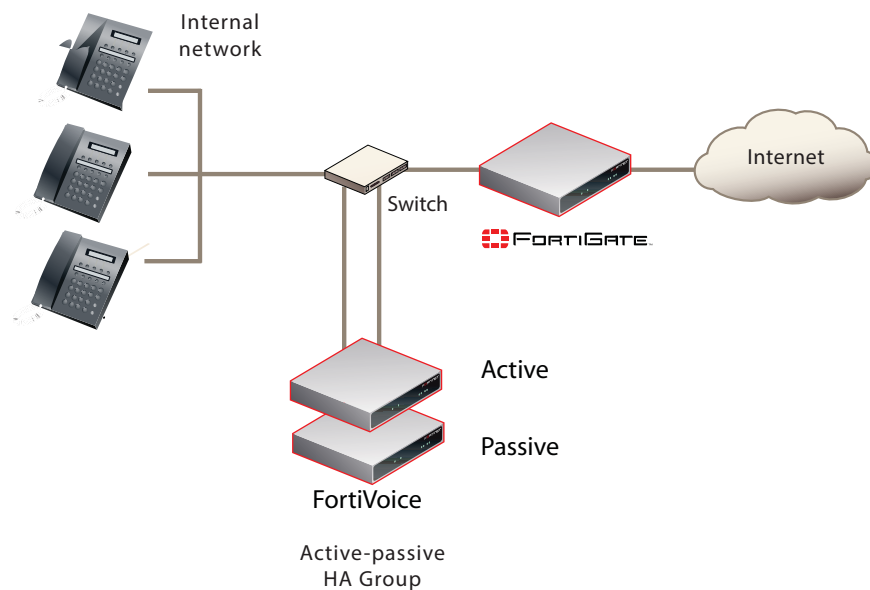
- [About high availability](#)
- [About the heartbeat and synchronization](#)
- [How to use HA](#)
- [Monitoring the HA status](#)
- [Configuring service-based failover](#)
- [Example: Failover scenarios](#)

## 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 57.
- 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 19:**Active-passive HA group



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

Communications between HA members occur through the heartbeat and synchronization connection. For details, see [“About the heartbeat and synchronization”](#) on page 57.

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 57.

For instructions of how to enable and configure HA, see [“How to use HA”](#) on page 58.



## 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 65.

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 57.
- 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 61. 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 70.

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 71.

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 72 and “Configuring alert email” on page 282.

### 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

<b>Host name</b>	The host name distinguishes members of the cluster.
<b>Static route</b>	Static routes are not synchronized because the HA units may be in different networks (see “Configuring static routes” on page 47).

**Table 6:** HA settings not synchronized

<b>Interface configuration</b>	<p>Each FortiVoice unit in the HA group must be configured with different network interface settings for connectivity purposes. For details, see “<a href="#">Configuring the network interfaces</a>” on page 42.</p> <p>Exceptions include some active-passive HA settings which affect the interface configuration for failover purposes. These settings are synchronized.</p>
<b>Main HA configuration</b>	<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 “<a href="#">Configuring the HA mode and group</a>” on page 62.</p>
<b>HA service monitoring configuration</b>	<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 “<a href="#">Configuring service-based failover</a>” on page 68.</p> <p><b>Note:</b> 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>
<b>System appearance</b>	<p>The appearance settings you configured under <i>System &gt; Configuration &gt; 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 56](#).
  - 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 68](#).
4. Monitor the status of each group member. For details, see [“Monitoring the HA status” on page 59](#). 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 270](#).

## Monitoring the HA status

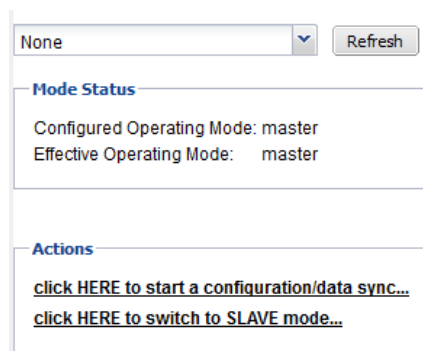
The *Status* tab in the *High Availability* submenu shows the configured HA mode of operation of a FortiVoice unit in an HA group. You can also manually initiate synchronization and reset the HA mode of operation. A reset may be required if a FortiVoice unit’s effective HA mode of operation differs from 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 58](#).

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

**Figure 20:** Active-passive HA status (primary unit)



**Table 7:** Viewing HA status

<b>GUI item</b>	<b>Description</b>
<b>Mode Status</b>	
<b>Configured Operating Mode</b>	<p>Displays the HA operating mode that you configured, either:</p> <ul style="list-style-type: none"><li>• <i>master</i>: Configured to be the primary unit of an active-passive group.</li><li>• <i>slave</i>: Configured to be the secondary unit of an active-passive group.</li></ul> <p>For information on configuring the HA operating mode, see <a href="#">“Mode of operation” on page 64</a>.</p> <p>After a failure, the FortiVoice unit may not be acting in its configured HA operating mode. For details, see <a href="#">“Effective Operating Mode” on page 60</a>.</p>
<b>Effective Operating Mode</b>	<p>Displays the mode that the unit is currently operating in, either:</p> <ul style="list-style-type: none"><li>• <i>master</i>: Acting as primary unit.</li><li>• <i>slave</i>: Acting as secondary unit.</li><li>• <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 <a href="#">“On failure” on page 64</a>.</li><li>• <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 <a href="#">“On failure” on page 64</a>.</li></ul> <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 <a href="#">Table 8</a>.</p> <p>For information on restoring the FortiVoice unit to an effective HA operating mode that matches the configured operating mode, see <a href="#">“click HERE to restore configured operating mode” on page 61</a>.</p>
<b>Daemon Status</b>	<p>This option appears only for secondary units in active-passive HA groups.</p>

**Table 7:** Viewing HA status

<b>GUI item</b>	<b>Description</b>
<b>Monitor</b>	<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 <a href="#">“HA base port” on page 65</a>.</p>
<b>Configuration</b>	<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 <a href="#">“Configuration settings that are not synchronized” on page 57</a>.</p>
<b>Data</b>	<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>
<b>Actions</b>	
<b>click HERE to start a configuration/data sync</b>	<p>Click to manually initiate synchronization of the configuration and call data. For information on items that are not synchronized, see <a href="#">“Configuration settings that are not synchronized” on page 57</a>.</p>
<b>click HERE to restore configured operating mode</b>	<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 <i>slave</i>, 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><b>Note:</b> 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 57.

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 21:** 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:** This section includes dropdown menus for 'Mode of operation' (set to 'master') and 'On failure' (set to 'switch off'), and a text field for 'Shared password' (set to 'change\_me'). There are 'Apply' and 'Cancel' buttons at the bottom.

**Interface:** This section contains a table with columns: Port, Heartbeat Status, Peer IP Address, Virtual IP Action, Virtual IP Address, and Port Monitor. The table lists four ports: port1, port2, port3, and port4.

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:** This section contains a table with columns: Name, Remote IP, Port, Timeout, Interval, Retries, and Enabled. The table lists four service monitors: Remote HTTP, SIP UDP, Interface monitor, and Local hard drives.

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 63
  - “Configuring the advanced options” on page 64
  - “Configuring interface monitoring” on page 65
  - “Configuring service-based failover” on page 68
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

<b>GUI item</b>	<b>Description</b>
<b>Mode of operation</b>	<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"><li>• <i>off</i>: The FortiVoice unit is not operating in HA mode.</li><li>• <i>master</i>: The FortiVoice unit is the primary unit in an active-passive HA group.</li><li>• <i>slave</i>: The FortiVoice unit is the secondary unit in an active-passive HA group.</li></ul>
<b>On failure</b>	<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"><li>• <i>switch off</i>: Do not process phone calls or join the HA group until you manually select the effective operating mode (see “<a href="#">click HERE to start a configuration/data sync</a>” on page 61 and “<a href="#">click HERE to restore configured operating mode</a>” on page 61).</li><li>• <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.</li><li>• <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 “<a href="#">click HERE to restore configured operating mode</a>” on page 61.</li></ul> <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 <a href="#">Table</a> . For information on configuring service/interface monitoring, see “<a href="#">Configuring service-based failover</a>” on page 68.</p> <p>This option appears only if “<a href="#">Mode of operation</a>” is <i>master</i>.</p>
<b>Shared password</b>	<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

<b>GUI item</b>	<b>Description</b>
<b>HA base port</b>	<p>Keep the default TCP port number (20000) that will be used for:</p> <ul style="list-style-type: none"><li>• the heartbeat signal</li><li>• synchronization control</li><li>• data synchronization</li><li>• configuration synchronization</li></ul> <p><b>Note:</b> In addition to configuring the heartbeat, you can configure service monitoring. For details, see <a href="#">“Configuring service-based failover”</a> on page 68.</p> <p><b>Note:</b> In addition to automatic immediate and periodic configuration synchronization, you can also manually initiate synchronization. For details, see <a href="#">“click HERE to start a configuration/data sync”</a> on page 61.</p>
<b>Heartbeat lost threshold</b>	<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><b>Note:</b> If the failure detection time is too short, the secondary unit may falsely detect a failure when during periods of high load.</p> <p><b>Caution:</b> 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>
<b>Remote services as heartbeat</b>	<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><b>Note:</b> 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><b>Note:</b> 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 42.



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.

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

---

<b>GUI item</b>	<b>Description</b>
<b>Heartbeat status</b>	<p>Specify if this interface will be used for HA heartbeat and synchronization.</p> <ul style="list-style-type: none"> <li>• <b>Disable</b> Do not use this interface for HA heartbeat and synchronization.</li> <li>• <b>Primary</b> Select the primary network interface for heartbeat and synchronization traffic. For more information, see <a href="#">“About the heartbeat and synchronization” on page 57.</a> 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.</li> <li>• <b>Secondary</b> Select the secondary network interface for heartbeat and synchronization traffic. For more information, see <a href="#">“About the heartbeat and synchronization” on page 57.</a> 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.</li> </ul> <p><b>Caution:</b> 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><b>Note:</b> 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>
<b>Peer IP address</b>	<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 <a href="#">“About the heartbeat and synchronization” on page 57.</a></p>

<b>GUI item</b>	<b>Description</b>
<b>Virtual IP action</b>	<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"> <li>• <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 “<a href="#">Configuring the network interfaces</a>” on page 42.</li> <li>• <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 <b>and</b> the virtual.</li> </ul>
<b>Virtual IP address</b>	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 62. For information on the effective HA operating mode, see “[Monitoring the HA status](#)” on page 59.

### 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:

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

<b>GUI item</b>	<b>Description</b>
<b>Timeout</b>	Enter the timeout period for one connection test.
<b>Interval</b>	Enter the frequency of the tests.
<b>Retries</b>	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:

<b>GUI item</b>	<b>Description</b>
<b>Enable</b>	Select to enable SIP UDP service.
<b>Name</b>	Displays the service name.
<b>Remote IP</b>	Enter the peer IP address.
<b>Port</b>	Enter the port number of the peer SIP UDP service.
<b>Timeout</b>	Enter the timeout period for one connection test.
<b>Interval</b>	Enter the frequency of the tests.
<b>Retries</b>	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:

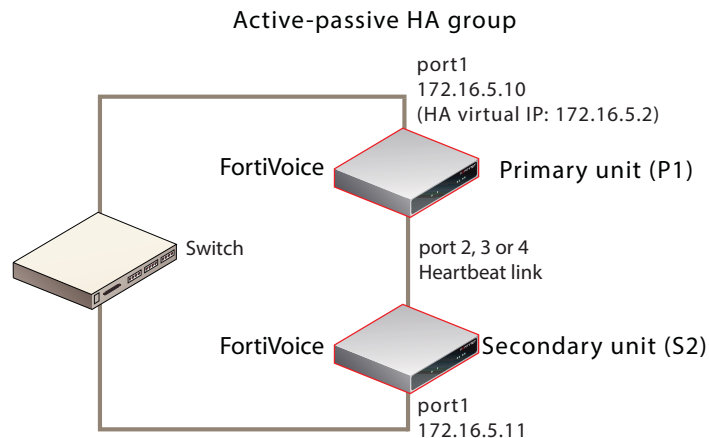
<b>GUI item</b>	<b>Description</b>
<b>Enable</b>	<p>Select to enable local hard drive monitoring. Interface monitoring is enabled when you configure interface monitoring. See <a href="#">“Configuring interface monitoring”</a> on page 65.</p> <p>Network interface monitoring tests all active network interfaces whose:</p> <ul style="list-style-type: none"> <li>• <a href="#">“Virtual IP action”</a> setting is <i>not ignore</i></li> <li>• <a href="#">“Configuring interface monitoring”</a> setting is enabled</li> </ul> <p>For details, see <a href="#">“Configuring interface monitoring”</a> on page 65 and <a href="#">“Virtual IP action”</a> on page 68.</p>
<b>Interval</b>	Enter the frequency of the test.
<b>Retries</b>	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 22](#). 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 22:**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.

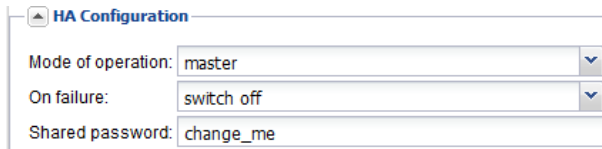
```
The following event has occurred
'MASTER heartbeat disappeared'
The state changed from 'SLAVE' to 'MASTER'
```

- 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 23:** 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 61).

- 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 61.

## 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 22 on page 70](#), 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 64](#). For information about remote service monitoring, see ["Configuring service-based failover" on page 68](#).

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

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

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

This is the HA machine at 172.16.5.11.

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

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

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

This is the HA machine at 172.16.5.10.

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

The state changed from 'MASTER' to 'FAILED'

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

## Recovering from a network connection failure

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

### To return to normal operation after the heartbeat link fails

1. Reconnect power to the switch.

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

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

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

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

4. P1 logs the event.

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

This is the HA machine at 172.16.5.10.

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

The state changed from 'FAILED' to 'SLAVE'

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

7. Check for synchronization messages.

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

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

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

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

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

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

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

This topic includes:

- Configuring the time and date
- Configuring system options
- Configuring SNMP queries and traps
- Configuring email settings
- Customizing the GUI appearance
- Selecting the call data storage location

## 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 24:** Time Settings tab

Time Settings

System time: 02/24/2014 11:21:26 Refresh

Time zone: (GMT-5:00)Eastern Time(US & Canada) [v]  
 Automatically adjust clock for daylight saving time changes

Synchronize with NTP Server (may take up to several minutes)  
Server: pool.ntp.org [v]  
Sync Interval: 60 (minutes)

Set date 02/24/14 Time 11 21 26

Apply Cancel

<b>GUI field</b>	<b>Description</b>
<b>System time</b>	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.

<b>Time zone</b>	<p>Select the time zone in which the FortiVoice unit is located.</p> <ul style="list-style-type: none"> <li>• <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.</li> </ul> <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 <a href="#">Table 11 on page 77</a>.</p>
<b>Synchronize with NTP Server</b>	<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"> <li>• <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 <a href="http://www.ntp.org">http://www.ntp.org</a>.</li> <li>• <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.</li> </ul> <p>Depending on your network traffic, it may take some time for the FortiVoice unit to synchronize its time with the NTP server.</p>
<b>Set date</b>	<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

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

<b>Code</b>	<b>Time Zone</b>
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 25: Options tab**

**Configuration Options**

Idle timeout:  (1-480 minutes)

**Password / PIN Policy**

Enable

Minimum password length:

Password must contain:

- Uppercase letter
- Lowercase letter
- Number (0-9)
- Non alphanumeric character

Apply password policy to:

- Administrators
- SIP users

Minimum PIN length:

PIN must contain:

- Number (0-9)
- PIN special

Apply PIN policy to:

- Voicemail users

**Administration Ports**

HTTP port number:

HTTPS port number:

SSH port number:

TELNET port number:

Web action host/IP:

---

<b>GUI field</b>	<b>Description</b>
<b>Idle timeout</b>	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.

---

---

**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 134](#).

- *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 call report and notification email templates” on page 109](#).

---

3. Click *Apply*.

## Configuring SNMP queries and traps

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

To monitor FortiVoice system information and receive FortiVoice traps, you must compile Fortinet proprietary MIBs as well as Fortinet-supported standard MIBs into your SNMP manager. RFC support includes support for most of [RFC 2665](#) (Ethernet-like MIB) and most of [RFC 1213](#) (MIB II). For more information, see “[FortiVoice MIBs](#)” on page 87.

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

The FortiVoice SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Before you can use its SNMP queries, you must enable SNMP access on the network interfaces that SNMP managers will use to access the FortiVoice unit. For more information, see “[Editing network interfaces](#)” on page 43.

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:

<b>GUI field</b>	<b>Description</b>
<b>SNMP agent enable</b>	Enable to activate the FortiVoice SNMP agent. This must be enabled to accept queries from SNMP managers or send traps from the FortiVoice unit.
<b>Description</b>	Enter a descriptive name for the FortiVoice unit.
<b>Location</b>	Enter the location of the FortiVoice unit.
<b>Contact</b>	Enter administrator contact information.
<b>SNMP Threshold</b>	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> .
<b>Trap Type</b>	Displays the type of trap, such as <i>CPU Usage</i> .
<b>Trigger</b>	You can enter either the percent of the resource in use or the number of times the trigger level must be reached before it is triggered.  For example, using the default value, if the mailbox disk is 90% or more full, it will trigger.
<b>Threshold</b>	Sets the number of triggers that will result in an SNMP trap.  For example, if the CPU level exceeds the set trigger percentage once before returning to a lower level, and the threshold is set to more than one, an SNMP trap will not be generated until that minimum number of triggers occurs during the sample period.
<b>Sample Period(s)</b>	Sets the time period in seconds during which the FortiVoice unit SNMP agent counts the number of triggers that occurred.  This value should <b>not</b> be less than the <i>Sample Freq(s)</i> value.
<b>Sample Freq(s)</b>	Sets the interval in seconds between measurements of the trap condition. You will not receive traps faster than this rate, depending on the selected sample period.  This value should be less than the <i>Sample Period(s)</i> value.
<b>Community</b>	Displays the list of SNMP communities (for SNMP v1 and v2c) added to the FortiVoice configuration. For information on configuring a community, see either <a href="#">“Configuring email settings”</a> or <a href="#">“Configuring an SNMP v3 user”</a> on page 86.
<b>Name</b>	Displays the name of the SNMP community. The SNMP Manager must be configured with this name.
<b>Status</b>	A green check mark icon indicates that the community is enabled.
<b>Queries</b>	A green check mark icon indicates that queries are enabled.
<b>Traps</b>	A green check mark icon indicates that traps are enabled.

<b>User</b>	Displays the list of SNMP v3 users added to the FortiVoice configuration. For information on configuring a v3 user, see <a href="#">“Configuring an SNMP v3 user” on page 86</a> .
<b>Name</b>	Displays the name of the SNMP v3 user. The SNMP Manager must be configured with this name.
<b>Status</b>	A green check mark icon indicates that the user is enabled.
<b>Queries</b>	A green check mark icon indicates that queries are enabled.
<b>Traps</b>	A green check mark icon indicates that traps are enabled.
<b>Security Level</b>	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:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	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.
<b>Enable</b>	Enable to send traps to and allow queries from the community's SNMP managers.
<b>Community Hosts</b>	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.
<b>IP Address</b>	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.
<b>Delete (button)</b>	Click to remove this SNMP manager.
<b>Create (button)</b>	Click to add a new default entry to the <i>Hosts</i> list that you can edit as needed.

<b>Queries</b>	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.
<b>Traps</b>	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.
<b>SNMP Event</b>	<p>Enable each SNMP event for which the FortiVoice unit should send traps to the SNMP managers in this community.</p> <p><b>Note:</b> 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:

<b>GUI field</b>	<b>Description</b>
<b>User name</b>	Enter a name to identify the SNMP user. If you are editing an existing user, you cannot change the name.
<b>Enable</b>	Enable to send traps to and allow queries from the user's SNMP managers.
<b>Security level</b>	<p>Choose one of the three security levels:</p> <ul style="list-style-type: none"> <li>• <i>No authentication, no privacy</i>: This option is similar to SNMP v1 and v2.</li> <li>• <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).</li> <li>• <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.</li> </ul>

<b>Authentication Protocol</b>	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.
<b>Privacy protocol</b>	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.
<b>Notification Hosts</b>	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.
<b>IP Address</b>	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.
<b>Delete</b> (button)	Click to remove this SNMP manager.
<b>Create</b> (button)	Click to add a new default entry to the <i>Hosts</i> list that you can edit as needed.
<b>Queries</b>	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.
<b>Traps</b>	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.
<b>SNMP Event</b>	<p>Enable each SNMP event for which the FortiVoice unit should send traps to the SNMP managers.</p> <p><b>Note:</b> 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

<b><i>MIB file name</i></b>	<b><i>Description</i></b>
<b>FortiVoice.mib</b>	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 88.

### 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

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

<b>MIB field</b>	<b>Description</b>
<b>fvSysModel</b>	FortiVoice model number, such as 400 for the FortiVoice-400.
<b>fvSysSerial</b>	FortiVoice unit serial number.
<b>fvSysVersion</b>	The firmware version currently running on the FortiVoice unit.
<b>fvSysCpuUsage</b>	The current CPU usage (%).
<b>fvSysMemUsage</b>	The current memory utilization (%).
<b>fvSysLogDiskUsage</b>	The log disk usage (%).
<b>fvSysStorageDiskUsage</b>	The storage disk usage (%).
<b>fvSysEventCode</b>	System component events.
<b>fvSysload</b>	Current system load.
<b>fvSysHA</b>	<ul style="list-style-type: none"><li>fvHAMode: Configured HA operating mode.</li><li>fvHAEffectiveMoce: Effective HA operating mode.</li></ul>
<b>fmIHAEventId</b>	HA event type ID.
<b>fmIHAUnitIp</b>	Unit IP address where the event occurs.
<b>fmIHAEventReason</b>	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 134.

### To configure email settings

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

**Figure 26:** Mail server settings

**Local Host**

Host name:

Local domain name:

---

**Mail Queue**

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

Time interval for retry (10-120 minutes):

---

**Relay Server**

Relay server name:

Relay server port:

Use SMTPs

**Authentication Required**

---

[Customize email template](#)

<b>GUI field</b>	<b>Description</b>
<b>Local Host</b>	
<b>Host name</b>	Enter the host name of the FortiVoice unit, such as <code>fortivoice-200D</code> .
<b>Local domain name</b>	Enter the local domain name of the FortiVoice unit, such as <code>example.com</code> .
<b>Mail Queue</b>	
<b>Maximum time for email in queue (1-240 hours)</b>	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.
<b>Time interval for retry (10-120 minutes)</b>	Enter the number of minutes between delivery retries for email messages in the deferred mail queues.
<b>Relay Server</b>	
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.	
<b>Relay server name</b>	Enter the domain name of an SMTP relay.
<b>Relay server port</b>	Enter the TCP port number on which the SMTP relay listens. This is typically provided by your Internet service provider (ISP).

<b>Use SMTPs</b>	<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>
<b>Authentication Required:</b>	<p>Select the checkbox and click the arrow to expand the section and configure:</p> <ul style="list-style-type: none"> <li>• <i>User name</i>: Enter the name of the FortiVoice unit's account on the SMTP relay.</li> <li>• <i>Password</i>: Enter the password for the FortiVoice unit's user name.</li> <li>• <i>Authentication type</i>: Available SMTP authentication types include: <ul style="list-style-type: none"> <li>• <i>AUTO</i> (automatically detect and use the most secure SMTP authentication type supported by the relay server)</li> <li>• <i>PLAIN</i> (provides an unencrypted, scrambled password)</li> <li>• <i>LOGIN</i> (provides an unencrypted, scrambled password)</li> <li>• <i>DIGEST-MD5</i> (provides an encrypted hash of the password)</li> <li>• <i>CRAM-MD5</i> (provides an encrypted hash of the password, with hash replay prevention, combined with a challenge and response mechanism)</li> </ul> </li> </ul>
<b>Customize email template</b>	<p>View and reword the default email history report and notification email templates. For more information, see <a href="#">"Customizing call report and notification email templates"</a> on page 109.</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 27:** Appearance tab

<b>GUI field</b>	<b>Description</b>
<b>Administration interface</b>	
<b>Product name</b>	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.
<b>Product icon</b>	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.
<b>Top logo</b>	<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><b>Note:</b> 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>
<b>Default UI language</b>	<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 <a href="#">“Configuring administrator accounts” on page 52.</a></p>
<b>Voicemail interface</b>	

<b>Voicemail login</b>	Enter a word or phrase that will appear on top of the voicemail login page, such as Voicemail Login.
<b>Login user name hint</b>	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.
<b>Voicemail theme</b>	Select a theme for the voicemail GUI.
<b>Voicemail UI language</b>	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
<b>Voicemail top logo</b>	<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><b>Note:</b> 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.

## Selecting the call data storage location

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

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

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



If the FortiVoice unit is a member of an active-passive HA group, and the HA group stores call data on a remote NAS server, disable call data synchronization to prevent duplicate call data traffic. For details, see [“Configuring the HA mode and group” on page 62](#).



If you store the call data on a remote NAS device, you cannot back up the data. You can only back up the call data stored locally on the FortiVoice hard disk. For information about backing up call data, see [“Backing up configuration” on page 103](#).

#### Tested and Supported NFS servers

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

#### Untested NFS servers

- Buffalo TeraStation
- Cisco Linksys NAS server

#### Non-Supported NFS Servers

- Windows 2003 R2 /Windows 2008 Service for NFS

#### To configure call data storage

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

<b>GUI field</b>	<b>Description</b>
<b>NAS section</b>	
<b>Local</b>	Select to store call data on the FortiVoice unit's local disk or RAID.
<b>NAS server</b>	Select to store call data on a remote network attached storage (NAS) server.
<b>Test</b> (button)	Click to verify the NAS server settings are correct and that the FortiVoice unit can access that location. The test action basically tries to discover, login, mount, and unmount the remote device.  This button is available only when <i>NAS server</i> is selected.

<b>Protocol</b>	<p>Select a type of the NAS server:</p> <ul style="list-style-type: none"> <li>• <i>NFS</i>: To configure a network file system (NFS) server. For this option, enter the following information: <ul style="list-style-type: none"> <li>• <i>Hostname/IP address</i>: the IP address or fully qualified domain name (FQDN) of the NFS server.</li> <li>• <i>Port</i>: the TCP port number on which the NFS server listens for connections.</li> <li>• <i>Directory</i>: the directory path of the NFS export on the NAS server where the FortiVoice unit will store call data.</li> </ul> </li> <li>• <i>iSCSI Server</i>: To configure an Internet SCSI (Small Computer System Interface) server. For this option, enter the following information: <ul style="list-style-type: none"> <li>• <i>Username</i>: the user name of the FortiVoice unit's account on the iSCSI server.</li> <li>• <i>Password</i>: the password of the FortiVoice unit's account on the iSCSI server.</li> <li>• <i>Hostname/IP address</i>: the IP address or fully qualified domain name (FQDN) of the iSCSI server.</li> <li>• <i>Port</i>: the TCP port number on which the iSCSI server listens for connections.</li> <li>• <i>Encryption key</i>: the key that will be used to encrypt data stored on the iSCSI server. Valid key lengths are between 6 and 64 single-byte characters.</li> <li>• <i>iSCSI ID</i>: the iSCSI identifier in the format expected by the iSCSI server, such as an iSCSI Qualified Name (IQN), Extended Unique Identifier (EUI), or T11 Network Address Authority (NAA).</li> </ul> </li> </ul> <p><i>Status</i>: When available, it indicates if the iSCSI share was successfully mounted on the FortiVoice unit's file system. This field appears only after you configure the iSCSI share and click <i>Apply</i>. <i>Status</i> may take some time to appear if the iSCSI server is slow to respond.</p> <p>If <i>Not mounted</i> appears, the iSCSI share was not successfully mounted. Verify that the iSCSI server is responding and the FortiVoice unit has both read and write permissions on the iSCSI server.</p>
<b>Refresh</b> (button)	This button appears when you configure an iSCSI server. Click it to update the information in the <i>Status</i> field.
<b>Click here to format this device</b>	These two links appear when you configure an iSCSI server and click <i>Apply</i> .
<b>Click here to check file system on this device</b>	Click a link to initiate the described action (that is, format the device or check its file system). A message appears saying the action is being executed. Click OK to close the message and click <i>Refresh</i> to see a <i>Status</i> update.
	<b>Note:</b> If the iSCSI disk has never been formatted, the FortiVoice unit needs to format it before it can be used. If the disk has been formatted before, you do not need to format it again, unless you want to wipe out the data on it.

## 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"><li>the web-based manager (HTTPS connections only)</li><li>phone user web interface (HTTPS connections only)</li><li>phone and FortiVoice unit (TLS and SRTP connections only), see <a href="#">“Configuring SIP profiles” on page 119</a>.</li></ul> For details, see <a href="#">“Managing local certificates” on page 96</a> .
CA certificates	The FortiVoice unit uses CA certificates to authenticate the PKI users, including administrators and phone users. For details, see <a href="#">“Managing certificate authority certificates” on page 102</a> .
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.

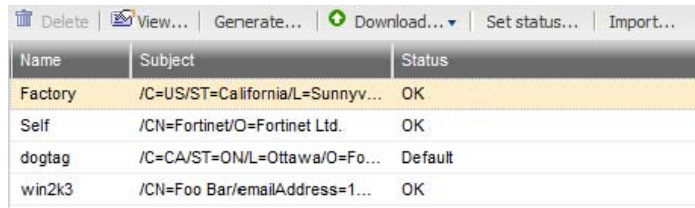
FortiVoice units require a local server certificate that it can present when clients request secure connections, including:

- 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 28:** 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

<b>GUI field</b>	<b>Description</b>
<b>View</b>	Select a certificate and click <i>View</i> to display its issuer, subject, and range of dates within which the certificate is valid.
<b>Generate</b>	Click to generate a local certificate request. For more information, see <a href="#">“Generating a certificate signing request” on page 98.</a>
<b>Download</b>	Click the row of a certificate file or certificate request file in order to select it, then click this button and select either: <ul style="list-style-type: none"><li>• <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 <a href="#">“Downloading a certificate signing request” on page 100.</a></li><li>• <i>Download PKCS12 File</i>: Download a PKCS #12 (.p12) file. For details, see <a href="#">“Downloading a PKCS #12 certificate” on page 102.</a></li></ul>
<b>Set status</b>	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.  This button is not available if the selected certificate is already the “default.”
<b>Import</b>	Click to import a signed certificate for local use. For more information, see <a href="#">“Importing a certificate” on page 101.</a>

## 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 101.](#)
- 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 97.

### To generate a certificate request

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

**Figure 29:** 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:  ▾

<b>GUI field</b>	<b>Description</b>
<b>Certification name</b>	Enter a unique name for the certificate request, such as fvlocal.
<b>Subject Information</b>	Information that the certificate is required to contain in order to uniquely identify the FortiVoice unit.

<b>ID type</b>	<p>Select the type of identifier to be used in the certificate to identify the FortiVoice unit:</p> <ul style="list-style-type: none"> <li>• Host IP</li> <li>• Domain name</li> <li>• E-mail</li> </ul> <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"> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> </ul>
<b>IP</b>	<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>
<b>Domain name</b>	<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 <a href="#">“Configuring the network interfaces” on page 42</a> and <a href="#">“Configuring DNS” on page 48</a>.</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>
<b>E-mail</b>	<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>
<b>Optional Information</b>	<p>Information that you may include in the certificate, but which is not required.</p>
<b>Organization unit</b>	<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>
<b>Organization</b>	<p>Type the legal name of your organization. (Optional)</p>

<b>Locality (City)</b>	Type the name of the city or town where the FortiVoice unit is located. (Optional)
<b>State/Province</b>	Type the name of the state or province where the FortiVoice unit is located. (Optional)
<b>Country</b>	Select the name of the country where the FortiVoice unit is located. (Optional)
<b>E-mail</b>	Type an email address that may be used for contact purposes. (Optional)
<b>Key type</b>	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.
<b>Key size</b>	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 100](#).

### 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 97](#).

#### 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 97](#).

#### 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 101](#).

## 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 97](#).

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 97.
  - *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 101.

### 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](#)

## 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 104](#).

#### 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 290.

### 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 287.

## 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

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 FortiFone 870i
- Reviewing system configuration

## 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 call 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:

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

<b>Outside line prefix</b>	Click the default number (9) to enter the prefix for making outbound calls.
<b>Area code</b>	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.
<b>Area code is required when dialing local numbers</b>	Select this option if the area code needs to be dialed for local phone calls.
<b>Main display name</b>	Enter the name displaying on the FortiVoice unit. This name is provided by your PSTN service provider.
<b>Main number</b>	Enter the main number of the FortiVoice unit. This number is provided by your PSTN service provider.
<b>Default prompt language</b>	<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 <a href="#">“Adding prompt languages” on page 113</a>.</p>
<b>Contact Information</b>	Optionally, enter your contact information.
<b>Emergency setting</b>	<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 134](#).

The FortiVoice unit supports the following pattern-matching syntax:

**Table 15:**Pattern-matching syntax

<b>Syntax</b>	<b>Description</b>
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.

**Table 15:**Pattern-matching syntax

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

**Table 16:**Pattern-matching examples

<b>Pattern</b>	<b>Description</b>
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:

<b>GUI field</b>	<b>Description</b>
<b>Number Management</b>	
<b>Extension number pattern</b>	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 <a href="#">“Configuring IP extensions” on page 134.</a>
<b>Speed dial pattern</b>	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 <a href="#">“Mapping speed dials” on page 242.</a>
<b>System prohibited prefix</b>	Enter the phone number prefix that you want to ban, such as 900. Click the + sign to add up to 10.
<b>System unrestricted prefix</b>	Enter the allowed phone number prefix, such as 800. Click the + sign to add up to 10.
<b>Operator extension</b>	Enter the extension for the operator of the FortiVoice unit.
<b>Supporting extension</b>	Enter the extension for technical support of the FortiVoice unit.
<b>Default Setting</b>	
<b>Default SIP user password</b>	<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 <a href="#">“Configuring IP extensions” on page 134.</a></p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>Generated:</i> Select to have a system-generated password.</li> </ul>
<b>Default user PIN</b>	<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 <a href="#">“Configuring IP extensions” on page 134.</a></p> <p>If you select <i>Specified</i>, the default password is 123123.</p>

<b>User ID prefix</b>	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 <a href="#">“Configuring IP extensions” on page 134</a> .
<b>Default ring duration</b>	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 call report and notification email templates

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

The FortiVoice unit sends out call reports based on your call report configuration (see [“Configuring report email notifications” on page 277](#)) and notification email when, for example, you have a new voicemail or fax in your mailbox or missed a call. You can customize the email templates for the call report and email notifications.

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

### To customize call report and email templates

1. Go to *Phone System > Settings > Custom Message*.
2. Open *Report* or *Email templates* to display the default templates.
3. To edit a template, double-click it or select it and click *Edit*.
4. To format template in HTML, use HTML tags, such as `<b>some bold text</b>`.  
There is a limit of 250 characters for the *Subject* field, 60 characters for the *From* field, and 4000 characters for *Htmlbody* and *Textbody* messages each in the *Content body* field.
5. To add a variable:
  - Select *Insert Variables* next to the area to insert a variable. A pop-up window appears.
  - Place your mouse cursor in the text message at the insertion point for the variable.
  - Click the name of the variable to add. It appears at the insertion point.
  - To add another variable, click the message area first, then click the variable name.
  - Click the Close (X) icon to close the window.
6. To insert a color:
  - Click *Insert Color Code*. A pop-up window of color selection appears.
  - Place your mouse cursor in the text at the insertion point for the color code, or highlight an existing color code to change.
  - Click a color in the color selection pop-up window.  
For example, to replace the color code in the HTML tag `<tr bgcolor="#3366ff">`, you can highlight `"#3366ff"`, then select the color you want from the color palette.  
To add a new color code, include it with HTML tags as applicable, such as `<tr bgcolor="#3366ff">`.
7. To determine if your HTML and color changes are correct, click *Preview*. The replacement message appears in HTML format.
8. Click *OK*, or click *Reset To Default* to revert the replacement message to its default text.

## Configuring 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:

<b>GUI field</b>	<b>Description</b>
<b>Transport Setting</b>	<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>
<b>Registration/Subscription Interval</b>	
<b>Extension registration/subscription interval range</b>	<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>
<b>Internal extension registration/subscription interval</b>	<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>

<b>External extension registration/subscription interval</b>	<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>
<b>Networks</b>	
<b>External static Host/IP</b>	Enter the FortiVoice unit's external static IP address to which the external extensions register. Also enter the port number.
<b>RTP Setting</b>	
<b>RTP port start</b>	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.
<b>RTP port end</b>	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.
<b>RTP timeout</b>	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.
<b>RTP hold timeout</b>	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.
<b>TLS Client Setting</b>	<p>If you have enabled TLS, configure the following:</p> <ul style="list-style-type: none"> <li>• <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 <a href="#">"Managing certificate authority certificates"</a> on page 102.</li> <li>• <i>TLS protocol</i>: Select the TLS protocol version.</li> </ul>
<b>Security</b>	By default, the FortiVoice unit screens out incoming calls from unauthenticated source. If you want to change this default setting, select <i>Accept unauthenticated incoming call</i> .
<b>Advanced Setting</b>	<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 <a href="#">"Inband ringtone"</a> on page 175.</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:

<b>GUI field</b>	<b>Description</b>
<b>Auto Provisioning Setting</b>	
<b>Enabled</b>	Select to activate the SIP phone auto-provisioning function for auto discovering the phones.
<b>Generate default configuration for unassigned phone</b>	<p>Select to generate phone configuration files for the supported unassigned SIP phones. For details, see <a href="#">“Viewing unassigned phones” on page 28</a>.</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, <b>do not</b> select this option. Otherwise your existing phone configuration will be overridden by the upgraded FortiVoice configuration.</p>
<b>Administrator PIN</b>	<p>Click and enter a global password to be used by an administrator to connect a FortiFone to the FortiVoice unit to set mobile extension number. This password is also used by the administrator to override schedules. For details, see <a href="#">“Configuring system capacity” on page 116</a>.</p> <p>For example, you can press the default Configure Phone feature code *17 (See <a href="#">“Modifying feature access codes” on page 262</a>) 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> <p>Click <i>Apply</i> and then <i>Auto Provisioning</i> to return to the <i>Auto Provisioning</i> page.</p>
<b>Server Settings for Phone Configuration</b>	



---

**Standard  
(apply to all  
server settings)**

Select to configure the server settings for the supported phones. The same settings apply to the SIP server, TFTP server, and NTP server.

- *Use IP address of interface:* 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 42.](#)
- *Use static IP or host name:* 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**

If you use different servers for SIP, TFTP, and NTP, select to configure the settings of each server for the supported phones.

- *SIP server*
  - *Use IP address of interface:* Select the interface for the server. The SIP phones connect to this server to register.
  - *Use static IP or host name:* Enter the current public IP address or public domain name of the server. The SIP phones connect to this server to register.
- *TFTP server*
  - *Use IP address of interface:* Select the interface for the server. The SIP phones connect to this server to receive the PBX setup information.
  - *Use static IP or host name:* 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.
- *NTP server*
  - *Use IP address of interface:* Select the interface for the server. The SIP phones connect to this server to synchronize time.
  - *Use static IP or host name:* 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 105.](#)

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

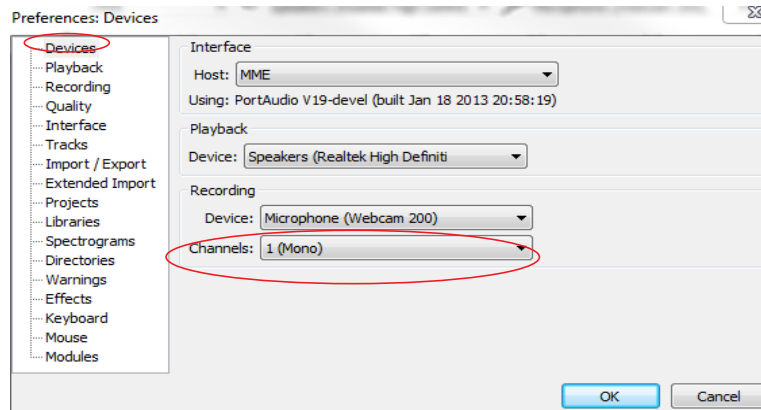
A prompt language file must be recorded in the FortiVoice language package format. This can be accomplished by using the free and robust audio program called Audacity which can be downloaded from <http://audacity.sourceforge.net> and a microphone.

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

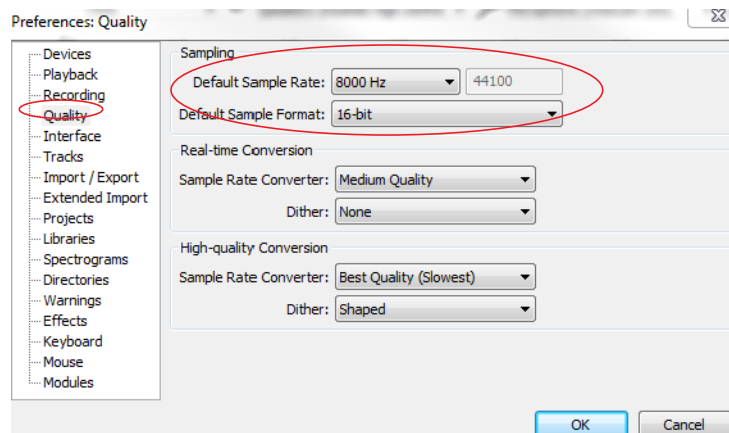
Audacity cannot natively record in the format that FortiVoice unit requires. Therefore, some adjustments need to be made in the software as described in the following procedure.

#### To generate a prompt language file

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

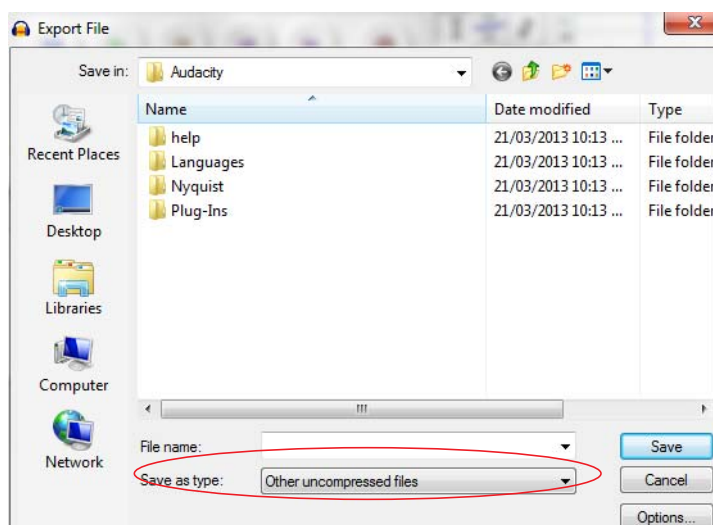


3. Click the *Quality* menu and set the *Default Sample Rate* to 8000 Hz and the *Default Sample Format* to 16 bit.



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 112.

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 134.

If your organization adds new FortiFones 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.

If your phones are not FortiFone, you can upload the third party phone configuration files to the FortiVoice TFTP server and migrate the files to your phones without using an external TFTP server.

### 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 .zip format. 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

#### **To upload third party configuration to FortiVoice TFTP server**

1. Go to *Phone System > Advanced Settings > Phone Management*.
2. Click *TFTP Service*.
3. Click *Upload* and browse for the file.
4. Click *Upload*.

## **Configuring system capacity**

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

#### **To configure system capacity**

1. Go to *Phone System > Advanced Settings > Miscellaneous*.
2. Under *Administrator PIN*, enter the password used by the administrator to override schedules.  

This global password is also used by an administrator to connect a FortiFone to the FortiVoice unit to set mobile extension number. For details, see “[Configuring SIP phone auto-provisioning](#)” on page 112.
3. Under *Schedule Override*, select *Allow admin user to override schedule* if required.  

An administrator with the privilege can dial \*821, \*822, or \*823 followed by the administrator PIN to temporarily replace the original schedule with one of the three default ones. You may also modify the temporary schedule. Dial \*820 to go back to the original schedule.
4. Under *Voicemail*, enter the maximum message and greeting length you want.

5. 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.
6. 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 32.
7. Under *Queue log*, enter the time in month that you want to keep the queue log and the maximum number of log records. For information about queue logs, see [“Viewing log messages”](#) on page 33.
8. 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 118 and [“Configuring Call Features”](#) on page 231.

### 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 134.
- 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:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for the music on hold file.
<b>Mode</b>	
<b>Files</b>	If you select to use existing sound files, do the following: <ul style="list-style-type: none"><li>• For <i>Sound files</i>, select the <i>Available</i> sound files and click <i>-&gt;</i> 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.</li><li>• 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>.</li><li>• For <i>Volume</i>, Set the music sound volume.</li></ul>
<b>Stream</b>	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.
<b>Volume</b>	Set the music sound volume.
<b>Description</b>	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](#)
- [Configuring phone profiles](#)
- [Configuring LDAP profiles](#)
- [Configuring user privileges](#)
- [Configuring location profile](#)
- [Scheduling the FortiVoice unit](#)

## 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 134.

For information on SIP trunks, see “Configuring Trunks” on page 173.

### To configure a SIP profile

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

<b>GUI field</b>	<b>Description</b>
<b>SIP</b>	<ul style="list-style-type: none"><li>• <i>Name</i>: Enter a name for this profile.</li><li>• <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.</li><li>• <i>NAT</i>: Select if the VoIP service provider supports SIP NAT translation.</li><li>• <i>Video</i>: Select if the service provider supports video calling over SIP.</li><li>• <i>T.38</i>: Select if the VoIP service provider supports fax over VoIP network.</li><li>• <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.</li></ul>

---

**Transport**

*Encryption:* Select *TLS* to encrypt the system connection between an extension and the FortiVoice unit. Select *TLS and SRTP* to encrypt both the system connection and voice communication between an extension and the FortiVoice unit.

To make this option work, you need to select a SIP profile with *TLS* or *TLS and SRTP* selected for *Encryption* when configuring an extension. You also need to enable TLS on the FortiVoice unit by going to *Phone System > Advanced Settings > SIP*.

*Transport:* SIP commonly uses TCP or UDP port 5060 and/or 5061. Port 5060 is used for non-encrypted SIP signaling sessions and port 5061 is typically used for SIP sessions encrypted with Transport Layer Security (TLS).

Enable the protocols as required.

This option, if applied to a user, overrides the system-wide transport settings. For more information, see [“Configuring SIP settings” on page 110](#).

*Secure RTP:* Select to provide encryption, message authentication and integrity, and replay protection to the FortiVoice Real-time Transport Protocol data.

---

**Codec**

Select the codecs supported by the VoIP service provider. Among the selected ones, choose the preferred one for the VoIP provider. The preferred codec is usually the most used one in your area and provides the best quality of communication.

If your preferred codec is different from that of your VoIP service provider, the service provider’s codec will be used as long as it is one of your supported codecs.

- 
3. Click *Create*.

## Modifying caller IDs

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

Caller ID modifications are used when configuring dial plans. For more information, see [“Configuring Call Routing” on page 187](#).

### To modify a caller ID

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

---

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

---



<b>Number Modification</b>	<p>If you have entered a <i>Match number</i>, configure the following values to modify it:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> </ul>
<b>Match option</b>	<p>Select the way to match a call with caller name and number in order to modify call number or caller ID.</p> <ul style="list-style-type: none"> <li>• <i>Match number or name</i>: If the number is matched, modifications will be done based on <i>Number Modification</i> configuration. If the name is matched, modifications will be done based on <i>Map to new caller ID name</i> configuration.</li> <li>• <i>Match number then name</i>: If the number is matched, modifications will be done based on <i>Number Modification</i> configuration. If both the number and name are matched, modifications will be done based on <i>Map to new caller ID name</i> configuration.</li> <li>• <i>Match name then number</i>: If the <i>Name</i> is matched, modification will be done based on <i>Map to new caller ID name</i> configuration. If both the name and number are matched, modifications will be done based on <i>Number Modification</i> configuration.</li> <li>• <i>Match number and name</i>: If both the number and name are matched, modifications will be done based on <i>Number Modification</i> and <i>Map to new caller ID name</i> configurations.</li> </ul>
<b>Match caller ID name</b>	<p>Enter the caller ID that you want to map to another one. Caller IDs are created when configuring SIP extensions. See <a href="#">“Configuring IP extensions” on page 134</a>.</p>
<b>Map to new caller ID name</b>	<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>
<b>Advanced Setting</b>	<p>Select <i>Block caller ID</i> to stop your caller ID from displaying on the destination phone.</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 *Phone System > 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*.

## 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 134.

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:

<b>GUI field</b>	<b>Description</b>
<b>Phone profile</b>	
<b>Name</b>	Enter a name for the profile.
<b>Phone type</b>	Select a phone model for the profile.
<b>Time format</b>	Select the time display format on the phone. <ul style="list-style-type: none"><li>• <i>North American</i>: mm/dd/yyyy</li><li>• <i>International</i>: dd/mm/yyyy</li></ul>
<b>Description</b>	Enter any notes you have for this profile.
<b>Configuration mode</b>	Select the profile mode. <ul style="list-style-type: none"><li>• <i>Automatic</i>: the FortiVoice unit will generate a phone configuration file based on the information you provide. See “<a href="#">Automatic Configuration</a>” on page 123. This option is only available for FortiFone-260i and above.</li><li>• <i>Manual</i>: This option allows you to manually edit the phone configuration file. See “<a href="#">Manual Configuration</a>” on page 124</li></ul>

<b>Phone book</b>	<p>Select <i>Local only</i> to include the phone directory on this FortiVoice unit, and <i>Global</i> to include the phone directories of any remote FortiVoice units connected to this unit.</p> <p>For information on phone directories, see <a href="#">“Viewing phone directories” on page 38</a>.</p>
<b>Vlan</b>	<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>
<b>Option</b>	<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"> <li>• 0: Background</li> <li>• 1: Best Effort</li> <li>• 2: Excellent Effort</li> <li>• 3: Critical Applications</li> <li>• 4: Video, &lt; 100 ms latency and jitter</li> <li>• 5: Voice, &lt; 10 ms latency and jitter</li> <li>• 6: Internetwork Control</li> <li>• 7: Network Control</li> </ul> <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>
<b>Automatic Configuration</b>	<p>This option is only available if you select <i>Automatic</i> for <i>Configuration mode</i>.</p>
<b>Display option</b>	<p>Select what to display on the extension: the extension user’s name only or name and number.</p>
<b>Provisioning lines</b>	<p>Enter the number of phone lines to which this profile applies. The maximum lines that you can provision is 4.</p>
<b>Digit map pause timer</b>	<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**

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.

You can enter the syntax or use the default syntax `x.T|x+#` where:

- `x.T` means you can dial any number and the call is initiated after the digit map pause timeout is reached.
- `|` is a choice operator that matches the expression before or after the operator. For example, `abc|def` matches "abc" or "def".
- `x+#` means you can enter any number and then press the # key to initiate the call.

For more information about digit map syntax definitions, see Section 2.1.5 of RFC 3435.

---

**Set Programmable Phone Key**

Allows you to program the phone keys for FortiFone-260i to 675i. For FortiFones with expansion modules, you can select the module to program the keys.

After completing programming the keys, you can click *Download printable label* to save and print out the configuration and label it on the phone.

Note that keys 1 and 2 are reserved and cannot be programmed.

If you select *One key dial* or *User Assigned* function for a key, you need to enter the information in the *Resource* field based on your phone configuration. For example, if you select *User defined* for key 3 and you want to map this key to your voicemail code such as \*78, enter \*78 in the *Resource* field.

Selecting *Centralized phonebook* 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 *System > Network > Network*.

If you select *Line Appearance*, the peer office will appear in the *Resource* field. Line appearance for peer office is to monitor analog lines connected through FXO gateway.

---

**Manual Configuration**

If you select *Manual* configuration mode, edit the phone configuration file.

---

**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*.

<b>GUI field</b>	<b>Description</b>
<b>Clone</b>	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> .
<b>Profile Name</b>	The name of the profile.
<b>Server</b>	The domain name or IP address of the LDAP server.
<b>Port</b>	The listening port of the LDAP server.
<b>Auth</b>	Indicates whether <i>User Authentication Options</i> is enabled.
<b>Cache</b>	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.

<b>GUI field</b>	<b>Description</b>
<b>Profile name</b>	For a new profile, enter its name.

<b>Server name/IP</b>	<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>
<b>Fallback server name/IP</b>	<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>
<b>Use secure connection</b>	<p>Select whether to connect to the LDAP servers using an encrypted connection.</p> <ul style="list-style-type: none"> <li>• <i>none</i>: Use a non-secure connection.</li> <li>• <i>SSL</i>: Use an SSL-secured (LDAPS) connection.</li> </ul> <p>Click <i>Test LDAP Query</i> to test the connection. A pop-up window appears. For details, see <a href="#">“Testing LDAP profile queries” on page 129</a>.</p>
<b>Base DN</b>	<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>
<b>Bind DN</b>	<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>
<b>Bind password</b>	<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 127](#)
- [“Configuring advanced options” on page 128](#)

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 129.

## 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:

<b>GUI field</b>	<b>Description</b>
<b>Try common name with base DN as bind DN</b>	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:

---

<b>GUI field</b>	<b>Description</b>
------------------	--------------------

---



<b>Timeout (seconds)</b>	Enter the maximum amount of time in seconds that the FortiVoice unit will wait for query responses from the LDAP server.
<b>Protocol version</b>	Select the LDAP protocol version used by the LDAP server.
<b>Enable cache</b>	<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>
<b>TTL (minutes)</b>	<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>
<b>Enable user password change</b>	Enable if you want to allow FortiVoice web portal users to change their password.
<b>Password schema</b>	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 237.

## Configuring location profile

Location profiles group phones into internal and external numbers based on their locations.

The *external* and *internal* profiles are system defined and can be modified but not be deleted.

### To configure a location profile

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

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	For a new profile, enter its name.
<b>Type</b>	Select the profile type: internal or external phones.
<b>Emergency caller ID</b>	Enter the caller ID to display on the destination phone when you dial the emergency number, such as 911.  If an extension in this profile already has an emergency caller ID, this ID is overridden by the extension's own ID. See “Emergency caller ID” on page 155.
<b>Members</b>	Select the extensions to include in the profile.
<b>Phone provision protocol</b>	Select the protocol used by the phones to get configuration file from the FortiVoice unit.

<b>Description</b>	Enter any notes you have for this profile.
<b>Emergency setting</b>	Configure to send an alert email when an emergency call is made. 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.
<b>Contact Information</b>	Enter the contact information for the profile.

3. Click *Create*.

## Scheduling the FortiVoice unit

You can schedule the FortiVoice operation time and use the schedules when configuring dial plans, virtual numbers, or call management. The default schedules, namely *after\_hour*, *any\_time*, *business\_hour*, and *holiday*, can be modified but cannot be deleted.

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

For information on dial plan, see “[Configuring Call Routing](#)” on page 187.

For information on virtual numbers, see “[Working with virtual numbers](#)” on page 171.

For information on call management, see “[Setting extension user preferences](#)” on page 154.

### To configure a standard schedule

1. Go to *Phone System > Profiles > Schedule* and click *New*.
2. Enter a profile name and select *Standard* for *Mode*.
3. Click *Create*.
4. In the schedule list, select the profile name you created.
5. For *Week Day*, select the days to include in the schedule and set the AM and PM time or select *Full Day*.
6. For *Holiday*, click *New* to set the holidays. For example, select 01/01/12 in the *Date* field and enter New Year's Day in the *Description* field, and click *Create*.
7. Click *OK*.

### To configure a calendar-based schedule

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

## Configuring FortiFone 870i

Each base FortiFone 870i can support up to 15 handsets. You can configure a FortiFone 870i to work with the FortiVoice unit by adding a primary phone (base) and multiple secondary phones (bases). For detailed information, see [FortiFone 870i Multi-Cell Deployment with FortiVoice Enterprise Technical Note](#).

The following prerequisites must be met for the configuration to work:

- FortiVoice v5.0 build 136 or later
- FortiVoice auto provisioning is enabled (see “Configuring SIP phone auto-provisioning” on page 112)
- FortiFone 870i firmware 3.23 or later
- Network connectivity available between FortiFone870i and the FortiVoice unit

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

### To configure the FortiFone 870i

1. Go to *Status > Phone System > Unassigned Phone* and find the MAC address of the intended primary station.
2. Select the intended primary station, click *Action*, and select *Assign to FortiFone-870i device*.
3. In *Device role*, set the station as primary with chain ID. The chain ID should be numbers up to 5 digits. Type any description as needed. Then click *Create*.
4. Go to *Phone System > Device > FortiFone-870i* to add extensions to the primary station. Note that we only need to add the extension configuration to the primary. All secondary stations can obtain the extension information from the primary.
5. Select the primary station just created, click *Action*, and select *Assign new extension or Apply existing extension*.
6. For *Assign new extension*, configure the extension information and enter *Handset ID* which should start with 1. Leave *Base MAC address* field empty and click *Create*.
7. Add more extensions as needed with a different handset IDs. Upon completion, you should see all the extensions listed for the primary station.
8. Since the primary station is provisioned now, we can proceed to provision the secondary stations. Factory reset the intended secondary station and connect it to the network. If the network and the FortiVoice unit are configured properly, it should appear under *Status > Phone System > Unassigned Phone*.
9. Select the unassigned FortiFone 870i station, click *Action > Assign to FortiFone-870i device*.
10. In *Device role*, set the base station as secondary and select *Prime* (primary station) from the drop down list. Type any description as needed.
11. Click *Create*.
12. On the secondary phone configuration, remove the temporary extension setting and reboot the station. See the phone guide for more information.

Note that the temporary extension is used for initial configuration of the base and has to be removed for the phone to work with the FortiVoice unit.

## Reviewing system configuration

*Phone System > Review* provides a snapshot of the FortiVoice system configuration, including:

- extension numbers
- extension numbers in conflict (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.)
- phone MAC addresses in conflict
- extension password check
- new voice mail check
- network summary
- DID handling information
- Call queues
- Agent information
- Extensions that are used by other objects and their roles in the objects

You can double click a record to modify or view the information.

# 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
- Modifying analog extension (200D-T, 1000E-T, and 20E2 models only)
- Setting up remote extensions
- Configuring fax extensions
- Setting extension user preferences
- Resetting voice messages

## 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*.

<b>GUI field</b>	<b>Description</b>
<b>Batch Edit</b>	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> .
<b>Export</b>	Select to save a copy of the extension list in CSV format.
<b>Import</b>	Select to upload a copy of the extension list in CSV format. For details, see “Importing a list of extensions” on page 142.
<b>Save</b>	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**

- *Apply phone configuration:* 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:

- 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 112.](#)
  - Phone type and MAC address is correctly configured. See [“To create or edit an IP extension” on page 136.](#)
  - Auto-provisioning is enabled for the extension associated with the phone through the user privilege applied to it. See [“Configuring user privileges” on page 237.](#)
- *Maintenance:* Select an extension and click this button to manage a user’s voicemail box. You can check the size of the box and empty the box.  
Click *Back* to return to the *SIP* tab.
  - *View phone configuration file:* Select a FortiFone extension and click this option to view the phone’s configuration file.  
When a phone is associated with an extension, the FortiVoice unit generates a configuration file for the phone. For details, see [“To create or edit an IP extension” on page 136.](#)
  - *Check the password strength of SIP accounts:* See [“Auditing SIP extension password” on page 141.](#)
  - *Number auditor:* Select to fix duplicate or missing numbers. See [“Fixing duplicate or missing numbers” on page 141.](#)
  - *Download programmable phone key labels:* If you need a copy of the programmable phone key labels of your users, select *All extensions* or *Selected extensions*, click *Yes* and then open or save the file.

---

<b>Enabled</b>	Select to activate an extension.
<b>Number</b>	The extension number.
<b>Display Name</b>	The name displaying on the extension. This is usually the name of the extension user.
<b>Status</b>	The extension statuses, including: <ul style="list-style-type: none"><li>• <i>Idle:</i> The extension is not in use.</li><li>• <i>In Use:</i> The extension is in use.</li><li>• <i>Busy:</i> The extension is busy.</li><li>• <i>Ringin</i>g: The extension is ringing.</li><li>• <i>On Hold:</i> The extension has an on-hold call.</li><li>• <i>Admin down:</i> The trunk of the extension is disabled</li><li>• <i>Not registered:</i> The extension is not registered with the FortiVoice unit and is not in service.</li><li>• <i>Unavailable:</i> The extension is not reachable.</li><li>• <i>Alarm detected:</i> There is a problem with the phone line.</li><li>• <i>Other:</i> The status other than the above.</li></ul>

---

<b>IP</b>	The link to the IP address of the phone using the extension number. See <a href="#">“IP” on page 141</a> .
<b>Department</b>	The link to the department of which this extension is a member. For information on creating departments, see <a href="#">“Creating extension departments” on page 164</a> .
<b>Disk Usage (KB)</b>	Displays the size of disk space used by voicemails for the user in kilobytes (KB).
<b>Phone Type</b>	The type of phone for this extension.
<b>Phone Profile</b>	Displays the phone profile applied to the user. For information on phone profile, see <a href="#">“Configuring phone profiles” on page 122</a> .
<b>Phone Info</b>	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:

<b>GUI field</b>	<b>Description</b>
<b>Extension Setting</b>	
<b>User ID</b>	<p>This is the system-generated ID based on the user ID prefix you set (see <a href="#">“User ID prefix” on page 109</a>) 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 <i>FortiVoice CLI Reference</i>.</p>
<b>Number</b>	Enter the extension number following the extension number pattern. See <a href="#">“Configuring PBX options” on page 106</a> .
<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers” on page 141</a>.</p>
<b>Enabled</b>	Select to activate the extension.
<b>Display name</b>	Enter the name displaying on the extension. This is usually the name of the extension user.



<b>External caller ID</b>	<p>If you want to display a particular caller ID on a called phone instead of the FortiVoice main number (see <a href="#">“Main number” on page 106</a>) or the trunk phone number (see <a href="#">“Phone Number” on page 177</a>), enter it here. The format must be <code>name&lt;phone number&gt;</code>, such as <code>HR&lt;2221111234&gt;</code>.</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 <a href="#">“Mapping DIDs” on page 191</a>.</p>
<b>SIP password</b>	<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 <a href="#">“Configuring system options” on page 80</a>.</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 <a href="#">“Default SIP user password” on page 108</a>), the password appears here. However, you can change it.</p>
<b>User PIN</b>	<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 <a href="#">“Default user PIN” on page 108</a>), the password appears here. However, you can change it.</p>
<b>Authentication type</b>	<p>Select the extension's authentication type: <i>Local</i> or <i>LDAP</i>.</p>
<b>LDAP profile</b>	<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 <a href="#">“Configuring LDAP profiles” on page 125</a>. You can click <i>New</i> to create a new profile or <i>Edit</i> to modify the selected one.</p>
<b>Authentication ID</b>	<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>

<b>Phone language</b>	Select the voice prompts for the extension, such as auto attendant and voicemail. The default is English.  For information on adding prompt languages, see <a href="#">“Adding prompt languages” on page 113</a> .
<b>Preference</b>	Select <i>Edit preference</i> to configure the extension user preferences. See <a href="#">“Setting extension user preferences” on page 154</a> .  This option is only available when you edit an extension.
<b>Description</b>	Enter any notes for the extension setting.
<b>Advanced Setting</b>	
<b>Location</b>	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. These are system defined locations.  You can also choose other customized locations.
<b>SIP setting</b>	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 <a href="#">“Working with FortiVoice profiles” on page 118</a> .
<b>User privilege</b>	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 <a href="#">“Configuring user privileges” on page 237</a> .
<b>Personal code</b>	Enter the extension specific account code that can be used to restrict calls. You can click <i>Generate</i> to get a code.
<b>Department</b>	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 <a href="#">“Configuring agents” on page 207</a> .
<b>Phone type</b>	Select a supported phone type for the extension.  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.  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.  If you select <i>FortiFone-870i</i> and want it to join the multi-cell configuration, select <i>Multi-Cell</i> . For more information, see <a href="#">“Configuring FortiFone 870i” on page 131</a> .

<b>MAC address</b>	<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>
<b>Handset ID</b>	<p>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.</p>
<b>Base MAC address</b>	<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>
<b>Phone profile</b>	<p>Select a profile type if your phone type is FortiFone 260i and above:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</li> </ul> <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 <a href="#">“Configuring phone profiles” on page 122</a>.</p> <p>The phone profile settings you select here synchronize with the same settings in extension preferences. For details, see <a href="#">“Phone profile” on page 160</a>.</p>
<b>Configure User Defined Profile</b>	<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 <a href="#">“Configuring phone profiles” on page 122</a>.</p>

<b>Auxiliary device</b>	<p>This option is only available when you edit an extension.</p> <p>Click to add SIP devices to the extension. This is known as SIP forking.</p> <p>SIP forking allows you to have your desk phone ring at the same time as your softphone or a SIP phone on your mobile. For example, you can use SIP forking to ring your desk phone and your Android SIP phone at the same time, allowing you to take the call from either device easily. No forwarding rules would be necessary as both devices would ring. In the same manner, SIP forking can be used in an office and allow the secretary to answer calls to the extension of his/her boss when he is away or unable to take the call.</p> <p>For more information, see <a href="#">“Configuring SIP forking” on page 142.</a></p>
<b>Call Center</b>	
<b>Agent</b>	<p>Enable or disable this extension as a call center agent. For more information about call center agents, see <a href="#">“Setting up a Call Center” on page 198.</a></p>
<b>Configure</b>	<p>If you enabled the agent, click to configure it. For more information, see <a href="#">“Configuring call center agent” on page 144.</a></p>
<b>Voice Mailbox</b>	
	<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>
<b>Main voice mailbox</b>	<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>
<b>Notify message waiting light to</b>	<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 -&gt; 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 <a href="#">“Modifying feature access codes” on page 262</a>) and enter the user’s own voicemail PIN.</p> <p>For information on creating user groups, see <a href="#">“Creating extension groups” on page 163.</a></p>
<b>Extra Information</b>	
	<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 134.

#### 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 80.
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 136.

### Fixing duplicate or missing numbers

When there are duplicate or missing 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.

For information on the *Show suggested numbers* field, see “[Show suggested numbers](#)” on page 171.

#### To fix duplicate or missing numbers

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

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 134.
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 134.
4. Close the *Numbers Auditor* 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.

### Configuring SIP forking

SIP forking allows you to have your desk phone ring at the same time as your softphone or a SIP phone on your mobile.

When a device is added, it inherits your master phone's user privileges except hot-desking and fax.

You can add two SIP extensions and one external phone number.

## To add a SIP device

1. Go to *Extensions > Extensions > IP Extensions*.
2. Click an extension and go to *Advanced Setting*.
3. Click *Auxiliary device* to add a device.
4. Click *New* and configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Status</b>	Select to enable the device.
<b>Type</b>	Select SIP for the type of device to add.
<b>User ID</b>	<p>This is the system-generated ID based on the user ID prefix you set (see <a href="#">“User ID prefix” on page 109</a>) and the master extension number.</p> <p>This option is view only. You can add a new user ID through the CLI. For more information, see the <a href="#">FortiVoice CLI Reference</a>.</p>
<b>Password</b>	<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 <a href="#">“Configuring system options” on page 80</a>.</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 <a href="#">“Default SIP user password” on page 108</a>), the password appears here. However, you can change it.</p>
<b>Location</b>	Designate the device as external, internal, or mobile. Click <i>Edit</i> to modify the current location or <i>New</i> to configure a new one.
<b>SIP setting</b>	Select the SIP profile for the device. Click <i>Edit</i> to modify the current profile or <i>New</i> to configure a new one. For more information, see <a href="#">“Working with FortiVoice profiles” on page 118</a> .
<b>Phone type</b>	<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>
<b>MAC address</b>	Enter the MAC address of the SIP device.

5. Click *Create*.

### To add an external phone number

1. Go to *Extensions > Extensions > IP Extensions*.
2. Click an extension and go to *Advanced Setting*.
3. Click *Auxiliary device* to add a device.
4. Click *New*.
5. Select *Status* to enable the device.
6. For *Type*, select *External number*.
7. Enter the external number.
8. Click *Create*.

## Configuring call center agent

Configure the departments that a call center agent manages, queues that the agent belongs to, skill sets, and skill levels. For more information on call center, see “[Setting up a Call Center](#)” on page 198.

### To configure an agent

1. Go to *Extensions > Extensions > IP Extensions > Call Center*.
2. Select *Enable for Agent*.
3. Click *Configure* and do the following:

<b>GUI field</b>	<b>Description</b>
<b>Agent profile</b>	Select the profile for the agent. You can also create a new one or modify an existing one. For more information about agent profiles, see “ <a href="#">Configuring agent profiles</a> ” on page 218.
<b>Managed departments</b>	An agent manager may need to monitor call queues in certain departments. For information on setting up departments, see “ <a href="#">Creating extension departments</a> ” on page 164.  Click >> to select the departments to be monitored and then click <i>Done</i> .
<b>Member of Queues</b>	Click to select the call queues to join. <ul style="list-style-type: none"> <li>• <i>Main/Outgoing queue</i>: This option is for collecting the outgoing calls from all queues by this agent and displaying them in “<a href="#">Working with call queue statistics</a>” on page 219. You can select any queue of which this agent is a member for that purpose except <i>None</i> which will not collect agent’s outgoing call information.</li> <li>• <i>Queues</i>: Select the queues of which you want the extension/agent to be a member, and click <i>Apply</i>.</li> </ul>
<b>Skill Sets</b>	Click <i>New</i> to select the skill set for the agent, including skill and level, and click <i>Create</i> . For more information about agent skills and levels, see “ <a href="#">Adding agent skill sets</a> ” on page 216 and “ <a href="#">Creating agent skill levels</a> ” on page 217.

4. Click *OK*.



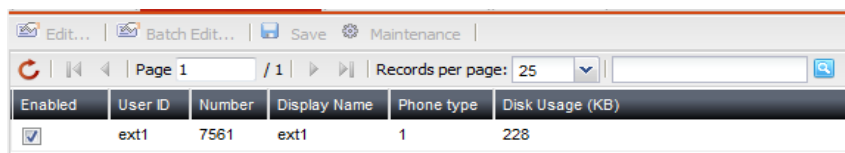
## Modifying analog extension (200D-T, 1000E-T, and 20E2 models only)

The FortiVoice 200D-T and 1000E-T each has one analog port and a default analog extension. The FortiVoice 20E2 has two analog ports and two default analog extensions. You can edit the extensions' default configuration.

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

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

**Figure 30:** Viewing analog extension



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

<b>GUI field</b>	<b>Description</b>
<b>Batch Edit</b>	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> .
<b>Maintenance</b>	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.
<b>Enabled</b>	Select to activate the extension.
<b>User ID</b>	This is the system-generated ID for the analog extension.
<b>Number</b>	The analog extension number.
<b>Display Name</b>	The name displaying on the extension.
<b>Phone Type</b>	The type of phone for this extension.
<b>Disk Usage (KB)</b>	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 31:** Analog extension configuration

**Extension Setting**

User ID:

Number:   Show suggested numbers

Enabled:

Display name:

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

**Password policy is disabled**

User PIN:    View PIN

Authentication type:

Language:

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

---

**Advanced Setting**

User privilege:

Department:

Analog port:

Enable fax:

<b>GUI field</b>	<b>Description</b>
<b>Extension Setting</b>	
<b>User ID</b>	This is the system-generated ID for the extension and is read-only.
<b>Number</b>	Enter the extension number following the extension number pattern. See <a href="#">“Configuring PBX options”</a> on page 106.
<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers”</a> on page 141.</p>
<b>Enabled</b>	Select to activate the extension.
<b>Display name</b>	Enter the name displaying on the extension. This is usually the name of the extension user.

<b>External caller ID</b>	<p>If you want to display a particular caller ID on a called phone instead of the FortiVoice main number (see <a href="#">“Main number” on page 106</a>) or the trunk phone number (see <a href="#">“Phone Number” on page 177</a>), enter it here. The format must be <code>name&lt;phone number&gt;</code>, such as <code>HR&lt;2221111234&gt;</code>.</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 <a href="#">“Mapping DIDs” on page 191</a>.</p>
<b>User PIN</b>	<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 <a href="#">“Configuring system options” on page 80</a>.</p> <p>Enter the password for the user to access voicemail (by dialing *98 or the customized code. See <a href="#">“Modifying feature access codes” on page 262</a>) 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 <a href="#">“Default user PIN” on page 108</a>), the password appears here. However, you can change it.</p>
<b>Authentication type</b>	<p>Select the extension’s authentication type: <i>Local</i> or <i>LDAP</i>.</p>
<b>LDAP profile</b>	<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 <a href="#">“Configuring LDAP profiles” on page 125</a>. You can click <i>New</i> to create a new profile or <i>Edit</i> to modify the selected one.</p>
<b>Authentication ID</b>	<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>
<b>Language</b>	<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 <a href="#">“Adding prompt languages” on page 113</a>.</p>

<b>Preference</b>	Select <i>Edit preference</i> to configure the extension user preferences. See “ <a href="#">Setting extension user preferences</a> ” on page 154.
<b>Advanced Setting</b>	
<b>User privilege</b>	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 “ <a href="#">Configuring user privileges</a> ” on page 237.
<b>Department</b>	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 “ <a href="#">Creating extension departments</a> ” on page 164.
<b>Analog port</b>	Enter the analog port number. By default, it is <i>fxs1</i> .
<b>Enable fax</b>	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:

<b>GUI field</b>	<b>Description</b>
<b>Extension Setting</b>	
<b>Number</b>	Enter the local extension number from which calls are transferred to a remote extension.

<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers” on page 141</a>.</p>
<b>Remote number</b>	<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>
<b>Enabled</b>	<p>Select to activate the remote extension.</p>
<b>Display name</b>	<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 <a href="#">“Modifying caller IDs” on page 120</a>.</p>
<b>External caller ID</b>	<p>If you want to display a particular caller ID on a called phone instead of the FortiVoice main number (see <a href="#">“Main number” on page 106</a>) or the trunk phone number (see <a href="#">“Phone Number” on page 177</a>, enter it here. The format must be <code>name&lt;phone number&gt;</code>, such as <code>HR&lt;2221111234&gt;</code>.</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 <a href="#">“Mapping DIDs” on page 191</a>.</p>

<b>User PIN</b>	<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 <a href="#">“Configuring system options” on page 80</a>.</p> <p>Enter the password for the user to access voicemail (by dialing *98 or the customized code. See <a href="#">“Modifying feature access codes” on page 262</a>) 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 <a href="#">“Default user PIN” on page 108</a>), the password appears here. However, you can change it.</p>
<b>Authentication type</b>	Select the extension’s authentication type: <i>Local</i> or <i>LDAP</i> .
<b>Description</b>	Enter any notes you have for the extension.
<b>LDAP profile</b>	<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 <a href="#">“Configuring LDAP profiles” on page 125</a>.</p> <p>You can click <i>New</i> to create a new profile or <i>Edit</i> to modify the selected one.</p>
<b>Authentication ID</b>	<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>
<b>Voice Mailbox</b>	<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>
<b>Main voice mailbox</b>	<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>

<b>Notify message waiting light to</b>	<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 -&gt; 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 “<a href="#">Modifying feature access codes</a>” on page 262) and enter the user’s own voicemail PIN.</p> <p>For information on creating user groups, see “<a href="#">Creating extension groups</a>” on page 163.</p>
<b>Search</b>	Enter an extension and look for it in the <i>User(s)/Group(s)</i> fields.

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 253.

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

<b>GUI field</b>	<b>Description</b>
<b>Enabled</b>	Select to activate this fax extension.
<b>Number</b>	The fax extension number.
<b>Display Name</b>	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:

<b>GUI field</b>	<b>Description</b>
<b>Extension Setting</b>	
<b>Number</b>	Enter the extension number following the extension number pattern. See “ <a href="#">Configuring PBX options</a> ” on page 106.

<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers” on page 141</a>.</p>
<b>User ID</b>	<p>This is the system-generated ID based on the user ID prefix you set (see <a href="#">“User ID prefix” on page 109</a>) 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 <i>FortiVoice CLI Reference</i>.</p>
<b>Enabled</b>	<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 <a href="#">“Configuring fax” on page 253</a>.</p>
<b>Display name</b>	<p>Enter the name displaying on the extension.</p>
<b>External caller ID</b>	<p>If you want to display a particular caller ID on a called phone instead of the FortiVoice main number (see <a href="#">“Main number” on page 106</a>) or the trunk phone number (see <a href="#">“Phone Number” on page 177</a>), enter it here. The format must be name&lt;phone number&gt;, such as HR&lt;2221111234&gt;.</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 <a href="#">“Mapping DIDs” on page 191</a>.</p>
<b>SIP password</b>	<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 <a href="#">“Configuring system options” on page 80</a>.</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 <a href="#">“Default SIP user password” on page 108</a>), the password appears here. However, you can change it.</p>



<b>User PIN</b>	<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 <a href="#">“Default user PIN” on page 108</a>), the password appears here. However, you can change it.</p>
<b>Authentication type</b>	Select the extension’s authentication type: <i>Local</i> or <i>LDAP</i> .
<b>LDAP profile</b>	<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 <a href="#">“Configuring LDAP profiles” on page 125</a>. You can click <i>New</i> to create a new profile or <i>Edit</i> to modify the selected one.</p>
<b>Authentication ID</b>	<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>
<b>Phone language</b>	<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 <a href="#">“Adding prompt languages” on page 113</a>.</p>
<b>Preference</b>	<p>Select <i>Edit preference</i> to configure the extension user preferences. See <a href="#">“Setting extension user preferences” on page 154</a>.</p> <p>This option is only available when you edit an extension.</p>
<b>Description</b>	Enter any notes you have for the extension.
<b>Advanced Setting</b>	
<b>Location</b>	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.
<b>SIP setting</b>	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 <a href="#">“Working with FortiVoice profiles” on page 118</a> .

<b>User privilege</b>	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 <a href="#">“Configuring user privileges” on page 237</a> .
<b>Personal code</b>	Enter the extension specific account code that can be used to restrict faxes. You can click <i>Generate</i> to get a code.
<b>Department</b>	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 <a href="#">“Creating extension departments” on page 164</a> .
<b>Phone type</b>	Select a supported phone type for the extension.  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.  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.
<b>MAC address</b>	Enter the MAC address of the adapter through which the fax machine connects to the FortiVoice unit.
<b>Extra Information</b>	This option is only available when you edit an extension.
<b>IP</b>	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*.

<b>GUI field</b>	<b>Description</b>
<b>Maintenance</b>	Select an extension and click this option to reset the user preferences to the default values.
<b>Number</b>	The extension number.
<b>User ID</b>	The system-generated ID based on the extension number.
<b>Display Name</b>	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:

<i>GUI field</i>	<i>Description</i>
<b>Voicemail Setting</b>	
<b>User ID</b>	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 <i>FortiVoice CLI Reference</i> .
<b>Number</b>	The extension number. This is not editable.
<b>Display name</b>	Enter the name displaying on the extension. This is usually the name of the extension user.
<b>Emergency caller ID</b>	<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 “<a href="#">External caller ID</a>” on page 155), that ID will not override the emergency caller ID when dialing the emergency number.</p> <p>If this extension is part of a phone group in a location profile which also has an emergency caller ID, this ID overrides the emergency caller ID in the location profile. See “<a href="#">Emergency caller ID</a>” on page 130.</p>
<b>External caller ID</b>	<p>The caller ID you want to display on a called phone instead of the FortiVoice main number (see “<a href="#">Main number</a>” on page 106) or the trunk phone number (see “<a href="#">Phone Number</a>” on page 177). This is not editable.</p> <p>For details, see “<a href="#">External caller ID</a>” on page 137 and “<a href="#">External caller ID</a>” on page 147.</p>
<b>Ring duration</b>	Enter the phone ringing duration in seconds before an incoming call goes to voicemail.
<b>Call forward</b>	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 “ <a href="#">Configuring user privileges</a> ” on page 237.
<b>Call waiting</b>	Select to enable call waiting. This function only works if call waiting is enabled in the extension’s user privilege. See “ <a href="#">Configuring user privileges</a> ” on page 237.
<b>Do not disturb</b>	Select to enable DND. This function only works if DND is enabled in the extension’s user privilege. See “ <a href="#">Configuring user privileges</a> ” on page 237.
<b>Message waiting indication</b>	Select to enable phone indication that a message is received.

<b>Voicemail handling (Caller press 0 during announcement)</b>	Select to enable reaching the operator by pressing 0 when you hear the announcement of a callee's voicemail.
<b>Notification Options</b>	
<b>Voicemail</b>	<p>Select the type of email notification when this extension has a voicemail:</p> <ul style="list-style-type: none"> <li>• <i>None</i>: Do not send any notification.</li> <li>• <i>Simple</i>: Send an email notification.</li> <li>• <i>With attachment</i>: Send an email notification with the voicemail attached.</li> </ul>
<b>Fax</b>	<p>Select the type of email notification when this extension has a fax:</p> <ul style="list-style-type: none"> <li>• <i>None</i>: Do not send any notification.</li> <li>• <i>Simple</i>: Send an email notification.</li> <li>• <i>With attachment</i>: Send an email notification with the fax attached.</li> </ul>
<b>Missed call</b>	Select <i>On</i> if you want to send an email notification when an incoming call is missed.

---

## Voicemail Options

Configure greeting, unavailable, and busy messages.

*Name:* Your name of the voicemail. For example, John Doe.

- *Standard:* Use the system default name for the voicemail. This will be the extension number.
- *Personal:* Use your own name for the voicemail.
  - Click *Call me* to ring your extension and record a name using the phone, such as your name or extension number.
  - Click *Upload* to import a name, such as your name or extension number.
  - Click *Play* to listen to a recorded name.
  - Click *Erase* to delete a recorded name.
  - Click *Download* to save a recorded name.

*Greeting:* Select the voicemail greeting mode and greeting content.

- *Standard:* The system defined greeting.
- *Simple:* The customer-recorded greeting that applies to any time except when the line is busy and extension is unavailable.
- *Scheduled:* The customer-recorded greeting that comes with a schedule.
- *Conditional:* The customer-recorded greeting that only applies to occasions when the line is busy or extension is unavailable.
- *Audio file:* Click to configure the greeting. This option is only available when you select *Simple*, *Scheduled* or *Conditional*.
  - Click *Call me* to ring your extension and record a message such as a greeting, unavailable, or busy message using the phone. This applies to the *Simple* and *Scheduled* modes.
  - Click *Upload* to import a message such as a greeting, unavailable, or busy message.
  - Click *Play* to listen to a message such as a greeting, unavailable, or busy message.
  - Click *Erase* to delete a message such as a greeting, unavailable, or busy message.
  - Click *Download* to save a message such as a greeting, unavailable, or busy message.

If you select *Scheduled* for *Greeting*, click *New* to add a system schedule or create a new one. You can also add a greeting which is the audio file you configured when clicking *Audio file*.

The purpose of having a separate voicemail name file is for occasions that you just want to change the name without touching the greeting file.

---

## Display Preference

<b>Default portal</b>	<p>Select the default user web portal interface.</p> <p>If <i>User portal</i> is disabled, it means that the user portal function in the user privilege for this extension is not enabled. For more information, see <a href="#">“Configuring user privileges” on page 237</a>.</p> <p>If <i>Operator 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 <a href="#">“Configuring user privileges” on page 237</a>.</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 <a href="#">“Call Center” on page 140</a>.</p>
<b>Phone language</b>	<p>Select the prompt language for the extension. The default is English.</p> <p>For information on adding prompt languages, see <a href="#">“Adding prompt languages” on page 113</a>.</p>
<b>Web language</b>	Select the language for the FortiVoice user web portal.
<b>Theme</b>	Select the display theme for the FortiVoice user web portal.
<b>Time zone</b>	Select the time zone for the FortiVoice user web portal.
<b>Idle timeout</b>	Set the timeout for the FortiVoice user web portal.
<b>Account Management</b>	Click <i>Change PIN number</i> to change the password for accessing the voice mailbox and the FortiVoice user web portal.
<b>Agent</b>	
<b>PIN required to login/logout from phone</b>	<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 <a href="#">“Configuring account codes” on page 241</a>.</p>
<b>PIN required to pause/unpause from phone</b>	<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 <a href="#">“Configuring account codes” on page 241</a>.</p>
<b>Auto-Pause after agent login queue</b>	<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 <a href="#">“Configuring account codes” on page 241</a>.</p>

---

**Speed Dial Setting**

Map a phone key to a phone number for speed dialing by clicking *Number* and enter the phone number.

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.

---

**Follow Me**

See [“Configuring follow me settings” on page 161](#).

---

**Black list**

Click *New* to enter the phone number you want to block from calling this extension.

This configuration serves as a profile for use in managing calls. See [“Handling calls” on page 161](#).

---

**Call Handling**

*Retain original caller ID*: Select to maintain the original caller's identity when forwarding an inbound call.

*Call screening*: Select if you want the FortiVoice unit to prompt callers for their names so that callees can identify the callers before the connect to you.

*Record caller name*: By default, this option is selected when you select *Call screening*. If you deselect this option, the FortiVoice unit will not prompt callers for their names. Instead, the FortiVoice unit will ring a callee's phone but will not connect to the caller. The callee is able to pick up the phone and see the caller's ID and decide whether to pick up the call.

For more information, see [“Handling calls” on page 161](#).

---

---

**Twinning Setting**

This option is only available if *Twinning* is selected in the user privileges of the extension. For more information, see [“Twinning” on page 238](#).

*Setting:* Select the twinning method.

- *Disabled:* Select to disable twinning.
- *Simple:* Select to configure a basic twinning by adding a phone number.
- *Scheduled:* Select to configure a twinning by adding phone numbers based on a schedule.

*Operation status:* If you choose to configure a twinning, select to turn it on or off.

*Number:* If you choose to configure a simple twinning, enter the phone (twin) number.

*Schedule:* If you choose to configure a scheduled twinning, select up to 3 time schedules (see [“Scheduling the FortiVoice unit” on page 131](#)), and enter a phone (twin) number for each schedule.

---

**Phone profile**

For details on phone profiles, see [“Configuring phone profiles” on page 122](#).

Select a profile type if your phone type is FortiFone 260i and above:

- *Admin defined:* This type allows you to choose a system level phone profile. You can also create a new profile or modify the selected one.
- *User defined:* 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.

Select an *Admin defined* profile if your phone type is other than FortiFone 260i and above. You can also create a new profile or modify the selected one.

The phone profile settings you select here synchronize with the same settings in extension configuration. For details, see [“Phone profile” on page 139](#).

---

**Configure User Defined Profile**

This option is only available if you select the *User defined* profile type, save the extension configuration and re-open the extension.

Click to configure the user defined phone profile. For details, see [“Configuring phone profiles” on page 122](#).

---

**FortiFone Call Preference**

If this extension is for a FortiFone, you can configure its call preferences.

---

**Direct call**

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.

---

**Direct call number**

If you select *Direct call*, enter the number to call. For example, the number of your paging system.

---



<b>Direct call timer</b>	Enter the time in seconds to wait before the number dialing starts after the phone is picked up.  You can enter a different number to call before the set time expires.
<b>Auto answer</b>	Select to enable this phone to automatically answer phone calls without being picked up.

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 161](#).

### 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.

You can manage a normal call handling by configuring the call process for different situations. You can also manage quick call handling by dialing a code to enter into a default mode and configure the call process for that particular mode if required.

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

### To handle a normal call

1. Go to *Extensions > Extensions > Preferences > Call Handling*.
2. Click *Normal call handling*.
3. Select a call status at the top of the page.

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

4. For *Call Process*, select *System default action* or *User defined action*.  
The *System default action* (action shows in brackets) changes depending on the status selection.
5. If you select *User defined*, click *New* to define a call process according to a schedule.
  - Select a pre-configured *Schedule* for the call action. You can click *View* to display the schedule details. For information on configuring schedules, see “[Scheduling the FortiVoice unit](#)” on page 131.
  - Add an *Action* for the call process.  
For some call handling processes that may require further actions, you need to add one or more call processes to complete the call handling. For example, after adding a process that contains a *Forward* action, you can add another process with a *Go voicemail* action to complete the call handling. In this case, the call will be forwarded to the phone specified and if the phone is not picked up, a voicemail will be left on this extension.  
*Default action* is equal to the action when you select *System default action* under *Call Process*.
    - If you select *Follow me*, select a follow me profile. For information on configuring follow me, see “[Follow Me](#)” on page 159.  
This option is available only if call forwarding is enabled in the extension’s user privilege. See “[Configuring user privileges](#)” on page 237.
    - 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 117.
    - If you select *Auto attendant*, select an auto attendant profile. For information on configuring auto attendant, see “[Configuring auto attendants](#)” on page 231.
    - 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 237.
  - Click *Create*.

6. Click *OK*.

### To handle a quick call

1. Go to *Extensions > Extensions > Preferences > Call Handling*.
2. Click *Quick call handling*.
3. Select a call status at the top of the page.  
Each status can only be used for one call management configuration.
4. For *Call Process*, select *System default action* or *User defined action* except for the *Out of office* status.
5. If you select *System default action*, the three quick call modes are the same as listed.
6. If you select *User defined*, click *New* to define a call process according to a schedule.
  - Select a pre-configured *Schedule* for the call action. You can click *View* to display the schedule details. For information on configuring schedules, see “[Scheduling the FortiVoice unit](#)” on page 131.
  - Add an *Action* for the call process. You can add multiple actions to process a call in sequence. For example, you can add *Play announcement* and then *Auto attendant*. In this case, an incoming call will be transferred to the auto attendant after an announcement is played.  
*Default action* is equal to the action when you select *System default action* under *Call Process*.
    - If you select *Follow me*, select a follow me profile. For information on configuring follow me, see “[Follow Me](#)” on page 159.

This option is available only if call forwarding is enabled in the extension's user privilege. See [“Configuring user privileges” on page 237](#).

- 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 117](#).
  - If you select *Auto attendant*, select an auto attendant profile. For information on configuring auto attendant, see [“Configuring auto attendants” on page 231](#).
  - 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 237](#).
  - Click *Create*.
7. 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 clicking *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 134](#).

For information on creating general voice mailboxes, see [“Setting up general voice mailboxes” on page 167](#).

### 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 134](#).

### 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. If you have call center license, the *Call Center* section appears. For configuration information, see [“Configuring agents” on page 207](#).
6. Click *Create*.

## Creating ring groups

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

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

### To create a ring group

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

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter the name for the ring group.
<b>Number</b>	<p>Enter the ring group number following the extension number pattern. See <a href="#">“Configuring PBX options” on page 106</a>.</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>
<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers” on page 141</a>.</p>

<b>Display Name</b>	Enter the name displaying on the extensions of the ring group, such as “HR”.
<b>Enabled</b>	Select to activate the ring group.
<b>Ring mode</b>	Select how you want the ring group to be called. <ul style="list-style-type: none"> <li>• <i>All</i>: All extensions in the group will ring when the ring group number is dialed.</li> <li>• <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.</li> </ul>
<b>Members</b>	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.  For information on creating extensions and user groups, see <a href="#">“Setting up local extensions” on page 134</a> and <a href="#">“Creating extension groups” on page 163</a> .
<b>External numbers</b>	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.
<b>Call Handling</b>	Use this option to configure the call handling for the ring group. For more information, see <a href="#">“Configuring ring group call handling” on page 165</a> .
<b>Advanced setting</b>	<ul style="list-style-type: none"> <li>• <i>Ring Pattern</i>: Select a ring pattern for the group.</li> <li>• <i>Ring duration</i>: Set the amount of time in seconds allowing all extensions or each one to ring before going to voicemail.</li> <li>• <i>Early media</i>: Select the ring tone for the group. For creating new sound files, see <a href="#">“Managing sound files and music on hold” on page 117</a>.</li> <li>• <i>Caller ID option</i>: Select how you want the caller ID to display.</li> <li>• <i>Call waiting</i>: Select to enable call waiting.</li> <li>• <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.</li> </ul>

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.

You can only configure ring group call handling when editing a ring group.

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

For information on the *Call Handling* option, see [“Call Handling” on page 165](#).

### To configure the call process

1. On the *Ring Group* page, click *Normal 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 131.
- Add an *Action* for the call process. You can add multiple actions to process a call in sequence. For example, you can add *Play announcement* and then *Auto attendant*. In this case, an incoming call will be transferred to the auto attendant after an announcement is played.

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

- If you select *Voicemail*, enter the extension number of the voice mail.
  - If you select *Play announcement*, select a sound file. For information on configuring sound files, see "[Managing sound files and music on hold](#)" on page 117.
  - If you select *Auto attendant*, select an auto attendant profile. For information on configuring auto attendant, see "[Configuring auto attendants](#)" on page 231.
  - 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 237.
- 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 106.

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 141](#).

6. Enter the name displaying on the extensions of the group, such as “HR”.
7. Select *Enabled* to activate this group.
8. 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.
9. For *Emergency call option*, do the following:
  - Select *Display emergency caller ID* to show the caller ID.
  - Select *Disconnect ongoing call* to interrupt a page in progress when an emergency page comes in.
10. Select the available extensions or extension groups that you want to include in the page group and click -> to move them into the *Selected* field.
11. Click *Create*.

## Creating 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 262](#).

### 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 134](#) and [“Creating extension groups” on page 163](#).
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*.

<b>GUI field</b>	<b>Description</b>
<b>Enabled</b>	Select to activate the mailbox.
<b>Number</b>	The extension number for the mailbox. This number is for the mailbox only and not associated with any phone.
<b>Display Name</b>	The name displaying on the extension.
<b>Disk Usage (KB)</b>	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 32:** Adding a general voice mailbox

**General Voicemail**

Number:   Show suggested numbers

User ID:

Enabled:

Display name:

User PIN:

Authentication type: Local

Phone language: --Default--

---

**Group Voice Mailbox**

Mode:  Centralized  Broadcast

Notify message waiting light

List as mailbox

Participants:

**User(s)** **Group(s)**

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 Diaio Vancouver) (sip)

<b>GUI field</b>	<b>Description</b>
------------------	--------------------

### General Voicemail



<b>Number</b>	Enter the mailbox extension number following the extension number pattern. See <a href="#">“Configuring PBX options” on page 106</a> .
<b>User ID</b>	<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 <a href="#">FortiVoice CLI Reference</a>.</p>
<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers” on page 141</a>.</p>
<b>Enabled</b>	Select to activate the mailbox extension.
<b>Display name</b>	Enter the name of the mailbox extension.
<b>User PIN</b>	<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 <a href="#">“Configuring system options” on page 80</a>.</p> <p>Enter the password for the user to access voicemail (by dialing *98 or the customized code. See <a href="#">“Modifying feature access codes” on page 262</a>) 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 <a href="#">“Default user PIN” on page 108</a>), the password appears here. However, you can change it.</p>
<b>Authentication type</b>	Select the mailbox extension’s authentication type: <i>Local</i> or <i>LDAP</i> .
<b>LDAP profile</b>	<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 <a href="#">“Configuring LDAP profiles” on page 125</a>.</p> <p>You can click <i>New</i> to create a new profile or <i>Edit</i> to modify the selected one.</p>

<b>Authentication ID</b>	<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 for Authentication type</i>.</p>
<b>Phone language</b>	<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 <a href="#">“Adding prompt languages” on page 113</a>.</p>
<b>Description</b>	<p>Enter any notes for the extension's mailbox.</p>
<b>Group Voice Mailbox</b>	<p>Configure the users for sharing this extension's mailbox.</p>
<b>Mode</b>	<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"> <li>• <b>Centralized:</b> 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. <ul style="list-style-type: none"> <li>• <i>Notify message waiting light:</i> 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.</li> <li>• <i>List as mailbox:</i> Users can listen to a centralized voicemail by dialing *97 or the customized code (see <a href="#">“Modifying feature access codes” on page 262</a>) from their own extensions and enter the user PIN for this general voicemail box.</li> </ul> </li> <li>• <b>Broadcast:</b> 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 <a href="#">“Modifying feature access codes” on page 262</a>) from any extensions and enter the personal user PIN.</li> </ul>
<b>Participants</b>	<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 -&gt; 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 -&gt; to move them to the <i>Selected</i> field.</p> <p>For information on creating user groups, see <a href="#">“Creating extension groups” on page 163</a>.</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:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for the virtual number.
<b>Number</b>	Enter the virtual number which is not assigned to any phone.
<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers”</a> on page 141.</p>
<b>Display name</b>	Enter the name displaying on the extension. This is usually the name of the extension user.
<b>Enabled</b>	Select to activate this virtual number.
<b>Bypass sub call handling</b>	Select if you want to bypass the call handling configuration embedded in the call handling of this virtual number.
<b>Comment</b>	Enter any notes you have for the virtual number.
<b>Call Handling</b>	Use this option to configure the call handling for the virtual number. For more information, see <a href="#">“Configuring virtual number call handling”</a> on page 172.

## 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 171](#).

### To configure the call process

1. On the *Virtual Number* page, click *New* under *Call Handling*.
2. Select a pre-configured *Schedule* for the call action. You can also click *New* to create a schedule or *Edit* to modify the selected one. For information on configuring schedules, see [“Scheduling the FortiVoice unit” on page 131](#).
3. Select an *Action* for the call handling.

Some actions require that you enter further information to complete the call process, such as *Dial extension* and *General mailbox*.

For some call handling processes that may require further actions, you need to add one or more call processes to complete the call handling. For example, after adding a process that contains a *Set call queue priority* action, you can add another process with a *Call queue* action to complete the call handling. In this case, the call will be processed again with new priority after it is transferred to the queue.

4. Click *Create*.
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 134 and “Configuring Call Routing” on page 187.

This topic includes:

- Setting up VoIP trunks
- Modifying PSTN/PRI trunks
- 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*.

<b>GUI field</b>	<b>Description</b>
<b>Test</b>	Select to test if the trunk is created successfully. For more information, see “Testing SIP trunks” on page 177.
<b>FortiCall</b>	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 178.
<b>Enabled</b>	Select to activate this trunk.
<b>Name</b>	The name of the VoIP service provider.
<b>Server</b>	The VoIP provider’s domain name or IP address. For example, 172.20.120.11 or voip.example.com.
<b>Port</b>	The port for SIP sessions.

<b>SIP Setting</b>	The SIP profile applied to this trunk.
<b>Status</b>	<p>The status of the SIP trunk.</p> <ul style="list-style-type: none"> <li>• <i>Not registered</i>: The trunk is not registered with the VoIP service provider and is not in service.</li> <li>• <i>In service</i>: The trunk is registered with the VoIP service provider and is in service.</li> <li>• <i>Unavailable</i>: The trunk is not reachable.</li> <li>• <i>Alarm detected</i>: There is a problem with the phone line.</li> <li>• <i>Admin down</i>: The trunk is disabled.</li> <li>• <i>Unmonitored</i>: The trunk is unknown.</li> </ul>

### To create a VoIP trunk

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

<b>GUI field</b>	<b>Description</b>
<b>SIP</b>	
<b>Name</b>	Enter the name of the VoIP service provider.
<b>Enabled</b>	Select to activate the SIP trunk.
<b>Display name</b>	Enter your caller ID that will appear on the called phone, such as Example Company.
<b>Main number</b>	<p>Enter the phone number that will appear on the called phone.</p> <p>If you entered the external caller ID in “<a href="#">External caller ID</a>” on page 137 or “<a href="#">External caller ID</a>” on page 155, this trunk phone number will be overridden by the external caller ID.</p>
<b>SIP Setting</b>	
<b>SIP server</b>	Enter the VoIP provider’s IP address or domain name. For example, 172.20.120.11 or voip.example.com.
<b>SIP port</b>	<p>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.</p> <p>If you select the <i>Using DNS record</i> option, this field is greyed out.</p>
<b>Using SRV record</b>	<p>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.</p> <p>You can only select this option if your VoIP provider uses the same setting.</p>
<b>User name</b>	Enter the user name provided by the VoIP service provider for the FortiVoice unit to register with the SIP server.

<b>Password</b>	Enter the password provided by the VoIP service provider for the FortiVoice unit to register with the SIP server.
<b>Auth. user name</b>	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.
<b>Realm/domain</b>	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.
<b>SIP setting</b>	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 <a href="#">“Configuring SIP profiles” on page 119</a> .
<b>Max channel</b>	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 <a href="#">“Configuring phone profiles” on page 122</a> .  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.
<b>Max outgoing channel</b>	With known max channels, if you need to reserve incoming channels, you may enter the number of outgoing channels allowed and the remaining channels are for incoming calls.  For example, the max channel number is 10 and you want to reserve 4 channels for incoming calls, you can enter 6 for <i>Max outgoing channel</i> .
<b>User=Phone in SIP URI</b>	Select if your service provider requires this option to make the FortiVoice unit to be compatible with the VoIP service provider's configurations.
<b>Caller ID modification</b>	Select if you want the trunk main number to appear on the called phone. See <a href="#">“Main number” on page 174</a> .  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 <a href="#">“User name” on page 174</a> .
<b>Inband ringtone</b>	Select to enable the FortiVoice unit to send ring tone to the caller of an incoming call before the establishment of a call connection.  This option is only editable if you enable early media in <a href="#">“Advanced Setting” on page 111</a> .

---

**Registration**

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.

- *Enable registration*: Select to activate the registration with the VoIP service provider. This trunk is ready to use.
- *Standard*: Select to use the standard registration method which automatically registers with the SIP server of the VoIP service provider.
- *Registrar*: Select to enter the registration information from the VoIP service provider:
  - *Registrar host/IP*: Enter the VoIP service provider's SIP registration server domain name or IP address. For example, 172.20.120.11 or voip.example.com.
  - *Registrar port*: Most SIP configurations use TCP or UDP port 5060 for SIP sessions. If your VoIP service provider uses a different port for SIP sessions, enter the port number.
  - *Transport protocol*: Select the transport protocol used for the registration.
- *Registration URI*: Enter the registration string provided by the VoIP service provider in the *Registration URI* field.

The string usually has the following formats:

```
register => user[:secret[:authuser]]@host  
[:port][:/extension]
```

or

```
register => fromuser@fromdomain:secret@host
```

or

```
register => fromuser@fromdomain:secret:  
authuser@host:port/extension
```

For example, a string could be: register =>  
2345:password@mysipprovider.com/1234

---

**Outbound Proxy**

Some VoIP service providers use proxy servers to direct its traffic. If this is the case, your registration request will go to the proxy server first before reaching the registration server. Configure the following:

- *Enable proxy*: Select to activate the proxy server settings.
- *Proxy host/IP*: Enter the proxy server's domain name or IP address. For example, 172.20.120.11 or voip.example.com.
- *Proxy port*: Enter the port number of the proxy server.
- *Transport protocol*: Select the transport protocol used for the registration.

---

**Fax**

Configure fax signal automatic detection and fax handling.

---



<b>Automatic fax detection</b>	Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically.  Selecting this option may delay the call response time on this trunk.
<b>Forward fax to eFax account</b>	Some incoming faxes' numbers do not match those of your eFax accounts. Selecting this option and a fax receiving account will send the faxes to the fax account. See " <a href="#">Forward tax to eFax account</a> " on page 181.  This option is only selectable if <i>Automatic fax detection</i> is selected.
<b>Phone Number</b>	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 173.

### 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:

<b>GUI field</b>	<b>Description</b>
<b>Test Dry Run</b>	Run a system SIP trunk test without making a real phone call.
<b>Destination number</b>	Enter a destination number to call.
<b>From number</b>	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.
<b>Test</b>	Click to start the dry run test and check the <i>Test result</i> .
<b>Reset</b>	Click to remove the test result in order to start a new test.
<b>Test Call</b>	Test the SIP trunk by making a real phone call.
<b>Destination number</b>	Enter a destination number to call.

<b>After call is established</b>	Select the FortiVoice action once it calls the destination number: <ul style="list-style-type: none"> <li>• <i>Play welcome message</i>: The FortiVoice unit will play a message to the destination number.</li> <li>• <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.</li> </ul>
<b>Test</b>	Click to start the test and check the <i>Test result</i> .
<b>Reset</b>	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 33:** Creating a SIP trunk with FortiCall service

**Create SIP Trunk**

Would you like to create SIP trunk utilizing our FortiCall service?

FortiCall

MAC Address: 000C29F6A088  
System ID: FO-SVM0000000091

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 179.
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 178.

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 179.
5. Click *Login*.

## Modifying PSTN/PRI trunks

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 FVE 200D-T, FVE 300E-T, FVE 500E-T2, FVE 1000E-T, and FVE 2000E-T2 models.

You can modify the default trunks or create new ones.

To view the PSTN trunks, go to *Trunks > PRI > PRI*.

<b>GUI field</b>	<b>Description</b>
<b>Enabled</b>	Select to activate the trunk.
<b>Name</b>	The name of the trunk.
<b>Status</b>	The trunk statuses, including: <ul style="list-style-type: none"><li>• <i>In service</i>: The trunk is currently in use.</li><li>• <i>Not activated</i>: The trunk is not enabled.</li><li>• <i>Idle</i>: The trunk is not in use.</li><li>• <i>Unavailable</i>: The trunk is not reachable.</li><li>• <i>Conflict</i>: The trunk conflicts with another one.</li><li>• <i>Alarm detected</i>: There is a problem with the trunk.</li><li>• <i>Admin down</i>: The trunk is disabled.</li></ul>
<b>Type</b>	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:

<b>GUI field</b>	<b>Description</b>
<b>Trunk Setting</b>	
<b>Name</b>	The name of this trunk. This is view only.
<b>Enabled</b>	Select to activate the trunk.
<b>Display name</b>	Enter your caller ID that will appear on the called phone, such as Example Company.
<b>Number</b>	Enter the phone number that will appear on the called phone.  If you entered the external caller ID in <a href="#">“External caller ID” on page 137</a> or <a href="#">“External caller ID” on page 155</a> , this trunk phone number will be overridden by the external caller ID.
<b>Hardware Property</b>	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 <a href="#">“Configuring the T1/E1 span” on page 182</a> .
<b>Share D-Channel (NFAS)</b>	For FVE 2000E-T2 that supports two T1/E1 voice circuit trunks - <i>pri1</i> and <i>pri2</i> , you can efficiently use your B channels on both spans by sharing the D channel to save one D channel which can be used as a B channel.  To do so: <ul style="list-style-type: none"> <li>• In the <i>D-Channel span</i> field, select the span of which you want to share the D channel.</li> <li>• Enter the channel number of <i>Backup D-channel</i> if required. 0 means no backup D channel.</li> </ul> This is useful when you have more than 3 spans.  Once you set the backup D channel, click <i>span2</i> and enter the backup D channel number in the <i>D-channel</i> field under <i>Advanced Options</i> . Make sure that this backup D channel number is not included in the channel range in the <i>B-channel</i> field.
<b>Max channel</b>	Indicates the total number of B channels on both spans.  This option is only available for FVE 2000E-T2.
<b>Max outgoing channel</b>	Enter the number of outgoing channels out of the maximum number of B channels.  This option is only available for FVE 2000E-T2.
<b>Fax</b>	Configure fax and phone signal automatic detection and fax handling.

<b>Automatic fax detection</b>	Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically.
<b>Forward tax to eFax account</b>	Select the fax receiving account for the detected faxes.
<b>Phone Number</b>	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:

<b>GUI field</b>	<b>Description</b>
<b>Analog Setting</b>	
<b>Name</b>	The name of this trunk. This is view only.
<b>Display name</b>	Enter your caller ID that will appear on the called phone, such as Example Company.
<b>Number</b>	Enter the phone number that will appear on the called phone.  If you entered the external caller ID in “ <a href="#">External caller ID</a> ” on <a href="#">page 137</a> or “ <a href="#">External caller ID</a> ” on <a href="#">page 155</a> , this trunk phone number will be overridden by the external caller ID.
<b>Enabled</b>	Select to activate the trunk.
<b>Hardware Property</b>	
<b>analog1</b>	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 “ <a href="#">Configuring the analog voice trunk</a> ” on <a href="#">page 184</a> .
<b>Port</b>	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.
<b>Fax</b>	Configure fax and phone signal automatic detection and fax handling.
<b>Automatic fax detection</b>	Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically.

<b>eFax account</b>	Select the fax receiving account for the detected faxes.
<b>Phone Number</b>	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 180.

### To configure the T1/E1 span

1. On the *PRI* page, click a span name under *Hardware Property*.
2. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Standard Options</b>	
<b>Name</b>	The name of this span. This is view-only.
<b>Type</b>	Select the span type: <i>PRI T1</i> or <i>PRI E1</i> .  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.
<b>Signalling</b>	Select the signaling type of the ISDN PRI: <ul style="list-style-type: none"> <li>• <i>PRI signalling, CPE (Customer Premises Equipment) side</i></li> <li>• <i>PRI signalling, Network Side</i></li> <li>• <i>PRI R2 signalling</i></li> </ul>
<b>Advanced Options</b>	
<b>Framing and coding option</b>	Specify the type of framing and coding to provision the PRI with your PSTN service provider.
<b>Clocking options</b>	Select the FortiVoice unit’s clock synchronization: <ul style="list-style-type: none"> <li>• Clock sourcing from PSTN network</li> <li>• Internal clocking source</li> </ul> <p>This option does not need to match that of your PSTN service provider.</p>

<b>Receive sensitivity</b>	<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>
<b>D-channel signalling format</b>	<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>
<b>Line build out</b>	<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>
<b>D-channel</b>	<p>By default, depending on your selection of “<a href="#">Type</a>” on page 182, the typical channel numbers are:</p> <ul style="list-style-type: none"> <li>• Full T1: 24</li> <li>• Full E1: 16</li> </ul> <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>B-channel</b>	<p>By default, depending on your selection of “<a href="#">Type</a>” on page 182, the typical channel settings are:</p> <ul style="list-style-type: none"> <li>• Full T1: 1-23</li> <li>• Full E1: 1-15, 17-31</li> </ul> <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"> <li>• 1-12</li> <li>• 2, 3, 4, 9-15</li> <li>• 2-4, 9-15</li> </ul> <p>The settings you configure must match the same settings of your PSTN service provider.</p>
<b>PRI R2 Settings</b>	<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 “<a href="#">Signalling</a>” on page 182.</p>
<b>Country</b>	<p>Select the country for PRI R2 settings.</p>

<b>Max ANI digits</b>	ANI (Automatic Number Identification) is a system used by telephone companies to identify the DN (Directory Number) of a calling subscriber. It allows subscribers to capture or display caller's telephone number.  Enter the number of digits of a caller's phone number to be captured.
<b>Max DNIS digits</b>	Dialed Number Identification Service (DNIS) is a service provided by telephone companies that lets the subscribers determine which telephone number was dialed by a caller.  Enter the number of digits of a dialed call to be sent by the telephone company.
<b>Caller category</b>	Select the caller type.
<b>Incoming digits mode</b>	Select the incoming digits mode by consulting your telephone company.
<b>DTMF dialing</b>	Select to enable dual-tone multi-frequency signaling (DTMF) dialing.
<b>DTMF answering</b>	Select to enable dual-tone multi-frequency signaling (DTMF) answering.
<b>Allow collect calls</b>	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 180](#).

### To configure the analog CO trunk

1. On the *Analog* page, click *Edit* under *Hardware Property*.
2. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>PSTN Analog Setting</b>	
<b>Name</b>	The name of this configuration. This is view-only.
<b>Codec</b>	Select the Codec for the trunk.
<b>Caller ID signalling</b>	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*.

<b>GUI field</b>	<b>Description</b>
<b>Fetch Office Directory</b>	Select a trunk and click this button to obtain the phone directory from this office peer.  This option only works if the PBX of the remote office is a FortiVoice unit and <i>Fetch directory</i> (see <a href="#">“Fetch Directory” on page 186</a> ) is selected on the remote unit.  You can view the directory by going to <i>Status &gt; Directory</i> and selecting this office in the <i>Office</i> field. For more information, see <a href="#">“Viewing phone directories” on page 38</a> .
<b>Enabled</b>	Select to activate this trunk.
<b>Name</b>	The name of the office peer.
<b>Display name</b>	The caller ID that will appear on the called phone, such as Example Company.
<b>Type</b>	The type of the trunk.
<b>Server</b>	The domain name or IP address of the remote office's PBX. For example, <code>172.20.120.11</code> or <code>peer.example.com</code> .
<b>Port</b>	The port number for VoIP network on the remote office's PBX.
<b>SIP Setting</b>	The SIP profile applied to this trunk.
<b>Status</b>	The status of the SIP trunk. <ul style="list-style-type: none"><li>• <i>Not registered</i>: The trunk is not registered with the VoIP service provider and is not in service.</li><li>• <i>In service</i>: The trunk is registered with the VoIP service provider and is in service.</li><li>• <i>Unavailable</i>: The trunk is not reachable.</li><li>• <i>Alarm detected</i>: There is a problem with the phone line.</li><li>• <i>Admin down</i>: The trunk is disabled.</li><li>• <i>Unmonitored</i>: The trunk is unknown.</li></ul>

### To set up an office peer

1. Go to *Trunks > Office Peers > Office Peers*.
2. Click *New*.

3. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Office Peer</b>	
<b>Name</b>	Enter a name for the trunk.
<b>Enabled</b>	Select to activate the trunk.
<b>Display name</b>	Enter the caller ID that will appear on the called phone, such as Example Company.
<b>Type</b>	Select the trunk type: <i>SIP</i> or <i>IAX2</i> .
<b>Remote server</b>	Enter the domain name or IP address of the remote office's PBX.
<b>Remote port</b>	Enter the port number for VoIP network on the remote office's PBX.
<b>SIP setting</b>	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 <a href="#">"Configuring SIP profiles" on page 119</a> .
<b>Max channel</b>	Enter the maximum voice channels for the trunk.
<b>Fetch Directory</b>	<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 &gt; Directory</i> and selecting this office in the <i>Office</i> field. For more information, see <a href="#">"Viewing phone directories" on page 38</a>.</p>
<b>Authentication Settings</b>	<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 187](#).

# 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*.

<b>GUI field</b>	<b>Description</b>
<b>Enabled</b>	Select to activate this dial plan.
<b>Name</b>	The name of the dial plan.
<b>Call handling</b>	The actions to process the incoming calls with matched dialed numbers and/or caller IDs. For details, see <a href="#">“Call Handling” on page 188</a> .
<b>Handling Description</b>	The specific call handling actions. For details, see <a href="#">“Action” on page 189</a> .
<b>From Trunk</b>	The trunks of the incoming calls that are subject to this dial plan.
<b>Match DID</b>	The phone number pattern in your dial plan that matches many different numbers. For details, see <a href="#">“Dialed Number Match” on page 188</a> .
<b>Match CID</b>	The caller ID pattern for this dial plan. For details, see <a href="#">“Caller ID Match” on page 188</a> .

### To set up an inbound dial plan

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

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for this plan.
<b>Enabled</b>	Select to activate this dial plan.

<b>From Trunk</b>	<p>Select the trunks of the incoming calls that are subject to this dial plan.</p> <p>Select the trunks in the <i>Available</i> field and click -&gt; to move them into the <i>Selected</i> field.</p>
<b>Dialed Number Match</b>	<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 called numbers matching this pattern will follow this dial plan rule.</p> <p>Create the number match following <a href="#">“Pattern-matching syntax” on page 195</a> and <a href="#">“Pattern-matching examples” on page 195</a>.</p>
<b>Caller ID Match</b>	<p>Click <i>New</i> to set the caller ID pattern following <a href="#">“Pattern-matching syntax” on page 195</a> and <a href="#">“Pattern-matching examples” on page 195</a> 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>
<b>Caller ID modification</b>	<p>Select one or more caller ID modification configurations. You can associate multiple caller ID modification configurations with a dial plan. For more information on caller ID modification, see <a href="#">“Modifying caller IDs” on page 120</a>.</p>
<b>Call Handling</b>	<p>Select the actions to process the incoming calls with matched dialed numbers and/or caller IDs.</p>
<b>Action type</b>	<p>Select the type of action for the plan and configure the actions accordingly. See <a href="#">“Action” on page 189</a>.</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> </ul>

---

**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 FortiVoice schedule, see [“Scheduling the FortiVoice unit” on page 131](#).
  - b. Select an action for the incoming calls under this plan.  
For some actions, you need to enter the extension (such as *Go voicemail*) or select a profile (such as *Play announcement*).
  - c. Click *Create*.
  - d. Repeat this procedure if you need more actions for this action type.  
Do not use the same schedule for more than one action to avoid schedule conflict.
- If you select the *Dial local number* type:
  - a. Click *New* to add the number pattern in the *Value* field following [“Pattern-matching syntax” on page 195](#) and [“Pattern-matching examples” on page 195](#) 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 191](#).

To view the DIDs, go to *Call Routing > Inbound > DID Mapping*.

<b>GUI field</b>	<b>Description</b>
<b>Enabled</b>	Select to activate this DID.
<b>Rule Name</b>	The name of the DID.
<b>Incoming Trunk</b>	The trunk used for dialing the DIDs.
<b>Schedule</b>	The schedule to apply the rule.
<b>Caller ID modification</b>	The caller ID modification configuration. For more information, see <a href="#">"Inbound caller ID modification" on page 190</a> .

### To configure a DID

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

<b>GUI field</b>	<b>Description</b>
<b>DID Rule</b>	
<b>Rule name</b>	Enter a name for this DID setting.
<b>Enabled</b>	Select to activate this DID setting.
<b>Trunk</b>	Select the trunk used for dialing the DIDs.
<b>Schedule</b>	Select a schedule to apply the rule. For information on creating schedules, see <a href="#">"Scheduling the FortiVoice unit" on page 131</a> .
<b>Inbound caller ID modification</b>	Select the caller ID modification configuration. For more information on caller ID modification, see <a href="#">"Modifying caller IDs" on page 120</a> .

<b>Inbound fallback action</b>	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 <a href="#">“Mapping DIDs” on page 191</a> .
<b>Number Mapping</b>	For adding a number mapping, see <a href="#">“Mapping DIDs” on page 191</a> .  Click <i>Export</i> to open or save the number mapping file and <i>Import</i> to browse for a number mapping file.

## Mapping DIDs

You can map a DID number to one extension. You can also map a DID to multiple extensions based on the callers' phone numbers. For example, calling numbers 123-4567, 123-4568, and 123-4569 can call the DID number 222-1000 to reach extension 1234. Calling numbers 234-4567, 234-4568, and 234-4569 can call the same DID number 222-1000 to reach extension 1265. In both cases, the calling numbers will display on the extension.

If a caller outside the configured caller list dialed the mapped DID number, the FortiVoice unit will react according to the selected fall back action. For details, see [“Inbound fallback action” on page 191](#).

### To map DIDs

1. Go to *Call Routing > Inbound > DID Mapping*.
2. Click *New*.
3. In *Number Mapping*, click *New*.
4. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Map Setting</b>	This option allows you to map a DID number to an extension.
<b>DID number</b>	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 <a href="#">“Advanced Setting” on page 192</a> ). Otherwise, an error message about duplicate entry appears and the DID mapping configuration cannot be saved.
<b>Extension</b>	Enter the extension that you want to map to the DID number.

<b>Option</b>	<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 “<a href="#">Inbound fallback action</a>” on <a href="#">page 191</a>. 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 “<a href="#">Main number</a>” on <a href="#">page 106</a>) or the trunk phone number (see “<a href="#">Phone Number</a>” on <a href="#">page 177</a>) associated with the extension. Alternatively, you can choose the caller ID to display on the called phone when configuring an extension (see “<a href="#">External caller ID</a>” on <a href="#">page 137</a>).</p> <p>By default, both <i>Inbound</i> and <i>Outbound</i> are selected.</p>
<b>Advanced Setting</b>	<p>This option allows you to bundle caller numbers to a DID number which can be mapped to any extension.</p>
<b>Caller number</b>	<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 “<a href="#">Pattern-matching syntax</a>” on <a href="#">page 195</a> and “<a href="#">Pattern-matching examples</a>” on <a href="#">page 195</a>.</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*.

<b>GUI field</b>	<b>Description</b>
------------------	--------------------



<b>Test</b>	Select to test if the dial plan is created successfully. For more information, see <a href="#">“Testing outbound dial plans”</a> on page 194.
<b>Enabled</b>	Select to activate this dial plan.
<b>Name</b>	The name of the dial plan.
<b>Pattern</b>	The phone number pattern in the dial plan that matches other numbers. For details, see <a href="#">“Dialed Number Match”</a> on page 193.
<b>Match CID</b>	The caller ID pattern for this dial plan. For details, see <a href="#">“Caller ID Match”</a> on page 193.
<b>Call handling</b>	The call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern. For details, see <a href="#">“Call Handling”</a> on page 193.

### To set up an outbound dial plan

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

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for this plan.
<b>Enable</b>	Select to activate this dial plan.
<b>Emergency call</b>	Select to allow emergency call with this plan. By default, this is selected.  For information on setting emergency number, see <a href="#">“Setting PBX location and contact information”</a> on page 105.
<b>Dialed Number Match</b>	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 <a href="#">“Creating dialed number match”</a> on page 194.
<b>Caller ID Match</b>	Click <i>New</i> to set the caller ID pattern following <a href="#">“Pattern-matching syntax”</a> on page 195 and <a href="#">“Pattern-matching examples”</a> on page 195 for this dial plan, and click <i>Create</i> .  You can enter a caller’s display name string or the caller’s phone number string as the pattern.  Callers with IDs under this pattern are subject to this plan.
<b>Call Handling</b>	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 <a href="#">“Configuring call handling actions”</a> on page 196.

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 193.

### 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:

<b>GUI field</b>	<b>Description</b>
<b>Test Call - Dry Run</b>	Run a system outbound dial plan test without making a real phone call.
<b>Destination number</b>	Enter a destination number to call.
<b>From number</b>	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.
<b>Test</b>	Click to start the dry run test and view the <i>Test result</i> .
<b>Reset</b>	Click to remove the test result in order to start a new test.
<b>Test Call</b>	Test the outbound dial plan by making a real phone call.
<b>Destination number</b>	Enter a destination number to call.
<b>After call is established</b>	Select the FortiVoice action once it calls the destination number: <ul style="list-style-type: none"> <li>• <i>Play welcome message</i>: The FortiVoice unit will play a message to the destination number.</li> <li>• <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.</li> </ul>
<b>Test</b>	Click to start the test and view the <i>Test result</i> .
<b>Reset</b>	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 17:**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 18:**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 Routing > Outbound > Outbound*.
2. Click *New*.
3. In *Dialed Number Match*, click *New*.
4. Configure the following:

GUI field	Description
<b>Match Pattern</b>	
<b>New</b>	Click to add the number pattern in the <i>Value</i> field following “ <a href="#">Pattern-matching syntax</a> ” on page 195 and “ <a href="#">Pattern-matching examples</a> ” on page 195 for this dial plan. Repeat to add more patterns.
<b>Modification</b>	You can manipulate the number patterns you entered.
<b>Strip</b>	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.

<b>Prefix</b>	<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>
<b>Postfix</b>	<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:

<b>GUI field</b>	<b>Description</b>
<b>Call Handling</b>	
<b>Schedule</b>	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 “ <a href="#">Scheduling the FortiVoice unit</a> ” on page 131.
<b>Action</b>	Select the call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern.
<b>Outgoing trunk</b>	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 “ <a href="#">Configuring Trunks</a> ” on page 173.
<b>Caller ID modification</b>	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 “ <a href="#">Modifying caller IDs</a> ” on page 120.

---

**Warning message** If you select *Allow with warning* or *Deny with warning* in the *Action* field, select the sound file for the warning. Click *Edit* to modify the selected file or click *New* to configure a new one. For more information on sound files, see [“Managing sound files and music on hold” on page 117](#).

---

**Delay** Optionally, if you want to discourage certain users for making outbound calls, enter the call delay time in seconds.

---

5. Click *Create*.

# Setting up a Call Center

A call center allows an organization to receive or transmit a large volume of requests by telephone in a centralized office.

You can configure a call center and operate the center on the user web portal.

This option is only available if you have purchased a call center license.

This topic includes:

- [Creating call queues](#)
- [Configuring agents](#)
- [Configuring IVRs](#)
- [Configuring surveys](#)
- [Configuring other agent information](#)
- [Configuring agent profiles](#)
- [Working with call queue statistics](#)
- [Configuring call center report profiles and generating reports](#)

## 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 187](#).

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 Center > Call Queue > Call Queue*.

<b>GUI field</b>	<b>Description</b>
<b>Queue ID</b>	The name of the call queue.
<b>Display Name</b>	The queue name displaying on the queue extension.

<b>Number</b>	The extension number for the call queue.
<b>Department</b>	The departments of the agents enrolled in the queue.
<b>Agents</b>	The extensions of the agents enrolled in the queue.

### To create a call queue

1. Go to *Call Center > Call Queue*.
2. Click *New* and configure the following.

<b>GUI field</b>	<b>Description</b>
<b>Call Queue</b>	
<b>Queue ID</b>	Enter an ID for the queue.
<b>Number</b>	<p>Enter an extension for callers to dial and enter into a call queue following the extension number pattern. See <a href="#">“Configuring PBX options” on page 106</a>.</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>
<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers” on page 141</a>.</p>

3. Click *Create*.
4. From the call queue list, select the queue you just create.
5. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Call Queue</b>	

<b>Number</b>	<p>Enter an extension for callers to dial and enter into a call queue following the extension number pattern. See <a href="#">“Configuring PBX options” on page 106</a>.</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>
<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers” on page 141</a>.</p>
<b>Status</b>	Select to enable the call queue.
<b>Display name</b>	Enter the queue name displaying on the queue extension, such as Support.
<b>Description</b>	Enter any notes about this queue.
<b>Department</b>	Select the department to which the queue belongs. For information on creating departments, see <a href="#">“Creating extension departments” on page 164</a> .
<b>Queue Setting</b>	
<b>Maximum queue capacity</b>	<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 <i>Queue Overflow</i> call handling action you set in <a href="#">“Queue Overflow” on page 206</a>.</p> <p>The maximum is 100.</p>
<b>Maximum queuing time</b>	<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 in <a href="#">“Queue Timeout” on page 206</a>.</p> <p>The maximum is 720 minutes.</p>
<b>Ring duration</b>	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.
<b>Music on hold</b>	Select a sound file or music on hold file to play when a caller is waiting. For more information, see <a href="#">“Managing sound files and music on hold” on page 117</a> .



---

## Call Distribution

---

- Skill Based Routing** Select and choose a call routing option. This option is based on agent skill level scores. For more information, see [“Creating agent skill levels” on page 217](#).
- **Lowest level first:** The call will ring the agent with the lowest skill level score first and move up the rank if the agent is unable to take the call, that is, the agent’s extension is in a Not Ready status.
  - **Highest level first:** The call will ring the agent with the highest skill level score first and move down the rank if the agent is unable to take the call, that is, the agent’s extension is in a Not Ready status.

---

**Default skill** Select the group, such as Billing, Sales, or Support, that the call distribution is executed. You can add a new skill or modify an existing one. For more information, see [“Adding agent skill sets” on page 216](#).

- 
- Distribution policy** Select a call *Distribution policy*.
- This option works like following:
- If *Skill Based Routing* is not selected, calls are distributed according to the policy you choose.
  - If *Skill Based Routing* is selected, calls are distributed according to the skill based call routing option you choose. This option only applies to the situation when you have agents with the same skill level in a queue. In such cases, calls are distributed to these agents according to the policy you choose.
    - *Ring all:* rings all available agents (default).
    - *Round robin:* rings all agents in a queue equally in some rational order, usually from the top to the bottom of a list and then starting again at the top of the list and so on.
    - *Sequential:* rings each agent in a sequential manner regardless of whether they have answered calls.
    - *Random:* rings an agent at random.
    - *Least recent:* rings the agent that least recently received a call.
    - *Fewest calls:* rings the agent that has completed the fewest calls in this queue.
    - *Weight random:* rings a random agent, but uses the agent’s number of received calls as a weight.
    - *Priority based:* rings agents based on call answering priorities for callers entering the call queue. A new call always starts with the lowest priority. However, a queue manager with privileges can change the priority of a call on the agent console of the user web portal. See [“Setting caller priorities” on page 217](#).

---

## Additional Settings

---

---

**Distinctive settings for agent**

*Announce queue name:* Select a sound file that announces the queue name. You can add a new one or modify an existing one. For more information, see [“Managing sound files and music on hold” on page 117](#).

*Caller ID option:* Select how you want the IDs of the calls to this queue to display. If you select *Prefix*, the queue [Display name](#) is added before the caller ID on the agent’s phone. If you select *Replace*, the queue [Display name](#) replaces the caller ID on the agent’s phone.

*Ring Pattern:* Select a queue extension ring pattern.

---

**Business schedule**

Click >> and 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. For information on scheduling, see [“Scheduling the FortiVoice unit” on page 131](#).

---

**Announcement to caller**

*Announce holdtime:* Select if you want to announce the queue waiting time to a caller at the set interval. You may also select to announce only once.

*Announce position:* Select to announce a caller’s waiting position in the queue, such as “You are caller No. 5 in the call queue”.

*No:* Do not announce a caller’s position.

*Always:* Always announce a caller’s position.

*Abbreviated:* Announce a caller’s position only once if the caller is over the marked position and always announce once the caller is within the marked position.

*Minimal:* Announce only when the caller is within the marked position.

*Mark position:* Enter the benchmark for selecting *Abbreviated* or *Minimal* setting.

For example, if you select *Abbreviated* and enter 5, a caller’s position is announced when the caller becomes No. 5 in the queue and announced only once before the caller becomes No. 5 in the queue.

*Announcement interval:* Enter the announcement frequency in seconds.

**Custom announcement:** You can also customize the announcement settings.

- *Mode:* Select the method of greeting announcement to the caller once the caller enters this call queue. You can also select to diable this function.

If you select *Periodic* or *Random*, enter the announcement frequency in seconds in *Announcement interval*.

- *Audio:* Select a greeting sound file for the announcement. For more information, see [“Managing sound files and music on hold” on page 117](#).
-

---

**Service Level**

*Interval:* Enter the time period in minutes for calculating the threshold.

*Threshold:* Enter the call answering rate for a certain period of time. The action triggered by the threshold being reached is configured in [“Call Handling” on page 205](#).

*Service level low threshold is used in call handling:* Click *Service level low call handling* to configure how other callers will be dealt with according to the *Queue Overflow* call handling action you set in [“Service Level Low” on page 206](#) when the call queue is full

---

**Alert Settings**

*Alert Event:* Select the event that triggers an action which is configured in [“Call Handling” on page 205](#).

*Send alert email:* Select if you want to send an email when an alert event is triggered. Click *New* to enter an email address.

*Call extension/number:* Select this option and an extension number if you want a phone call when an alert event is triggered. Click *New* to add an extension.

*GUI popup:* Select to have a popup notification on the user web portal GUI when an alert event is triggered. This only applies to agents with the particular privilege called *Queue alert*. See *Agent Console Privilege* in [“Configuring agent profiles” on page 218](#).

*Alert interval:* Enter a value in minutes during which time no alert is sent. For example, if you enter 60, you will not receive any alerts for an hour even if an alert event is triggered. This will be the case each time when you receive an alert notification.

If you enter 0, you will receive notifications each time when an event is triggered.

---

**Callback Setting**

This option allows callers waiting in a queue to request a callback following the recorded instructions and wait for an agent to return their call.

*Status:* Select to enable this option.

*Callback mode:*

- *Agent call back manually(from call center console):* Select to allow an agent to manually call the caller using the agent console on the user web portal.
  - *System call back automatically:* Select to allow the FortiVoice unit to call the caller automatically based on the callback number collected when an agent is available.
-

---

	<p><i>Prompt to caller to leave the call back number:</i> Select the method to collect the callback number.</p> <ul style="list-style-type: none"> <li>• <i>System default:</i> Select to use system defined voice file.</li> <li>• <i>User defined IVR:</i> Select to use user configured IVR.</li> </ul> <p>For more information on IVR, see <a href="#">“Configuring IVRs” on page 208.</a></p>
	<p><i>Prompt to caller after callback call established:</i> Select to ring the caller when a callback call is set up.</p>
<b>Survey Setting</b>	<p>Surveys are used to collect customer feedback to ensure that the service delivered by your call center agents consistently meets corporate standards and drives high customer satisfaction.</p>
	<p><i>Status:</i> Select to enable this option.</p>
	<p><i>Survey:</i> Choose the survey configuration for the call queue. For more information on surveys, see <a href="#">“Configuring surveys” on page 214.</a></p>
<b>Agent</b>	
<b>Agent type</b>	<p>Select the agent login mode.</p> <p>Once enrolled into the queue, static agents are always connected to the queues while dynamic agents need to log into the queue in order to process calls.</p> <p>For information on enrolling agents into a queue, see <a href="#">“Agent members” on page 205.</a></p>
<b>Auto-logout time</b>	<p>If you select <i>Dynamic</i> login mode, enter the agent login expiry time in hours. For example, if you enter 5, the agent will be logged out 5 hours after having logged into the queue.</p>
<b>Logout all agents after scheduled business hour</b>	<p>Select to log out all agents in the queue when the scheduled business hour is due.</p>
<b>Wrap up time</b>	<p>Enter the time (in seconds) needed by agents to complete a queue call including taking notes or record-keeping, starting from the moment that call is hang up.</p> <p>The default is 0 second.</p>
<b>Wrap up outgoing call</b>	<p>Select if the agent needs to make an outgoing customer call and time to take notes or record-keeping, starting from the moment that call is hang up.</p> <p>You can enter the wrap up time in the <a href="#">“Wrap up time”</a> field.</p>

---

<b>Call waiting</b>	<p>Select this option so that if an agent is on the phone when a queue call comes in, the caller information will display on the agent's phone. The agent can choose to answer the call or not. If the agent does not answer the call, after the ring duration is due, the call is transferred to the next agent.</p> <p>This option is different from the call waiting feature of a regular extension (See "<a href="#">Setting extension user preferences</a>" on <a href="#">page 154</a>). On a regular extension, the call waiting feature only applies to the calls that directly go to the extension. On a queue extension, the call waiting feature only applies to the calls that go to the extension from the queue.</p>
<b>Agent members</b>	<ul style="list-style-type: none"> <li>• Click to expand <i>Agent members</i> for enrolling agents into the queue.</li> <li>• In the <i>Available</i> field, select the agents for this queue.</li> <li>• Click -&gt; to move it into the <i>Selected</i> field.</li> <li>• Click <i>Done</i>.</li> </ul> <p>You can type an agent's extension or name in the <i>Search</i> field and press Enter to search for the agent.</p>
<b>Call Handling</b>	
<b>When no logged-in agent</b>	<p>You may select to queue a caller or not if there is no agents available.</p> <p>If you select <i>Do not queue</i>, an incoming call will be handled by your general call handling configuration, such as auto attendant.</p> <p>This option is only available if agent type is <i>Dynamic</i>.</p>
<b>Scheduled Business Hour call handling</b>	<p>Click to configure the business hour call handling action for the queue. For details, see "<a href="#">Configuring scheduled business hour queue call handling actions</a>" on <a href="#">page 205</a>.</p>
<b>Non Scheduled Business Hour call handling</b>	<p>Click to configure the non business hour call handling action for the queue. For details, see "<a href="#">Configuring scheduled business hour queue call handling actions</a>" on <a href="#">page 205</a>.</p>

6. Click *OK*.

### Configuring scheduled business hour queue call handling actions

Configure the call handling action for the queue. This action applies to all calls once they enter into the queue.

This option is only available when you edit a queue.

#### To configure the call handling action

1. Go to *Call Center > Call Queue*.
2. Select a call queue for which you want to configure queue call handling actions and click *Edit*.
3. In *Call Handling*, click *Scheduled Business Hour call handling*.

- Configure the situation upon which the FortiVoice unit can be configured to take corresponding actions:

<b>GUI field</b>	<b>Description</b>
<b>Queue Overflow</b>	<p>The situation when callers exceed the maximum waiting callers you set. See <a href="#">“Maximum queue capacity” on page 200</a>.</p> <p>A popup notification appears when this barometer is triggered.</p>
<b>Queue Timeout</b>	<p>Callers waiting time exceeds the maximum waiting time set in <a href="#">“Maximum queuing time” on page 200</a>.</p> <p>A popup notification appears when this barometer is triggered.</p>
<b>Service Level Low</b>	<p>Service level represents the maximum amount of time a caller should ideally have to wait before being presented to an agent. You need to set service level and service level interval in the FortiVoice CLI.</p> <p>For example, if service level interval is set to 60 seconds and the service level percentage is 80 percent, that means 80 percent of the calls that came into the queue were presented to an agent in less than 60 seconds. Any service level percentage lower than 80 is considered to be low.</p>
<b>All Agents Logout</b>	<p>There are no agents in the queue to answer calls. The action for this option only works if you select <i>Queue caller</i> for <a href="#">“When no logged-in agent” on page 205</a>.</p>
<b>All Agents Paused</b>	<p>There are no agents in the queue to answer calls. The action for this option only works if you select <i>Queue caller</i> for <a href="#">“When no logged-in agent” on page 205</a>.</p>
<b>Unclassified</b>	<p>Any reason that you need to schedule call handlings.</p>
<b>Call Processing</b>	<p>Click <i>New</i> to configure call handling action for the situation you selected.</p> <p>For some processes that may require further actions, you need to add one or more call processes to complete the call handling. For example, after adding a process that contains a <i>Set call queue priority</i> action, you can add another process with a <i>Transfer to queue</i> action to complete the call handling. In this case, the call will be processed again with new priority after it is transferred to the queue.</p>
<b>Schedule</b>	<p>Select the FortiVoice operation schedule to implement this call handling action. For more information on schedules, see <a href="#">“Scheduling the FortiVoice unit” on page 131</a>.</p>
<b>Action</b>	<p>Select the call handling action. Depending on the action selected, further configuration may be needed. For example, if you select <i>Dial extension</i> for <i>Action</i>, enter the extension to which a call is transferred.</p>

- Click *Create*, then *OK*.

## Configuring non scheduled business hour queue call handling actions

Configure the call handling action for the queue. This action applies to all calls once they enter into the queue.

For some processes that may require further actions, you need to add one or more call processes to complete the call handling. For example, after adding a process that contains a *Set call queue priority* action, you can add another process with a *Transfer to queue* action to complete the call handling. In this case, the call will be processed again with new priority after it is transferred to the queue.

This option is only available when you edit a queue.

### To configure the call handling action

1. Go to *Call Center > Call Queue*.
2. Select a call queue for which you want to configure queue call handling actions and click *Edit*.
3. In *Call Handling*, click *Non Scheduled Business Hour call handling*.
4. On the *Call Processing* page, click *New* to configure call handling action.
5. For *Schedule*, select the FortiVoice operation schedule to implement this call handling action. For more information on schedules, see “[Scheduling the FortiVoice unit](#)” on [page 131](#).
6. For *Action*, select the call handling action. Depending on the action selected, further configuration may be needed. For example, if you select *Dial extension* for *Action*, enter the extension to which a call is transferred.
7. Click *Create*, then *OK*.

## Configuring agents

Extensions with call center agent function enabled can be further configured with other call center information, such as agent profile, managed departments, and skill sets. Call center departments can also be set up to form the basis for department management.

### To configure an agent

1. Go to *Call Center > Agents > Agents*.  
All extensions with call center agent function enabled display. Clicking *Extensions* opens the IP extensions configuration page. For information, see “[Configuring IP extensions](#)” on [page 134](#).
2. Select the extension you want to configure and click *Edit*.
3. Select an agent profile. For more information, see “[Configuring agent profiles](#)” on [page 218](#).
4. For *Managed departments*, click *>>*.
5. Select the departments to be managed by this agent if required, and click *Done*.
6. Click *Member of Queues* to select the call queues to join.
  - *Main/Outgoing queue*: This option is for collecting the outgoing calls from all queues by this agent and displaying them in “[Working with call queue statistics](#)” on [page 219](#). You can select any queue of which this agent is a member for that purpose except *None* which will not collect agent’s outgoing call information.
  - *Queues*: Select the queues of which you want the extension/agent to be a member, and click *Apply*.
7. Add skill sets for the agent by clicking *New* under *Skill Sets*.

8. Select the skill set for the agent, including skills and level, and click *Create*. For more information about agent skills and levels, see “Adding agent skill sets” on page 216 and “Creating agent skill levels” on page 217.
9. Click *OK*.

#### To set up a department

1. Go to *Call Center > Agents > Department*.
2. Click *New* and configure the following:

<i>GUI field</i>	<i>Description</i>
<b>Department</b>	
<b>Name</b>	Enter a name for the department.
<b>Comment</b>	Click <i>Click to edit</i> and enter any notes you have for this department.
<b>Call Center</b>	
<b>Manager</b>	From the <i>Available</i> extension list, select the ones to be department managers and click <i>Done</i> .  Managers can view call queue reports.
<b>Member</b>	From the <i>Available</i> extension list, select the ones to be members of the department and click <i>Done</i> .  Each member can only belong to one department.
<b>Queue</b>	From the <i>Available</i> extension list, select the ones to be call queues of the department and click <i>Done</i> .  Each queue can only belong to one department.

3. Click *Create*.

## Configuring IVRs

FortiVoice Interactive Voice Response (IVR) function allows it to interact with callers through the use of voice and DTMF tones input via keypad. Callers proceed according to the IVR audio instructions to reach the callees or get the information they need.

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

FortiVoice IVR interfaces with RESTful Web service for querying caller information from the database.

This topic includes:

- [Setting up an IVR](#)
- [Configuring restful service](#)

## Setting up an IVR

*Call Center > IVR > IVR* allows you to view the existing IVR list and create new IVRs.



Creating new IVRs includes configuring:

- SIP header collector to share IVR information among multiple FortiVoice units based on information gathered by digit and RESTful collectors (see [To configure a SIP header collector](#))
- the digits collector to collect digit inputs from callers (see [To configure a digit collector](#))
- the RESTful collector to gather caller information from database (see [To configure a restful collector](#))
- call handling to route the calls based on information gathered by digit and RESTful collectors, and
- error handling to deal with unknown errors and RESTful service errors.

#### **To view the IVR list**

1. Go to *Call Center > IVR > IVR*.
2. Click the *Expand all* icon.

The IVR tree list displays. Under each IVR name, configuration items are listed. Clicking an item opens its configuration page.

#### **To configure a SIP header collector**

1. Go to *Call Center > IVR > IVR* and click the *Switch* icon.
2. Click *New* and type the name of the IVR and description.
3. Click *Create*.
4. From the IVR name list, select the name you created and click *Edit* to open the IVR configuration page.
5. For *Description*, select *Click to edit* to enter any notes you have for the IVR.

6. Click *Add SIP header collector*..

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for the SIP header collector.
<b>Description</b>	Enter any notes you have for the SIP header collector.
<b>Variable</b>	<p>Click <i>New</i> and do the following:</p> <ol style="list-style-type: none"><li>1. For <i>Variable</i>, enter a value for a SIP header field based on your organization's SIP header definitions, for example, <i>ticket_id</i>. This value must be the same on every FortiVoice unit that shares IVR information.</li><li>2. For <i>Share with</i>, do the following:<ul style="list-style-type: none"><li>• <i>None</i>: Select if you do not want to share the information that the SIP header collector gathers with other interfaces.</li><li>• <i>Agent console name</i>: Select if you want agents in the queues where the IVR calls are routed to see the information that the SIP header collector gathers. Enter a name for the information to display on the agent console.</li><li>• <i>SIP header name</i>: Select if you want to share the information that the SIP header collector gathers with other SIP header collectors. Enter a value in the <i>Name</i> field that matches the value on the SIP header to enable information sharing.</li><li>• <i>Remote CDR name</i>: Select if you want to share the information that the SIP header collector gathers with a remote CDR database. Enter a value in the <i>Name</i> field that matches the value on the remote CDR to enable information sharing.</li></ul></li><li>3. Click <i>Create</i>, then <i>Create</i>.</li></ol>

You can create a maximum of 10 SIP header collectors which are saved as variables.

**To configure a digit collector**

1. After configuring the SIP header collector, click *Add digit collector* to configure digit inputs collection from callers. You can create a maximum of 10 digits collectors.

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for the digit collector.
<b>Prompt</b>	Select the audio file that you want callers to listen to. You can also create a new file or edit the selected one. For more information, see <a href="#">“Managing sound files and music on hold”</a> on page 117.
<b>Enable read back</b>	Select if you want the digit inputs to be read out to the caller.

<b>Share with</b>	<p><i>None:</i> Select if you do not want to share the information that the digit collector gathers with other interfaces.</p> <p><i>Agent console name:</i> Select if you want agents in the queues where the IVR calls are routed to see the information that the digit collector gathers. Enter a name for the information to display on the agent console.</p> <p><i>SIP header name:</i> Select if you want to share the information that the digit collector gathers with SIP header collector. Enter a value in the <i>Name</i> field that matches the value on the SIP header to enable information sharing.</p> <p><i>Remote CDR name:</i> Select if you want to share the information that the digit collector gathers with a remote CDR database. Enter a value in the <i>Name</i> field that matches the value on the remote CDR to enable information sharing.</p>
<b>Description</b>	Enter any notes you have for the digit collector.
<b>Digits Settings</b>	
<b>Min digits</b>	Enter the minimum digits the digits collector allows. The range is 1-30.
<b>Max digits</b>	Enter the maximum digits the digits collector allows. The range is 1-30.
<b>Max invalid input allowed</b>	Enter the number of times a caller is allowed for inputting wrong digits. The call will be terminated if the limit is reached. The range is 0-10.
<b>Timeout</b>	Enter the time limit that a caller is allowed for taking NO action after the call is put through. The call will be terminated if the time limit is reached. The range is 0-600 seconds.
<b>Max timeout allowed</b>	<p>Enter the number of timeouts a caller is allowed for taking no action after the call is put through. The call will be terminated if the number of timeouts limit is reached. The range is 0-10.</p> <p>For example, if <i>Timeout</i> is set to 10 seconds and <i>Max timeout allowed</i> to 3, a caller would have a total of 30 seconds timeout time after he or she dials in and takes no action afterwards.</p>

2. Click *Create*.

You can create a maximum of 10 digit collectors which are saved as variables.

**To configure a restful collector**

1. After configuring the digit collector, click *Add restful collector* to configure the database collector for resource querying.

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for the restful collector.
<b>Service</b>	Select the restful service for the collector. You can also create a new service or edit the selected one. For more information, see <a href="#">“Configuring restful service” on page 214</a> .

<b>Method</b>	Choose the method to submit the information collected by the FortiVoice IVR system to the database server (as HTTP POST or HTTP GET) and use the value as a variable in your SQL statement.
<b>Parameters</b>	<p>Select <i>Click to edit</i> to enter query parameters to customize the results returned from a GET or POST operation on the database, such as sorting or filtering.</p> <p>Optionally, click <i>Add variable</i> to insert self or system defined variables into the parameters.</p>
<b>URL</b>	
<b>Posting HTTP Headers</b>	<p>Select <i>Click to edit</i> to enter a HTTP header for information querying on the RESTful web service.</p> <p>Optionally, click <i>Add variable</i> to insert self or system defined variables into the HTTP header.</p> <p>This option is only available if you select <i>Post</i> for <i>Method</i>.</p>
<b>Posting Message Body</b>	<p>Select <i>Click to edit</i> to enter a HTTP message body for information querying on the RESTful web service.</p> <p>Optionally, click <i>Add variable</i> to insert self or system defined variables into the HTTP body.</p> <p>This option is only available if you select <i>Post</i> for <i>Method</i>.</p>
<b>Timeout</b>	Enter the time allowed for the query to be processed. If the time elapses before the query response is complete, partial information may be returned. The range is 0-600 seconds.
<b>Max retry allowed</b>	Enter the number of database query tries allowed. The query will be denied if the retry limit is reached. The range is 0-10.
<b>Description</b>	Enter any notes you have for the restful collector.
<b>New (under Fields)</b>	Click to name each of the attributes returned from a database query to present it or use it as a variable.
<b>Field</b>	Enter a name for the attribute you want to define.
<b>Query</b>	Enter the query parameter for the attribute you want to define. Optionally, click <i>Add variable</i> to insert self or system defined variables into the parameter.

---

**Share with**

*None*: Select if you do not want to share the information that the restful collector gathers with other interfaces.

*Agent console name*: Select if you want agents in the queues where the IVR calls are routed to see the information that the restful collector gathers. Enter a name for the information to display on the agent console.

*SIP header name*: Select if you want to share the information that the restful collector gathers with SIP header collector. Enter a value in the *Name* field that matches the value on the SIP header to enable information sharing.

*Remote CDR name*: Select if you want to share the information that the restful collector gathers with a remote CDR database. Enter a value in the *Name* field that matches the value on the remote CDR to enable information sharing.

---

2. Click *Create* and then *Create*.

You can create a maximum of 10 restful collectors which are saved as variables.

**To configure IVR handling**

1. After configuring the restful collectors, click *Add IVR handling* to configure call processing using the digit and restful collector configurations.

SIP header, digit and restful collector configurations only take effect after IVR handling is set up.

---

<b>GUI field</b>	<b>Description</b>
<b>Condition</b>	Configure the conditions based on which call processing actions are taken.
<b>Unconditional</b>	Select if you do not need to configure the conditions. In this case, the system default condition applies.
<b>Variable</b>	Click <i>Add</i> to insert self or system defined digit or restful variable for the condition.  This option appears if you deselect <i>Unconditional</i> .
<b>Operator</b>	Use query operators to assign a value to the variable, or perform mathematical operations.  This option appears if you deselect <i>Unconditional</i> .
<b>Value</b>	Enter the value assigned by the operator to the variable. Optionally, click <i>Add variable</i> to insert self or system defined variables into the value.  This option appears if you deselect <i>Unconditional</i> .
<b>Description</b>	Enter any notes you have for the IVR handling.
<b>Action</b>	Click <i>New</i> to configure the actions to take based on the conditions.

---

<b>Action type</b>	Select the IVR action. Depending on the action type selected, further configuration may be needed. For example, if you select <i>Dial extension</i> , enter the extension to which a call is transferred.  Click <i>Create, Create</i> .  You can create multiple actions.
--------------------	--

#### To configure error handling

1. After configuring IVR handling, click *Add error handling* to deal with unknown errors and restful service errors.
2. For *Error Type*, select *Unspecified* for unknown errors and *Restful* for restful service errors.
3. For *Action*, click *New*.
4. Select the action. Depending on the action type selected, further configuration may be needed. For example, if you select *Dial extension*, enter the extension to which a call is transferred.
5. Click *Create, Create*.
6. Click *OK* to complete the IVR configuration.

#### See also

- [Configuring restful service](#)

## Configuring restful service

FortiVoice IVR interfaces with restful web service for querying caller information from the database.

*Call Center > IVR > Restful service* allows you to configure the restful web service.

#### To configure restful service

1. Go to *Call Center > IVR > Restful service*, click *New* and do the following:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for the configuration.
<b>Protocol</b>	Select the protocol for the service.
<b>Base URL</b>	Enter the URL of the server hosting restful service.  Click <i>Test</i> to validate the URL.
<b>Authentication</b>	Select to enter the user name and password for logging onto the restful server.
<b>SSL verification</b>	Select if required.
<b>Description</b>	Click <i>Click to edit</i> to enter any notes for the configuration.

## Configuring surveys

You can use surveys to collect customer feedback to ensure that the service delivered by your call center agents consistently meets corporate standards and drives high customer satisfaction. You can also set survey rules.

### To configure a survey

1. Go to *Call Center > Survey > Survey*.
2. Click *New* and type the name of the survey.
3. Click *Create*.
4. From the survey name list, select the name you created and click *Edit* to open the survey configuration page.
5. Click *Add digit collector* to configure collecting digit inputs from callers. You can create a maximum of 10 digits collectors.

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for the digits collector.
<b>Prompt</b>	Select the audio file that you want callers to listen to. You can also create a new file or edit the selected one. For more information, see <a href="#">“Managing sound files and music on hold” on page 117</a> .
<b>Enable read back</b>	Select if you want the digit inputs to be read out to the caller.
<b>Question</b>	Enter the survey question.
<b>Digits settings</b>	
<b>Max digits</b>	Enter the maximum digits the digits collector allows. The range is 1-30.
<b>Max invalid input allowed</b>	Enter the number of times a caller is allowed for inputting wrong digits. The call will be terminated if the limit is reached. The range is 0-10.
<b>Timeout</b>	Enter the time limit that a caller is allowed for taking NO action after the call is put through. The call will be terminated if the time limit is reached. The range is 0-600 seconds.
<b>Max timeout allowed</b>	Enter the number of timeouts a caller is allowed for taking no action after the call is put through. The call will be terminated if the number of timeouts limit is reached. The range is 0-10.  For example, if <i>Timeout</i> is set to 10 seconds and <i>Max timeout allowed</i> to 3, a caller would have a total of 30 seconds timeout time after he or she dials in and takes no action afterwards.

6. Click *Create*.  
The digit collector is listed under *Questionnaire*. You may click *New* to add more.
7. If you want callers to comment on the survey, select *Caller Comment*.
8. For *Audio prompt*, select the audio file that explains to callers how to comment on the survey. Click *New* to create a new audio file. For more information, see [“Managing sound files and music on hold” on page 117](#).
9. For *Description*, enter any notes for the *Caller Comment*.
10. Click *OK*.

### To configure survey settings

1. Go to *Call Center > Survey > Setting*.
2. For *Survey retention month*, enter the number of months that you want to keep the surveys.

3. For *Max survey records*, enter the maximum number of surveys you want to keep.
4. Click *Apply*.

## Setting up queue view

You can create a queue view to let agents with privileges to view the snapshot of the key information of queues on the user web portal, such as number of calls in queue, longest waiting calls, and abandoned calls.

To apply the queue view configuration, you need to enable it in agent profile and apply the profile to an agent. As a result, the agent will have a *Queue Monitor* icon once he or she logs into the user web portal.

### To set up a queue view

1. Go to *Call Center > Monitor View > Monitor*.
2. Click *New* and configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for the queue view.
<b>Monitor Items</b>	Click <i>New</i> to include the queues or agents that you want to monitor.
<b>Title</b>	Enter a name for the configuration.
<b>Type</b>	Choose to monitor queues or agents.
<b>Refresh interval</b>	Enter the refresh interval time for the monitor view in seconds.
<b>Queue</b>	From the <i>Available</i> field select the queues to be included and click <i>-&gt;</i> . Click <i>Create</i> .
<b>Logo</b>	Select <i>Customized logo</i> to add text or logo for agents with privileges to view on the user web portal.  In the text editor window, you can type the text or copy and paste a logo here.

3. Click *Create*.

## Configuring other agent information

Configure call agent skill sets, skill levels, reason codes, data service, and global settings to be used for configuring agent profiles.

### Adding agent skill sets

Depending on the agents skill sets and the nature of your business, you can classify agents into different groups, such as Billing, Sales, or Support.

#### To add an agent skill set

1. Go to *Call Center > Configuration > Skill Set*.



2. Click *New*.
3. Enter a name and description for the skill set.
4. Click *Create*.

## Creating agent skill levels

The FortiVoice unit comes with 9 default skill levels, ranging from 10 to 90, with 10 to 30 being junior, 40 to 60 being intermediate, and 70 to 90 being senior. You can modify the default skill level descriptions, or create new skill levels.

### To create an agent skill level

1. Go to *Call Center > Configuration > Skill Level*.
2. Click *New*.
3. Enter the skill level and description.
4. Click *Create*.

## Modifying agent reason code descriptions

Agent reason codes explain why agents are not able to take calls, such as due to lunch break, meeting, or vacation. You cannot change the default reason codes, but you can modify the code descriptions.

### To modify an agent reason code description

1. Go to *Call Center > Configuration > Reason Code*.
2. Double-click a reason code.
3. Enter the code description.
4. Click *OK*.

## Configuring data service

If you use a third party software to generate call center reports or statistics, you can configure the FortiVoice database to provide all data needed.

### To configure data service

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

## Setting caller priorities

You can set call answering priorities for callers entering the call queue. A new call always starts with the lowest priority. However, a queue manager with privileges can change the priority of a call on the agent console of the user web portal.

### To set caller priorities

1. Go to *Call Center > Configuration > Global Settings*.
2. For *Call Center Settings*, enter the caller's highest and lowest priorities.
3. Click *Apply*.

## Configuring agent profiles

Create agent profiles to define agent privileges for processing calls. Agent profiles become effective when they are applied to the agent extensions. For more information, see “[Setting up local extensions](#)” on page 134.

### To create an agent profile

1. Go to *Call Center > Profile > Profile*.
2. Click *New*.
3. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Agent</b>	Select the calls an agent can make or process.
<b>Pickup call from queue</b>	Select to allow the agent to answer queue calls.
<b>Ring no answer</b>	Select the action to take when nobody answer a call in the queue. <ul style="list-style-type: none"><li>• <i>Do nothing</i>: No action is taken and the call keeps ringing.</li><li>• <i>Auto pause</i>: The call is paused automatically.</li><li>• <i>Auto logout</i>: The agent to whom this profile applies is automatically logged out of the queue.</li><li>• <i>Auto hold off</i>: The call is automatically put on hold.</li></ul>
<b>Queue</b>	Select to allow an agent to prioritize the calls in the queue or transfer calls to another queue on the agent console of the user web portal.  If you select <i>Caller prioritization</i> , the <i>Priority</i> button appears on the agent console of the user web portal. If you select <i>Transfer call to another queue</i> , the <i>Transfer</i> button appears on the agent console of the user web portal.
<b>Manager Privilege</b>	If the agent is a manager, select the privileges to manage the agents using the agent console of the user web portal.  The privileges include coaching, listening, and logging in and logging out agents, or pausing and resuming agents.
<b>Agent Console Privilege</b>	Select <i>Enable agent console</i> to choose the widget and GUI popup alert for an agent to view on the agent console of the user web portal.
<b>Monitoring Console Privilege</b>	Select to enable monitoring console on the user web portal.
<b>Monitoring Queue</b>	

<b>Member of queues</b>	Select to enable the agent to only monitor the queues of which the agent is a member.
<b>Selected</b>	Select the queues the agent is allowed to monitor by moving the selected queues from the <i>Available</i> field to the <i>Selected</i> field. The <i>Available</i> field lists all queues regardless if the agent is a member of them.
<b>All</b>	Select to allow the agent to monitor all call queues.

4. Click *Create*.

## Working with call queue statistics

Go to *Call Center > Statistics* to view agent and queue daily summaries. You can also download the summaries. The summaries cover a period of 30 days.

### To view agent daily summary

1. Go to *Call Center > Statistics > Agent Daily Summary*.

<b>GUI field</b>	<b>Description</b>
<b>Date</b>	The date of the agent call summary.
<b>Agent</b>	The agent ID.
<b>Work Time</b>	The agent's total work hours for the queue that the agent worked the longest.
<b>Talk Time</b>	The total time the agent talked on the phone in all queues combined.
<b>N/A Time</b>	The total time the agent was away from the phone in all queues combined.
<b>Total Answered</b>	The total calls the agent answered in all queues combined.
<b>Total RNA</b>	The total calls not answered by the agent in all queues combined.
<b>Out Call</b>	The outgoing calls made by the agent. This option is dependant on your queue management configuration in " <a href="#">Member of Queues</a> " on page 144.
<b>Out Talk Time</b>	The total time of outgoing calls made by the agent. This option is dependant on your queue management configuration in " <a href="#">Member of Queues</a> " on page 144.
<b>Voicemail</b>	The number of voicemails left on the agent's extension.

### To view queue daily summary

1. Go to *Call Center > Statistics > Queue Daily Summary*.

<b>GUI field</b>	<b>Description</b>
<b>Date</b>	The date of the call queue summary.

<b>Queue</b>	The queue name.
<b>Calls</b>	The number of calls reached this queue.
<b>Abandoned</b>	The number of calls that gave up after reaching the queue.
<b>Overflow</b>	The number of callers exceeding the maximum waiting callers you set for the queue. See <a href="#">“Maximum queue capacity” on page 200</a> .
<b>Talk Time</b>	The total phone talk time of the queue.
<b>Hold Time</b>	The total time for holding calls in the queue.
<b>Out Call</b>	The outgoing calls made by the agents in the queue. This option is dependant on your queue management configuration in <a href="#">“Member of Queues” on page 144</a> .
<b>Out Talk Time</b>	The total time of outgoing calls made by the agents in the queue. This option is dependant on your queue management configuration in <a href="#">“Member of Queues” on page 144</a> .

## Configuring call center report profiles and generating reports

The *Call Center > Report > Report* tab displays a list of call center report profiles.

A report profile is a group of settings that contains the report name, its subject matter, its schedule, and other aspects that the FortiVoice unit considers when generating reports from call center log data. The FortiVoice unit presents the information in tabular and graphical format.

You can create one report profile for each type of report that you will generate on demand or on a schedule.



Generating reports can be resource intensive. To avoid phone processing performance impacts, you may want to generate reports during times with low traffic volume, such as at night. For more information on scheduling the generation of reports, see [“Configuring report email notifications” on page 222](#).

### To view and configure report profiles

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

<b>GUI field</b>	<b>Description</b>
<b>Generate</b>	Select a report and click this button to generate a report immediately. See <a href="#">“Generating a report manually” on page 223</a> .
<b>View Reports</b>	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 <a href="#">“Viewing generated reports” on page 32</a> .
<b>View supported query</b>	Click to display supported query summary.
<b>Name</b>	Displays the name of the report profiles.

<b>Department</b>	The department to which the report belongs.
<b>Schedule</b>	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.
3. In *Name*, enter a name for the report profile.  
Report names cannot include spaces.
4. In *Department*, select the department for this report.  
For information on departments, see “[Creating extension departments](#)” on page 164.
5. 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](#)
  - [Generating a report manually](#)
6. Click *Create*.

## Configuring the report query selection

When configuring a report profile, you can select the queries that define the subject matter of the report.

Each report profile corresponds to a chart that will appear in the generated report.

### To configure the report query selection

1. Go to *Call Center > Report > Report*.
2. Click *New*.
3. Expand *Query List* and click *New*.
4. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for this query.
<b>Category</b>	Select a query type for the report profile. The report chart will correspond to the type selected.
<b>Sub category</b>	Select a sub query type for the report profile. The report chart will correspond to the type selected.
<b>Query</b>	Depending on your selection of <i>Category</i> and <i>Sub category</i> , choose the specific report you want to generate.  Depending on the report you choose, select queues or agents for which you want to generate reports.

5. Click *Create*.

## Configuring the report time period

When configuring a call center report profile, you can select the time span of log messages from which to generate the report.

### To configure the report time period

1. Go to *Call Center > Report > Report*.
2. 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.
  - If you select *Not used* for *Type*, 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 call center report profile, you can have the FortiVoice unit email an attached copy of the generated report, in either HTML or PDF file format, to designated recipients.

You can customize the report email notification. For more information, see [“Customizing call report and notification email templates” on page 109](#).

### To configure an email notification

1. Go to *Call Center > Report > Report*.
2. Expand *Email*.
3. Enter the email address of the person who will receive the report notification in the *Recipients* field. Click + to enter more email addresses if necessary, or click - to remove an address.
4. In the *File format* field, select the format of the generated attachment, either *HTML*, *PDF* or *CSV*.

## Configuring the report schedule

When configuring a call center 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 223](#).

### To configure the report schedule

1. Go to *Call Center > Report > Report*.
2. Expand *Schedule*.

3. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Type</b>	<ul style="list-style-type: none"><li>• <i>None</i>: Select if you do <b>not</b> 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 <a href="#">“Generating a report manually” on page 223</a>.</li><li>• <i>Daily</i>: Select to generate the report each day. Also configure <i>Hour</i>.</li><li>• <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>.</li><li>• <i>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>.</li></ul>

## Generating a report manually

You can always generate a report on demand whether the call center report profile includes a schedule or not.

### To manually generate a report

1. Go to *Call Center > Report > Report*.
2. Click to select the report profile whose settings you want to use when generating the report.
3. Click *Generate*.

The FortiVoice unit immediately begins to generate a report. To view the resulting report, see [“Viewing generated reports” on page 32](#).

# Working with Property Management System

Businesses such as hotels use Property Management System (PMS) to manage their services. The PMS can be connected to a PBX such as the FortiVoice unit to configure a customer's room phone by displaying the customer's name on the phone, emptying voicemails when a new customer checks in, logging phone calls, setting wake-up calls, and other services. You can also set the room condition codes for room maids to record the room cleaning status using the room phone.

This option is only available if you have purchased the license.

This topic includes:

- [Configuring hotel management settings](#)
- [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. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Enabled</b>	Select to enable the PMS.
<b>Protocol</b>	Select the protocol used by the FortiVoice unit to communicate with the PMS.
<b>Port</b>	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.
<b>Serial connection</b>	Select to connect to the PMS using a serial cable.  This option is only available for <i>Micros</i> protocol.
<b>LRC</b>	Select to perform longitudinal redundancy check (LRC).  This option is only available for <i>Micros</i> protocol.



<b>Mode</b>	<p>Choose to use the FortiVoice unit as server or client when connecting to the PMS. If it is used as client, enter the server IP address in the <i>Server</i> field.</p> <p>This option is only available for <i>Micros</i> and <i>Comtrol</i> protocols.</p>
<b>Call billing</b>	Select to activate call billing.
<b>Network Settings</b>	
<b>Trusted hosts</b>	<p>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.</p> <p>If you have multiple PMSes, you may enter multiple trusted hosts.</p>
<b>Data sync</b>	<p>This option is only available for <i>Micros</i> and <i>Comtrol</i> protocols.</p> <p>When the FortiVoice unit is connected to the PMS, it constantly receives all room-based information such as guest name, room privileges, and check in and check out times from the PMS.</p> <p>Normally, you do not need to click the <i>Data sync</i> button since the data synchronization is automatic. You only do so when there is a data mismatch between the FortiVoice unit and the PMS.</p> <p>Fortinet recommends performing a manual data sync at off hours because all related operations, such as check in and check out, are suspended during a data sync.</p>

3. Click *Apply*.

### To configure check in and check out actions

1. Go to *Hotel Management > Setting > Option*.
2. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Check in action</b>	
<b>Reset</b>	<p>Set the guest information and room condition to make a room check-in ready.</p> <ul style="list-style-type: none"> <li>• <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 <a href="#">“Configuring user privileges” on page 130</a></li> <li>• <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%%.</li> <li>• <i>Room condition</i>: Select to clear any condition set for the room.</li> </ul>
<b>Check out action</b>	

<b>Reset</b>	<p>Set the guest information and room condition to make a room check-out ready.</p> <ul style="list-style-type: none"> <li>• <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 <a href="#">“Configuring user privileges” on page 130</a></li> <li>• <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%%.</li> <li>• <i>Room condition</i>: Select to clear any condition set for the room.</li> <li>• <i>Voice mail</i>: Select to clear all voicemails for the room extension.</li> <li>• <i>Wakeup call</i>: Select to clear all wakeup call setups for the room extension.</li> </ul>
<b>Advanced</b>	<p>Choose the order for room maids to request for room item by phone. You can choose to dial the item code or number first.</p> <p>For example, if you choose to dial code first and want to request for two beers (code 1) and three waters (code 2), you can dial 1*2*2*3.</p> <p>For information on item code, see <a href="#">“To set mini bar code for room maids to order room items” on page 226</a>.</p>

3. Click *Apply*.

#### To set mini bar code for room maids to order room items

1. Go to *Hotel Management > Setting > Mini Bar Code*.
2. Click *New*.
3. Enter the item name, for example, Beer.
4. Enter the item code, for example, 5.
5. Click *Create*.

A room maid can dial the code to order beer for the room using the room phone. For more information, see [“Advanced” on page 226](#).

## Configuring hotel room status

*Hotel Management > Room Status* lets you set hotel room status.

Once the PMS and the FortiVoice unit is properly connected and the PMS is enabled on the FortiVoice unit, all hotel room extensions appear on the FortiVoice unit.

#### To batch-configure hotel room statuses

1. Go to *Hotel Management > Room Status*.

A green dot at the top of the screen means the FortiVoice unit is connected with the PMS. Otherwise, a red dot appears.

2. Select more than one room in the list.

Depending on the situations of the rooms you select, the *Check in*, *Check out*, *Privilege*, *Room condition*, *Room setting*, and *VIP setting* buttons become active.

A green dot under *Guest* means this guest room’s extension is bound with the room. Otherwise, a red dot appears. For more information, see [“Guest phone” on page 227](#).

3. Click a button to batch-configure the room status and apply it to all rooms selected.

### To configure a single hotel room status

1. Go to *Hotel Management > Room Status*.
2. Select a room extension and click *Edit*.
3. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Number</b>	The extension number of the room. You can click the number and modify it if required. For more information, see <a href="#">“Configuring IP extensions” on page 134</a> .
<b>Guest phone</b>	Select to bind the extension with the room and make the room a guest room.
<b>Room</b>	The hotel room number. You can click the number and modify it if required.
<b>Location</b>	Click to enter the room location.

If you have selected *Guest phone*, configure the following:

<b>Checkin status</b>	Choose the room status to configure: <i>Checked-out</i> or <i>Checked-in</i> .
<b>Guest name</b>	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> .
<b>Privilege</b>	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 <a href="#">“Configuring user privileges” on page 130</a> . This option is available only if the <i>Checkin status</i> is <i>Checked-in</i> .
<b>DND</b>	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> .
<b>VIP setting</b>	Select to set the guest as a VIP. Specific VIP treatments are determined by each hotel.
<b>Room condition</b>	Select the cleaning status of the room. You can add a new code or edit the current one: <ul style="list-style-type: none"><li>• Click <i>New</i> to add a code or select an existing code and click <i>Edit</i> to modify it.</li><li>• Select the protocol for connecting to your PMS.</li><li>• Enter a code number.</li><li>• Enter the code description.</li><li>• Click <i>Create</i>.</li></ul>

4. Click *OK*.

# Configuring phone auto dialer

With the auto dialer function, the FortiVoice unit can automatically dial telephone numbers. Once the call is answered, the FortiVoice unit plays a recorded message.

This topic includes:

- [Setting up an auto dialer campaign](#)
- [Creating a recorded broadcast message](#)
- [Adding contacts and contact groups](#)
- [Configuring auto dialer settings](#)
- [Viewing auto dialer reports](#)

## Setting up an auto dialer campaign

*Auto Dialer > Campaign > Campaign* allows you to set up an auto dialer task to broadcast a recorded message to the dialed phone numbers.

### To set up an auto dialer campaign

1. Go to *Auto Dialer > Campaign > Campaign*.
2. Click *New* and configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for the campaign.
<b>Caller ID</b>	Enter the caller ID to be displayed on a called phone. You can also select an extension number instead.
<b>Status</b>	The current status of the campaign.
<b>Sound file</b>	Select a recorded message that you want to broadcast. You can also create a new one. For more information, see <a href="#">“Creating a recorded broadcast message” on page 229</a> .
<b>Retry</b>	Enter the number of times you want to retry calling.
<b>Description</b>	Enter any notes you have for this campaign.
<b>External Numbers</b>	Select the external phone numbers you want to autodial. You can add these numbers by going to <i>Auto Dialer &gt; Contact &gt; Contact/Contact Group</i> . See <a href="#">“Adding contacts and contact groups” on page 229</a> .
<b>Internal Numbers</b>	Select the internal phone numbers you want to autodial. These numbers are the internal extensions on the FortiVoice unit.

3. Click *Create*.
4. If you want to start a campaign, in the campaign list, select one with a status other than *Completed* and click *Start* on top of the screen.
5. Select a campaign start and end time.
6. Click *OK*.

## Creating a recorded broadcast message

*Auto Dialer > Campaign > Audio* allows you to create a sound file for the auto dialer to broadcast.

### To create a sound file

1. Go to *Auto Dialer > Campaign > Audio*.
2. Click *New*.
3. Enter a name for the sound file.
4. Select an *Action*:
  - *Upload*: Click to upload a sound file. Uploaded sound file should be a WAVE file (\*.wav) in 16bit PCM(8000Hz) compression format.
  - *Record*: Click to enter a phone number and click *Send*. When the phone rings, pick it up and record the message.
  - *Download*: Once a file is uploaded or recorded, click to download it.
  - *Play*: Once a file is uploaded or recorded, click to play it.
5. Click *OK*.

## Adding contacts and contact groups

*Auto Dialer > Contact > Contact/Contact Group* allows you to add contacts and contact groups that can be used in an auto dialer campaign.

### To add a contact

1. Go to *Auto Dialer > Contact > Contact*.
2. Click *New* and enter the contact information.
3. Click *Create*.

### To add a contact group

1. Go to *Auto Dialer > Contact > Contact Group*.
2. Click *New*.
3. Enter a name for the group.
4. Select the members for the group.  
Members are created by adding contacts. See “To add a contact” on page 229.
5. Click *Create*.

## Configuring auto dialer settings

*Auto Dialer > Setting* allows you to

- set the maximum call channels (64 by default) for campaigns. This value represents the number of phones that can be auto dialed at the same time.
- set call timeout (600 seconds by default).

These values can be modified through the CLI.

## Viewing auto dialer reports

*Auto Dialer > Report* allows you to view the status of the auto dialer campaigns, including campaign IDs, call status, total number of campaigns, number of uncalled, answered, unanswered calls, and retries, and call duration and time.

# Configuring Call Features

The *Call Features* menu lets you configure the settings for many call features such as conference call, auto attendant, faxing, and much more.

This topic includes:

- [Configuring auto attendants](#)
- [Configuring user privileges](#)
- [Configuring account codes](#)
- [Mapping speed dials](#)
- [Configuring conference calls](#)
- [Recording calls](#)
- [Creating call queues](#)
- [Configuring call parking](#)
- [Configuring fax](#)
- [Setting calendar reminder](#)
- [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*.

<b>GUI field</b>	<b>Description</b>
<b>View Hierarchy</b>	Click to view the hierarchical structure of the selected auto attendant. For more information, see <a href="#">“Viewing auto attendant hierarchies” on page 233</a> .
<b>Delete</b>	Removes a selected auto attendant. You cannot remove an auto attendant that is used in another auto attendant configuration.
<b>Name</b>	The name of the auto attendant.
<b>Direct Actions</b>	The number of key actions configured for the main auto attendant, excluding the key actions for the subsidiary auto attendants. For more information, see <a href="#">“Viewing auto attendant hierarchies” on page 233</a> .

### To create an auto attendant

1. Go to *Call Features > Auto Attendant > Auto Attendant* and click *New*.

2. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Auto Attendant</b>	
<b>Name</b>	Enter a name for the auto attendant.
<b>Default language</b>	<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 <a href="#">“Setting PBX location and contact information”</a> on page 105.</p> <p>You can also select other languages. The language files are created in <a href="#">“Adding prompt languages”</a> on page 113.</p>
<b>Greeting mode</b>	<p>If you select <i>Simple</i>, select a greeting message (sound file) for the auto attendant. See <a href="#">“Greeting”</a> on page 232.</p> <p>If you select <i>Scheduled</i> to add a scheduled greeting, do the following:</p> <ul style="list-style-type: none"> <li>• In <i>Scheduled Greeting Setting</i>, click <i>New</i>.</li> <li>• In the <i>Schedule</i> field, select a schedule for the greeting. Schedules are created in <a href="#">“Scheduling the FortiVoice unit”</a> on page 131.</li> <li>• 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 <a href="#">“Managing sound files and music on hold”</a> on page 117.</li> <li>• Click <i>Create</i>.</li> </ul>
<b>Greeting</b>	<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 <a href="#">“Managing sound files and music on hold”</a> on page 117.</p> <p>This option is only available if you select the <i>Simple</i> greeting mode.</p>
<b>Ring for</b>	Enter the number of seconds for the phone to ring before the auto attendant answers with the greeting message.
<b>Timeout after</b>	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.
<b>Timeout action</b>	<p>Select the action when the auto attendant timeout is reached.</p> <ul style="list-style-type: none"> <li>• <i>Dial operator</i>: The call is transferred to an operator.</li> <li>• <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 <a href="#">“Configuring IP extensions”</a> on page 134.</li> <li>• <i>Start over</i>: The auto attendant will repeat the instructions for the caller. Also enter the maximum times to repeat.</li> <li>• <i>Hang up</i>: The call will be terminated.</li> </ul>
<b>Invalid input action</b>	Select the action when the caller enters an invalid input.



<b>Dial Pad Key Action</b>	Configure the auto attendant keys for callers to use when navigating through the auto attendant hierarchy. For more information, see <a href="#">“Configuring key actions” on page 235</a> .
<b>Key</b>	The key that transfers a call to a resource, for example, voicemail, if pressed.
<b>Action</b>	The resource to which a call is transferred by pressing a key.
<b>Target</b>	The resource target if applicable. For example, an extension number, sound file, or external phone number that leads to a resource.
<b>Advanced</b>	<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"> <li>• <i>Access voicemail</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 <a href="#">“Modifying feature access codes” on page 262</a>.</li> <li>• <i>Dial local number</i>: Select to enable an external caller to dial local extensions.</li> <li>• <i>Override schedule</i>: Select to allow a system administrator to dial a code to replace the schedule with a system schedule. For more information, see <a href="#">“Configuring system capacity” on page 116</a>.</li> <li>• <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 <a href="#">“Modifying feature access codes” on page 262</a>. For more information on account code, see <a href="#">“Configuring account codes” on page 241</a>.</li> <li>• <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 <a href="#">“Configuring outbound dial plans” on page 192</a>.</li> </ul>

3. Click *Create*.

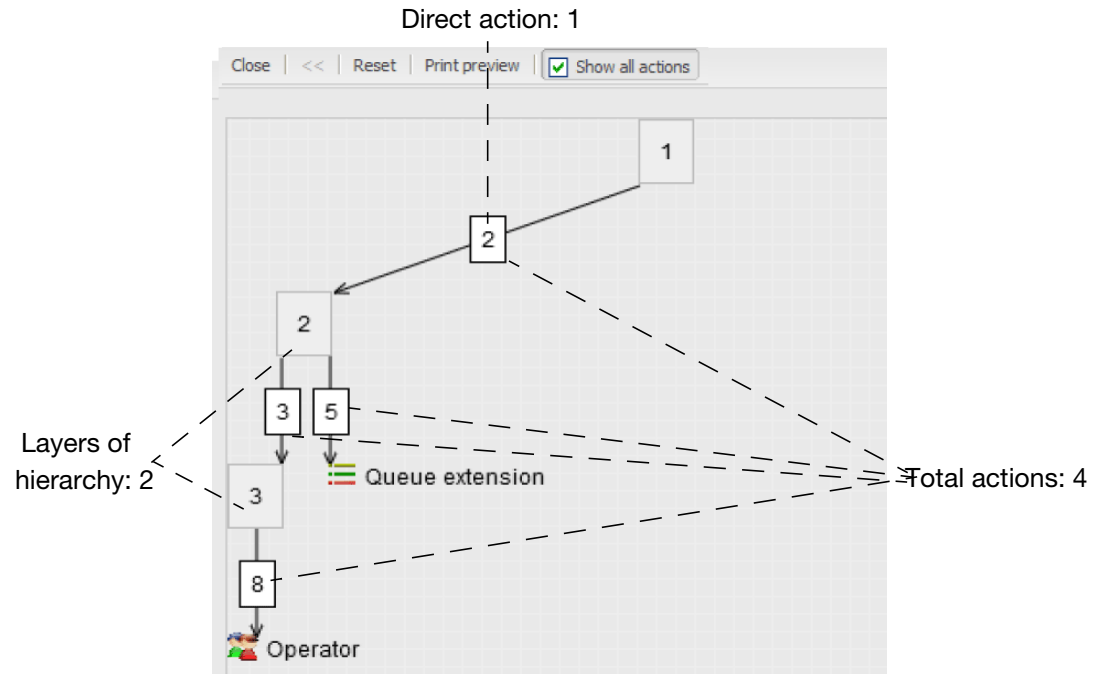
## Viewing auto attendant hierarchies

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 1:** 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 1:** Sample auto attendant hierarchy

<b>Close</b>	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.
<b>Reset</b>	Sets the chart to its default view. All the saved and unsaved views will be lost.
<b>Print preview</b>	Click to preview the chart before printing it.
<b>Show all actions</b>	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 233](#).

### 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:

<b>GUI field</b>	<b>Description</b>
<b>No action</b>	The call is not transferred to any resource.
<b>Play announcement</b>	Play an announcement with directions, business hours, etc. <ul style="list-style-type: none"><li>• Select an action to follow the announcement:<ul style="list-style-type: none"><li>• <i>No action</i>: The auto attendant takes no action.</li><li>• <i>Start over</i>: The auto attendant will repeat the announcement.</li><li>• <i>Hang up</i>: The call will be terminated.</li></ul></li><li>• 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 <a href="#">“Managing sound files and music on hold” on page 117</a>.</li></ul>
<b>Dial operator</b>	The call is transferred to the operator.
<b>Dial extension</b>	The call is transferred to a specified local extension.  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 <a href="#">“Configuring Extensions” on page 134</a> .

<b>Go voicemail</b>	<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 <a href="#">“Configuring IP extensions” on page 134.</a></p>
<b>Ring group</b>	<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 <a href="#">“Creating extension groups” on page 163.</a></p>
<b>Dial number</b>	<p>The call is transferred to a specified remote extension number.</p> <p>Enter the remote extension number. For more information, see <a href="#">“Setting up remote extensions” on page 148.</a></p>
<b>Call queue</b>	<p>The call is transferred to a call queue.</p> <p>Enter the call queue configuration. For more information, see <a href="#">“Creating call queues” on page 198.</a></p>
<b>Lookup name directory</b>	<p>Access the dial-by-name directory so the caller can find a user’s extension number by entering the user’s name.</p>
<b>Change language</b>	<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 <a href="#">“Setting PBX location and contact information” on page 105.</a></p> <p>You can also select other languages. The language files are created in <a href="#">“Adding prompt languages” on page 113.</a></p>
<b>Auto attendant</b>	<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. Oprimos 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 <a href="#">“Configuring auto attendants” on page 231.</a></p>
<b>Start over</b>	<p>The auto attendant will repeat the announcement.</p>
<b>Go back</b>	<p>The auto attendant will repeat the previous level announcement.</p>
<b>Hang up</b>	<p>The call is terminated.</p>
<b>IVR</b>	<p>Route the call to the FortiVoice IVR system. For more information, see <a href="#">“Configuring IVRs” on page 208.</a></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 134.

### To configure a user privilege

1. Go to *Call Features > User Privileges > User Privileges* and click *New*.
2. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for this class of service.
<b>Basic Settings</b>	
<b>Auto provisioning</b>	Select to enable auto-provisioning for the extension. For more information, see “ <a href="#">Configuring SIP phone auto-provisioning</a> ” on page 112.  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.
<b>List in directory</b>	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.
<b>Configure programmable phone feature key/PFK</b>	Select to enable configuring the feature access codes. For more information, see “ <a href="#">Modifying feature access codes</a> ” on page 262.
<b>Lookup directory</b>	Select to enable a user to view the phone directory of the local office. For more information, see “ <a href="#">Viewing phone directories</a> ” on page 38.
<b>Lookup directory in remote office(s)</b>	Select to enable a user to view the phone directories of remote offices. For more information, see “ <a href="#">Viewing phone directories</a> ” on page 38.

<b>Twinning</b>	<p>Select to enable twinning function on an extension.</p> <p>The twinning feature allows you to use an external telephone (often a smartphone or home phone) to replicate your internal office extension (often your desk phone), so that when your desk phone rings, so does the “twin” phone. Once you return to your desk, you may press the Twinning key on the phone to terminate the twinning.</p> <p>This is useful when you are away from your desk but still want to receive calls to your desk phone.</p> <p>With this feature selected, you can configure twinning. For more information, see <a href="#">“Setting extension user preferences” on page 154.</a></p>
<b>Role Settings</b>	
<b>Operator role</b>	<p>Select to enable an extension user to process phone calls using the FortiVoice user web portal.</p> <p>You can select the four options to handle calls in each category.</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>
<b>Voice Mail</b>	
<b>Enabled</b>	Select to enable the voicemail service.
<b>Maximum messages</b>	Enter the number of voice mails allowed.
<b>Voicemail retention days</b>	Enter the number of days to keep the voicemails.
<b>Music</b>	
<b>Music on hold</b>	Select a music on hold file. For details, see <a href="#">“Managing sound files and music on hold” on page 117.</a>
<b>Early media</b>	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 <a href="#">“Managing sound files and music on hold” on page 117.</a>
<b>Fax</b>	Set the user rules for faxing. For information on fax, see <a href="#">“Configuring fax” on page 253.</a>
<b>Enabled</b>	Select to set the fax rules for users.
<b>Max incoming messages</b>	Enter the number of incoming faxes allowed.

<b>Max incoming fax retention days</b>	Enter the number of days to keep the incoming faxes.
<b>Max outgoing messages</b>	Enter the number of outgoing faxes allowed.
<b>Max outgoing fax retention days</b>	Enter the number of days to keep the outgoing faxes.
<b>Call Restriction</b>	<p>Select call dialing restrictions for international, long distance, local, and internal calls.</p> <ul style="list-style-type: none"> <li>• <i>Forbidden</i>: Call is not allowed.</li> <li>• <i>Allowed</i>: Call is allowed.</li> <li>• <i>Allowed with account code</i>: Call is allowed by entering the system account/exempt code. For information on account code, see <a href="#">“Configuring account codes” on page 241</a>. Not applicable to internal calls.</li> <li>• <i>Allowed with personal code</i>: Call is allowed by entering an extension’s account/exempt code. For more information, see <a href="#">“Configuring account codes” on page 241</a>. Not applicable to internal calls.</li> </ul>
<b>Other restricted area code</b>	<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"> <li>1. Click <i>New</i>.</li> <li>2. Enter a name for this call restriction.</li> <li>3. Select <i>Enable</i> to activate this restriction.</li> <li>4. Enter the area code that you want to set restriction.</li> <li>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 <a href="#">“Configuring account codes” on page 241</a>.</li> <li>6. Click <i>Create</i>.</li> </ol>
<b>Misc</b>	<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. The default is 4.
<b>Monitor/Recording</b>	Configure monitoring and recording outgoing and incoming calls of an extension to which this user privilege is applied.
<b>Personal recording</b>	Select to allow users to configure personal recording of their incoming and outgoing calls on the user web interface.
<b>System recording</b>	Select to allow users to configure system recording of their incoming and outgoing calls on the user web interface.
<b>Allow being barged</b>	Select to allow monitoring an extension to which this user privilege is applied.

<b>Allow barging</b>	<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 <a href="#">“User PIN” on page 137</a>.</p>
<b>Call barge option</b>	<p>If you select <i>Allow barging</i>, choose a barging method.</p>
<b>Hot-desking</b>	<p>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.</p> <p>You can view hot desking configurations by going to <a href="#">“Viewing hot desking configurations” on page 27</a>.</p> <ul style="list-style-type: none"> <li>• <i>Enable hot-desking login</i>: Select to enable the hot-desking login function.</li> <li>• <i>Automatic logout hours</i>: Enter the time in hours for the phone to automatically log out of hot-desking.</li> <li>• <i>Enable hosting hot-desking</i>: 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 <i>Automatic logout hours</i> expires.</li> </ul> <p>If the two phones use different programmable phone keys, the host phone will reboot. For information on programmable phone keys, see <a href="#">“Configuring phone profiles” on page 122</a>.</p>
<b>User Portal Options</b>	<p>Enable or disable the web portal and select the features of the user web portal. Only the selected ones will appear for the extension to which this user privilege is applied.</p>
<b>Advanced</b>	



---

<b>Conference number</b>	<p>Select the permission for conference calls:</p> <ul style="list-style-type: none"> <li>• <i>Allow all</i>: Select to allow the extension to join all conference calls.</li> <li>• <i>Disallow all</i>: Select to prohibit the extension from joining all conference calls.</li> <li>• <i>Allow all with exempt</i>: If you select this option, click <i>New</i> to enter the conference call number(s) that the extension is banned to join.</li> <li>• <i>Disallow all with exempt</i>: If you select this option, click <i>New</i> to enter the conference call number(s) that the extension is allowed to join.</li> </ul> <p>For more information, see <a href="#">“Configuring auto attendants” on page 231</a>.</p>
<b>Paging/Intercom</b>	<p>Select the permission for paging/intercom:</p> <ul style="list-style-type: none"> <li>• <i>Allow all</i>: Select to allow the extension to page/intercom all paging numbers.</li> <li>• <i>Disallow all</i>: Select to prohibit the extension to page/intercom all paging numbers.</li> <li>• <i>Allow all with exempt</i>: If you select this option, click <i>New</i> to enter the paging/intercom number(s) that the extension is banned to page/intercom.</li> <li>• <i>Disallow all with exempt</i>: If you select this option, click <i>New</i> to enter the paging/intercom number(s) that the extension is allowed to page/intercom.</li> </ul> <p>For more information on paging, see <a href="#">“Configuring auto attendants” on page 231</a>.</p>
<b>Trusted hosts</b>	<p>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.</p>
<b>Permit outgoing rules</b>	<p>Select the available outbound calling rules in the <i>Available rules</i> field and click -&gt; 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 <a href="#">“Configuring outbound dial plans” on page 192</a>.</p>

---

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 237](#).

### 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 account 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 106.

### To map speed dials

1. Go to *Call Features > Speed Dials*.
2. Click *New*.
3. Enter a name for the speed dial mapping.
4. For *Code*, enter the number based on the speed dial number pattern you set. For example, 333.
5. 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.

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

## Configuring conference calls

The *Call Features > Conferencing > Conferencing* tab lets you configure and enable conference call settings.

Depending on your preference, you can create either a static or dynamic (calendar-based) conference call.

### To configure a static conference call

1. Go to *Call Features > Conferencing > Conferencing* and click *New*.
2. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a conference call name.
<b>Enabled</b>	Select to activate this conference call.

<b>Number</b>	Select an extension number that callers can call and enter the user PIN to join a conference call.
<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers” on page 141</a>.</p>
<b>Display name</b>	Enter the name displaying on the conference call extension, such as “HR”.
<b>User PIN</b>	<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>
<b>Admin PIN</b>	<p>Enter the PIN number to be used by the conference host 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>
<b>Description</b>	Enter any notes you have for this conference call.
<b>Music on hold</b>	<p>Select to play background music that callers hear after the joining message and leaving message are played.</p> <p>For information on creating music on hold file, see <a href="#">“Managing sound files and music on hold” on page 117</a>.</p>
<b>Quiet mode</b>	Select to not to record and announce participate's name.

---

**Recursive Schedules**

If you want conference calls on repeating schedules, select *Enabled* and click *New* to select a schedule. Enter a password for joining the conference call and click *Create*.

This option is useful if you want to limit the participants to a particular recursive conference call only provided that they do not have the *User PIN* or *Admin PIN* for the conference call. They can only join the conference call during the scheduled time period and by entering the password you set.

For information on setting up a schedule, see [“Scheduling the FortiVoice unit” on page 131](#).

---

**One Time Schedules**

If you want to set up a one time conference call, select *Enabled* and click *New* to enter the start and end time. Enter a password for joining the conference call and click *Create*.

This option is useful if you want to limit the participants to a particular one time conference call only provided that they do not have the *User PIN* or *Admin PIN* for the conference call. They can only join the conference call during the scheduled time period and by entering the password you set.

If the one time schedule conflicts with the recursive schedule, the one time schedule has priority.

---

3. Click *Create*.

**To configure a dynamic conference call**

1. Go to *Call Features > Conferencing > Dynamic Conferencing* and click *New*.
2. Configure the following:

---

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a conference call name.
<b>Enabled</b>	Select to activate this conference call.
<b>Number</b>	Select an extension number that callers can call and enter the user PIN to join a conference call.
<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers” on page 141</a>.</p>

---

**Setting**

---

<b>Display name</b>	Enter the name displaying on the conference call extension, such as “HR”.
---------------------	---

---

<b>Description</b>	Enter any notes you have for this conference call.
<b>Music on hold</b>	Select to play background music that callers hear after the joining message and leaving message are played.  For information on creating music on hold file, see <a href="#">“Managing sound files and music on hold”</a> on page 117.
<b>Quiet mode</b>	Select to not to record and announce participate's name.

3. Click *Create*.
4. In the conference call list, select the one you created.
5. Enter an extension number that callers can call and enter their user PIN to join a conference call.
6. Double-click a date to schedule an event.
7. Click *OK*.

## Recording calls

For supervising and monitoring purposes, you can record incoming and outgoing calls to and from the extensions matching the caller number patterns or dialed number patterns you set. You can also select the recorded file format and archive the recorded calls.

### Configuring call recordings

*Call Features > Call Recording > Policy* allows you to configure call recordings by creating, editing, removing, saving, or viewing a recording.

<b>GUI field</b>	<b>Description</b>
<b>View Recordings</b>	Click to view, listen, search, or save the recordings. You can also do so by going to <i>Status &gt; Storage &gt; Recorded Calls</i> . For details, see <a href="#">“Playing recorded calls”</a> on page 31.
<b>Enabled</b>	Select to activate this call recording service.
<b>Name</b>	The name of the call recording service.
<b>Description</b>	Information of call recording configuration.

#### To configure call recording

1. Go to *Call Features > Call Recording > Policy*.
2. Click *New*.

<b>GUI field</b>	<b>Description</b>
<b>Recording Policy</b>	
<b>Name</b>	Enter a name for this configuration.
<b>Enabled</b>	Select to activate this configuration.

<b>Type</b>	Select the category of calls you want to record: by phone number, department, group, or trunk.
If you select <i>By phone number</i> for <i>Type</i> , configure the following:	
<b>Caller number pattern</b>	<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 <a href="#">“Configuring PBX options” on page 106</a>.</p> <p>The phone calls from the numbers matching the pattern will be recorded.</p>
<b>Dialed number pattern</b>	<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 <a href="#">“Configuring PBX options” on page 106</a>.</p> <p>The phone calls to the numbers matching the pattern will be recorded.</p>
If you select <i>By department</i> for <i>Type</i> , configure the following:	
<b>Department</b>	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 <a href="#">“Creating extension departments” on page 164</a> .
If you select <i>By group</i> for <i>Type</i> , configure the following:	
<b>Group</b>	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 <a href="#">“Creating user groups” on page 163</a> .
If you select <i>By trunk</i> for <i>Type</i> , configure the following:	
<b>Trunk</b>	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 <a href="#">“Configuring Trunks” on page 173</a> .
<b>Direction</b>	Select the direction of which you want to record the calls.
<b>File name format</b>	<p>Select the format of the downloaded recorded call files generated under this policy.</p> <p>The file format is useful when you filter downloaded recorded call files by going to <i>Status &gt; Storage</i>.</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*.
2. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Rotation Settings</b>	
<b>Recording rotation size/time</b>	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.
<b>Archiving options when disk quota is full</b>	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.
<b>Schedule</b>	Select a schedule for the rotation.
<b>Destination Settings</b>	
<b>Destination</b>	Select an archiving destination: <ul style="list-style-type: none"><li>• <i>Local</i>: the FortiVoice unit's local hard drive or a NAS server.</li><li>• <i>Remote</i>: a remote FTP or SFTP storage server.</li></ul>
<b>Local disk quota</b>	If <i>Local</i> is the archiving destination, enter the disk space quota.  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.  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 " <a href="#">Rotation Settings</a> " on page 247.
If <i>Remote</i> is the archiving destination, configure the following:	
<b>Protocol</b>	Select the protocol that the FortiVoice unit will use to connect to the remote storage server, either SFTP or FTP.
<b>IP address</b>	Enter the IP address of the remote storage server.

<b>User name</b>	Enter the user name of an account the FortiVoice unit will use to access the remote storage server, such as FortiVoice.
<b>Password</b>	Enter the password for the user name of the account on the remote storage server.
<b>Remote directory</b>	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> .
<b>Remote cache quota</b>	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

This option is available if you do not have the Call Center license. If you do, see [“Setting up a Call Center” on page 198](#).

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 187](#).

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*.

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	The name of the call queue.
<b>Display Name</b>	The queue name displaying on the queue extension.
<b>Number</b>	The extension number for the call queue.



<b>Department</b>	The departments of the agents enrolled in the queue.
<b>Agents</b>	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:

<b>GUI field</b>	<b>Description</b>
<b>Queue</b>	
<b>Name</b>	Enter a name for the queue.
<b>Number</b>	<p>Enter an extension for callers to dial and enter into a call queue following the extension number pattern. See <a href="#">“Configuring PBX options” on page 106</a>.</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>
<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers” on page 141</a>.</p>
<b>Status</b>	Select to enable the call queue.
<b>Display name</b>	Enter the queue name displaying on the queue extension, such as Support.
<b>Description</b>	Enter any notes about this queue.
<b>Queue Setting</b>	
<b>Distribution policy</b>	Select the method for calls in the queue to be delivered to the agents.
<b>Maximum caller</b>	<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 <i>Overflow</i> call handling action you set in <a href="#">“Overflow” on page 252</a>.</p> <p>The maximum is 100.</p>

<b>Queue time</b>	<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 in <a href="#">“Waiting Timeout” on page 252</a>.</p> <p>The maximum is 720 minutes.</p>
<b>Ring duration</b>	<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>
<b>On hold music</b>	<p>Select a sound file or music on hold file to play when a caller is waiting. For more information, see <a href="#">“Managing sound files and music on hold” on page 117</a>.</p>
<b>More Settings</b>	
<b>Distinctive settings</b>	<p><i>Announce queue name:</i> Select a sound file that announces the queue name. You can add a new one or modify an existing one. For more information, see <a href="#">“Managing sound files and music on hold” on page 117</a>.</p> <p><i>Caller ID option:</i> Select how you want the IDs of the calls to this queue to display. If you select <i>Prefix</i>, the queue <a href="#">Display name</a> is added before the caller ID on the agent’s phone. If you select <i>Replace</i>, the queue <a href="#">Display name</a> replaces the caller ID on the agent’s phone.</p> <p><i>Ring Pattern:</i> Select a queue extension ring pattern.</p>
<b>Business schedule</b>	<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. For information on scheduling, see <a href="#">“Scheduling the FortiVoice unit” on page 131</a>.</p>

---

**Announcement**

*Announcement holdtime:* Select if you want to announce the queue waiting time to a caller at the set interval. You may also select to announce only once.

*Announcement position:* Select to announce a caller's waiting position in the queue, such as "You are caller No. 5 in the call queue".

*No:* Do not announce a caller's position.

*Always:* Always announce a caller's position.

*Abbreviated:* Announce a caller's position only once if the caller is over the marked position and always announce once the caller is within the marked position.

*Minimal:* Announce only when the caller is within the marked position.

*Mark position:* Enter the benchmark for selecting *Abbreviated* or *Minimal* setting.

For example, if you select *Abbreviated* and enter 5, a caller's position is announced when the caller becomes No. 5 in the queue and announced only once before the caller becomes No. 5 in the queue.

*Announcement interval:* Enter the announcement frequency in seconds.

**Custom announcement:** You can also customize the announcement settings.

- *Mode:* Select the method of greeting announcement to the caller once the caller enters this call queue. You can also select to disable this function.

If you select *Periodic* or *Random*, enter the announcement frequency in seconds in *Announcement interval*.

- *Audio:* Select a greeting sound file for the announcement. For more information, see "[Managing sound files and music on hold](#)" on page 117.

---

**Agent**

---

**Agent members**

- Click >> to expand *Agent members* for enrolling agents into the queue.
- In the *Available* field, select the agents for this queue.
- Click -> to move it into the *Selected* field.
- Click *Done*.

You can type an agent's extension or name in the *Search* field and press Enter to search for the agent.

---

**Call Handling**

---

**Configure call handling**

Click to configure the call handling action for the queue. For details, see "[Configuring queue call handling actions](#)" on page 252.

---

**4. Click *Create*.**

## Configuring queue call handling actions

Configure the call handling action for the queue. This action applies to all calls once they enter into the queue.

This option is only available when you edit a queue.

### To configure the call handling action

1. Go to *Call Features > Call Queue*.
2. Select a call queue for which you want to configure queue call handling actions and click *Edit*.
3. In *Call Handling*, click *Configure call handling*.
4. Configure the situation upon which the FortiVoice unit can be configured to take corresponding actions:

<b>GUI field</b>	<b>Description</b>
<b>Overflow</b>	The situation when callers exceed the maximum waiting callers you set. See <a href="#">“Maximum caller” on page 249</a> . A popup notification appears when this barometer is triggered.
<b>Waiting Timeout</b>	Callers waiting time exceeds the maximum waiting time set in <a href="#">“Queue time” on page 250</a> . A popup notification appears when this barometer is triggered.
<b>Non Business Hour</b>	The option to schedule call handlings for after-hour time slots.

5. Click *OK*.

## 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 26](#).

### 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 117](#).
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 253](#) and [“Sending faxes” on page 255](#).
- 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 151](#), [“Receiving Faxes” on page 253](#) and [“Sending faxes” on page 255](#).

- With FortiVoice 200D-T, if you want to use your existing analog phone line, connect the fax machine directly to the FXS port. Make sure that the fax function is enabled when configuring the analog extension. See [“Modifying analog extension \(200D-T, 1000E-T, and 20E2 models only\)” on page 145](#).

## 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:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for the receiving fax configuration.
<b>Number</b>	Enter an extension for this fax. This is where the incoming faxes go to.
<b>Display name</b>	Enter the name displaying on the extension.

<b>Show suggested numbers</b>	<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 <a href="#">“Fixing duplicate or missing numbers” on page 141</a>.</p>
<b>Enabled</b>	Select to activate this fax.
<b>External Numbers</b>	<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 <a href="#">“Mapping DIDs” on page 191</a>.</p> <p>To map the DID numbers:</p> <ul style="list-style-type: none"> <li>• Click <i>New</i>.</li> <li>• Select <i>Enabled</i> to activate this DID mapping.</li> <li>• Select the trunk used for dialing the DIDs.</li> <li>• Enter the DID number that you want to map to an extension.</li> <li>• Click <i>Create</i>.</li> </ul>
<b>Select Fax Monitors</b>	<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 <a href="#">“Setting extension user preferences” on page 154</a>.</p> <p>This is useful if you have a fax that serves several departments.</p>
<b>Fax to Email</b>	Enter the email addresses to receive the faxes sent to this extension. Users will receive the faxes in PDF format.
<b>Relay to Fax Machine</b>	Select the fax machines connected to the FortiVoice unit via T.38 adapters. Faxes will be relayed to the selected machines.
<b>Archive</b>	<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 <a href="#">“Viewing archived faxes” on page 31</a>.</p>
<b>Description</b>	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 187](#).

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 154](#).

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*.

<b>GUI field</b>	<b>Description</b>
<b>Test</b>	Select to test if the dial plan is created successfully. For more information, see <a href="#">“Testing dial plans for sending faxes” on page 256</a> .
<b>Enabled</b>	Select to activate this dial plan.
<b>Name</b>	The name of the dial plan.
<b>Pattern</b>	The phone number pattern in the dial plan that matches other numbers. For details, see <a href="#">“Dialed Number Match” on page 256</a> .
<b>Call handling</b>	The call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern. For details, see <a href="#">“Call Handling” on page 256</a> .

### To set up a fax sending dial plan

1. Go to *Call Features > Fax > Sending Rule*.
2. Click *New*.
3. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for this plan.
<b>Enabled</b>	Select to activate this dial plan.

---

**Dialed Number Match**

With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers.

The dialed numbers matching this pattern will follow this dial plan rule.

For information on adding a dialed number match, see [“Creating dialed number match” on page 257](#).

---

**Call Handling**

Click *New* to configure the call handling action for the numbers matching the configured number pattern. For details, see [“Configuring call handling actions” on page 258](#).

---

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 255](#).

#### 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:

<i>GUI field</i>	<i>Description</i>
<b>Test Call - Dry Run</b>	Run a system outbound dial plan test without making a real phone call.
<b>Destination number</b>	Enter a destination number to call.
<b>From number</b>	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.
<b>Test</b>	Click to start the dry run test and view the <i>Test result</i> .
<b>Reset</b>	Click to remove the test result in order to start a new test.
<b>Test Call</b>	Test the dial plan by making a real phone call.
<b>Destination number</b>	Enter a destination number to call.
<b>After call is established</b>	Select the FortiVoice action once it calls the destination number: <ul style="list-style-type: none"><li>• <i>Play welcome message</i>: The FortiVoice unit will play a message to the destination number.</li><li>• <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.</li></ul>

---



<b>Test</b>	Click to start the test and view the <i>Test result</i> .
<b>Reset</b>	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 2:** 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 3:** 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:

<b>GUI field</b>	<b>Description</b>
<b>Match Pattern</b>	

<b>New</b>	Click to add the number pattern in the <i>Value</i> field following “ <a href="#">Pattern-matching syntax</a> ” on page 257 and “ <a href="#">Pattern-matching examples</a> ” on page 257 for this dial plan. Repeat to add more patterns.
<b>Modification</b>	You can manipulate the number patterns you entered.
<b>Strip</b>	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.
<b>Prefix</b>	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.
<b>Postfix</b>	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:

<b>GUI field</b>	<b>Description</b>
<b>Call Handling Action</b>	
<b>Schedule</b>	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 “ <a href="#">Scheduling the FortiVoice unit</a> ” on page 131.
<b>Action</b>	Select the call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern.
<b>Outgoing trunk</b>	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 “ <a href="#">Configuring Trunks</a> ” on page 173.

<b>Caller ID modification</b>	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 “ <a href="#">Modifying caller IDs</a> ” on page 120.
<b>Warning message</b>	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 “ <a href="#">Managing sound files and music on hold</a> ” on page 117.
<b>Delay</b>	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:

<b>GUI field</b>	<b>Description</b>
<b>System station ID</b>	Enter a station ID that shows on each fax sent from the FortiVoice unit.
<b>System fax header</b>	Enter a fax subject header that shows on each fax sent from the FortiVoice unit.
<b>T.38 Fax</b>	
<b>Sending Fax: Initiate a T.38 reinvite if the remote end does not</b>	Select if the fax receiving terminal does not reply to a T.38 invitation.
<b>Sending/Receiving: Fallback to audio (G.711) mode on T.38 failure</b>	Select to use G.711 mode if T.38 communication fails.
<b>Send Queue</b>	
<b>Max retry times</b>	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.

<b>Retry interval</b>	Enter the time interval between fax sending retries.
<b>Wait time for an answer</b>	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*.
2. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Rotation Settings</b>	
<b>Fax rotation size/time</b>	Enter the archived fax file rotation size and time.  When the file reaches either the rotation size or time specified, whichever comes first, the archiving file is automatically renamed. The FortiVoice unit generates a new file, where it continues saving recording archives. You can access all rotated files through search.
<b>Archiving options when disk quota is full</b>	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.
<b>Schedule</b>	Select a schedule for the rotation.
<b>Destination Settings</b>	
<b>Destination</b>	Select an archiving destination: <ul style="list-style-type: none"> <li>• <i>Local</i>: the FortiVoice unit’s local hard drive or a NAS server.</li> <li>• <i>Remote</i>: a remote FTP or SFTP storage server.</li> </ul>
<b>Local disk quota</b>	If <i>Local</i> is the archiving destination, enter the disk space quota.  The total disk quota for archiving calls cannot exceed 20% of the total data disk size. For example, if the data disk has a size of 100 GB, a maximum of 20 GB can be used for fax archiving.  If this quota is met and a new fax must be archived, the FortiVoice unit either automatically removes the oldest fax archive folder in order to make space for the new archive or stops archiving, depending on the settings you specify under “ <a href="#">Rotation Settings</a> ” on page 247.

If *Remote* is the archiving destination, configure the following:

<b>Protocol</b>	Select the protocol that the FortiVoice unit will use to connect to the remote storage server, either SFTP or FTP.
<b>IP address</b>	Enter the IP address of the remote storage server.
<b>User name</b>	Enter the user name of an account the FortiVoice unit will use to access the remote storage server, such as FortiVoice.
<b>Password</b>	Enter the password for the user name of the account on the remote storage server.
<b>Remote directory</b>	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> .
<b>Remote cache quota</b>	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*.

## Setting calendar reminder

You can schedule daily events and send event reminders. You first create a reminder record before setting up reminder events. One reminder record can contain multiple reminder events.

### To schedule an event

1. Go to *Call Features > Reminder* and click *New*.
2. Enter a name for the reminder.
3. Enable the reminder and add notes if required.
4. Click *Create*.
5. In the reminder list, select the reminder record you just created.
6. Click *Edit in calendar mode*.
7. Double-click a date.
8. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Title</b>	Enter a name for the reminder event.
<b>Location</b>	Enter the location for the event.
<b>Start time</b>	Specify when the event starts.
<b>Recurrence</b>	Click <i>None</i> to configure recurrence settings.
<b>Description</b>	Enter any notes as required.

<b>Guest</b>	<p>Click <i>Add</i> to select the internal and external phone numbers to which you want to send event reminder calls.</p> <p>If you want to delete a number, select the number and click <i>Remove</i>.</p>
<b>Reminder audio</b>	<p>Configure the reminder audio that are sent to the selected guest phones.</p> <ul style="list-style-type: none"> <li>• <i>Default</i>: The reminder audio will be a beep sound.</li> <li>• <i>Create New</i>: Click to customize the reminder audio. For <i>Action</i>, click <i>Call me</i> to record a message from an extension; <i>Upload</i> to look for an existing reminder audio; and <i>Download</i> to save the audio file. For <i>Extension</i>, if you select <i>Call me</i> for <i>Action</i>, select the extension on which you want to record a message.</li> <li>• Click <i>Create</i> and <i>Create</i> to exit.</li> </ul>

## 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.

There are:

- **Vertical Service Codes**: a sequence of digits and the signals star (\*) and number sign (#) dialed on a telephone keypad or rotary dial to enable or disable certain telephony service features.
- **Mid-Call/DTMF Codes**: allow you to hold, transfer, and conference calls by using DTMF digit codes entered on the phone.

**Table 4:** Vertical Service Codes

<b>GUI field</b>	<b>Description</b>
<b>Call bridge (DISA)</b>	<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 &gt; Class of Service &gt; Account code</i>). Once you pass authorization, you can use PBX service just like a local extension.</p>
<b>Check hot desk login status</b>	<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>
<b>Hot desk user login</b>	<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>

**Table 4:** Vertical Service Codes

<b>GUI field</b>	<b>Description</b>
<b>Hot desk user logout</b>	To log out hot desking, press *12 or the code you set.
<b>Reset phone to be 'unassigned' by admin</b>	<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 <a href="#">“Configuring SIP phone auto-provisioning” on page 112.</a></p>
<b>Reset phone to be 'unassigned' by user</b>	<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 <a href="#">“Configuring SIP phone auto-provisioning” on page 112.</a></p>
<b>Configure phone to extension by administrator</b>	<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 <a href="#">“Configuring SIP phone auto-provisioning” on page 112.</a></p>
<b>Configure phone to extension by user</b>	<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>
<b>Lookup name directory from extension</b>	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.
<b>Listen/Barge</b>	Dial *50 or the code you set to monitor a call by listening to it. You also need to enter your voicemail PIN. For details, see <a href="#">“Monitor/Recording” on page 239</a>
<b>Agent login to all queues</b>	Dial *61 or the code you set to log into the queues of which your extension is a member.
<b>Agent logout from all queues</b>	Dial *62 or the code you set to log out of the queues of which your extension is a member.
<b>Agent login to a queue</b>	<p>Dial *63 or the code you set and enter your voicemail password and the queue extension to log into this queue.</p> <p>The voicemail password is required only if this option is selected for your extension. For more information, see <a href="#">“Call Center” on page 140.</a></p>

**Table 4:** Vertical Service Codes

<b>GUI field</b>	<b>Description</b>
<b>Agent login from a queue</b>	Dial *64 or the code you set and enter your voicemail password and the queue extension to log out of this queue.  The voicemail password is required only if this option is selected for your extension. For more information, see <a href="#">“Call Center” on page 140</a> .
<b>Login all queue members</b>	Dial *65 or the code you set to login all members of a queue of which your extension is a member. This is an action by the administrator.
<b>Logout all queue members</b>	Dial *66 or the code you set to logout all members of a queue of which your extension is a member. This is an action by the administrator.
<b>Pause agent all queues</b>	Dial *67 or the code you set and enter your voicemail password and the reason code to pause all queues of which this extension is a member.  For information on reason codes, see <a href="#">“Modifying agent reason code descriptions” on page 217</a> .
<b>Unpause agent all queues</b>	Dial *68 or the code you set and enter your voicemail password and the reason code to unpause all queues of which this extension is a member.  For information on reason codes, see <a href="#">“Modifying agent reason code descriptions” on page 217</a> .
<b>Set call forward</b>	Dial *71 followed by a code to set user’s call forward: 1 to enable, 0 to disable, and 9 to change the forwarding number.
<b>User’s quick mode switch</b>	Dial *72 followed by 1, 2, or 3 and enter your voicemail password to temporarily replace the original personal schedule with one of the three default ones. You may also modify the temporary schedule. Dial *720 to go back to the original schedule.
<b>User’s twinning mode switch</b>	Dial *73 followed by 1 to enable twinning and 0 to disable twinning. For information on twinning, see <a href="#">“Twinning Setting” on page 160</a> .
<b>Enter floating mode and make outgoing call on floating host device</b>	This code allows you to make international or long distance calls from a floating host device which is a device (usually a phone) that allows other extensions to originate a call.  Dial *74 or the code you set and dial the outgoing call number when hearing the dial tone. When you are prompted to input the code, enter the code based on the call restriction in the user privileges associated with your extension. For more information, see <a href="#">“Floating code format” on page 267</a> .



**Table 4:** Vertical Service Codes

<b>GUI field</b>	<b>Description</b>
<b>Hotel room condition</b>	<p>Dial *75 or the code you set and enter a maid code to show the room condition.</p> <p>The maid codes include:</p> <ul style="list-style-type: none"> <li>• 1: Maid present</li> <li>• 2: Clean</li> <li>• 3: Not clean</li> <li>• 4: Out of service</li> <li>• 5: To be inspected</li> <li>• 6: Occupied/clean</li> <li>• 7: Occupied/not clean</li> <li>• 8: Vacant/clean</li> <li>• 9: Vacant/not clean</li> </ul> <p>For information on maid codes, see <a href="#">“Configuring hotel management settings”</a> on page 224.</p>
<b>Minibar notification</b>	<p>Dial *76 or the code you set and enter a minibar code to order room items.</p> <p>For information on minibar codes, see <a href="#">“Configuring hotel management settings”</a> on page 224.</p>
<b>Wake-up call</b>	<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>
<b>DND on</b>	<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>
<b>DND off</b>	<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>
<b>Pickup any ringing extension in pickup group</b>	<p>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.</p> <p>For information on pickup groups, see <a href="#">“Creating pickup groups”</a> on page 167.</p>
<b>Pickup group extension</b>	<p>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.</p> <p>For information on pickup groups, see <a href="#">“Creating pickup groups”</a> on page 167.</p>
<b>System schedule override</b>	<p>An administrator with the privilege can dial *82 followed by 1, 2, or 3 and the administrator PIN to temporarily replace the original system schedule with one of the three default ones. You may also modify the temporary schedule. Dial *820 to go back to the original schedule. See <a href="#">“Configuring system capacity”</a> on page 116.</p>
<b>Intercom</b>	<p>Dial *92 or the code you set and an extension to intercom that extension.</p>

**Table 4:** Vertical Service Codes

<b>GUI field</b>	<b>Description</b>
<b>Voicemail direct</b>	Dial *97 or the code you set from your own phone and then enter your voicemail password to directly access your voice mailbox.
<b>Voicemail prompt</b>	Dial *98 or the code you set from any extension and then enter your extension number and voicemail password to access your voice mailbox.
<b>Operator</b>	Dial 0 or the code you set to access the operator.
<b>One key DND</b>	This is for supporting the DND key on the FortiFones. Press the DND key on the FortiFone to turn DND on or off.
<b>Page group</b>	Enter PAGEGROUP or the code you set then the page group number to page the extension group.
<b>Unpark</b>	This is for supporting the Unpark key on the FortiFones. Press this key on the FortiFone to unpark a call.

**Table 5:** Mid-Call/DTMF Codes

<b>GUI field</b>	<b>Description</b>
<b>Blind transfer</b>	Blind transfer serves 2 purposes: <ul style="list-style-type: none"> <li>• During a call, dial *11 or the code you set and then the extension number of a second person to transfer the call to the person without talking to the person.</li> <li>• During a call, dial *11 and then the call parking number (default is 300) to park a call. For details, see <a href="#">“Configuring call parking”</a> on page 252.</li> </ul>
<b>Attended transfer</b>	During a call, dial *12 or the code you set and then the extension number of a second person to transfer the call to the person. Since you want to inform the second person about the call, you can have a private conversation with the person without the first person who made the call hearing it.
<b>Start personal recording</b>	Dial *30 or the code you set to start personal call recording. Personal recordings can be reviewed on the user web portal.  Before doing so, have the agreement of the person you talk with or check your local laws regarding phone recording.
<b>Start system recording</b>	Dial *35 or the code you set to start system call recording. System recordings need administrator permission and can be viewed on the system administration web GUI.  Before doing so, have the agreement of the person you talk with or check your local laws regarding phone recording.
<b>Pause system recording</b>	Dial *36 or the code you set to pause system call recording.
<b>Resume system recording</b>	Dial *37 or the code you set to resume system call recording.

**Table 5:** Mid-Call/DTMF Codes

<b>GUI field</b>	<b>Description</b>
<b>Cancel system recording</b>	Dial *38 or the code you set to cancel system call recording.
<b>Park</b>	Dial *40 or the code you set to park a call.

**Table 6:** Floating code format

<b>Caller privilege</b>	<b>Code format</b>
Allow	Extension number + * + extension user PIN <b>or</b> extension number + * + extension PIN (account code)
Allow with personal code	Extension number + * + extension user PIN
Allow with account code	Extension number + * + user privilege account code
Allow with account and personal code	Extension number + * + user privilege account code <b>or</b> extension number + * + extension user PIN

# Configuring Logs and Reports

The *Log & Report* menu lets you configure FortiVoice logging and reporting.

FortiVoice units provide extensive logging capabilities for voice incidents and system events. Detailed log information provides analysis of network activity to help you identify network issues and reduce network misuse and abuse.

Logs are useful when diagnosing problems or when you want to track actions the FortiVoice unit performs as it receives and processes phone calls.

Reports provide a way to analyze log data without manually going through a large amount of logs to get to the information you need.

This topic includes:

- [About FortiVoice logging](#)
- [Configuring logging](#)
- [Configuring report profiles and generating call reports](#)
- [Submitting CDRs to a database](#)
- [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 269](#).

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 270](#). It can also use log messages as the basis for reports. For more information, see [“Configuring report profiles and generating call reports” on page 274](#).

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 7:** 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.
Call center	IVR	Includes call center events.



Avoid recording highly frequent log types such as voice logs to the local hard disk for an extended period of time. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

## Log message severity levels

Each log message contains a field that indicates the severity level of the log message, such as warning.

**Table 8:** 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 269.

For information on viewing locally stored log messages, see “[Viewing log messages](#)” on page 33.

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 33.

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 76.

#### 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 271](#).
  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 9:** Events logging options

<b>Event Log</b>	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"><li>• <i>When configuration has changed:</i> Log configuration changes.</li><li>• <i>Admin login/logout event:</i> Log all administrative events, such as logins, resets, and configuration updates.</li><li>• <i>System activity event:</i> Log all system-related events, such as rebooting the FortiVoice unit.</li><li>• <i>SMTP server event:</i> Log SMTP relay or proxy events. This option is for local log setting only.</li><li>• <i>HA:</i> Log all high availability (HA) activity.</li><li>• <i>DHCP event:</i> Log DHCP server events. This option is for local log setting only.</li><li>• <i>Voice mail event:</i> Log voicemail events. This option is for remote log setting only.</li><li>• <i>Monitor:</i> Log call recording, call barging, and traffic capture events.</li></ul>
<b>Voice Log</b>	Log phone call events. This option is for local log setting only.
<b>Fax Log</b>	Log fax events.
<b>DTMF Log</b>	DTMF (Dual Tone Multi-Frequency) events.
<b>Hotel Log</b>	Log hotel management events, such as guest check-in and check-out.
<b>Call Center Log</b>	Log call center events, such as IVR events.

## 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 270.

Before you can log to a remote location, you must first enable logging. For details, see “Choosing which events to log” on page 271. 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 76.

### To configure logging to a Syslog server or FortiAnalyzer unit

1. Go to *Log & Report > Log Settings > Remote Log Settings*.

<b>GUI field</b>	<b>Description</b>
<b>Enabled</b>	Select to enable remote storage on the server. Clear to disable storage.



<b>Profile Name</b>	Displays the remote host name.
<b>Server</b>	Displays the IP of the Syslog server or FortiAnalyzer unit.
<b>Port</b>	Displays the port on the Syslog server or FortiAnalyzer unit.
<b>Level</b>	Displays the minimum severity level for logging purposes.
<b>Facility</b>	Displays the facility identifier the FortiVoice unit uses to identify itself.

- Click *New* to create a new entry or double-click an existing entry to modify it.

<b>GUI field</b>	<b>Description</b>
<b>Log to Remote Host</b>	
<b>Enable</b>	Select to allow logging to a remote host.
<b>Name</b>	Enter a name for the remote host.
<b>IP</b>	Enter the IP address of the Syslog server or FortiAnalyzer unit where the FortiVoice unit will store the logs.
<b>Port</b>	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).
<b>Level</b>	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 <a href="#">“Log message severity levels”</a> on page 269.
<b>Facility</b>	Select the facility identifier that the FortiVoice unit will use to identify itself when sending log messages.  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.
<b>CSV format</b>	Enable this option if you want to send log messages in comma-separated value (CSV) format.  Do not enable this option if the remote host is a FortiAnalyzer unit. FortiAnalyzer units do not support CSV-formatted log messages.
<b>Logging Policy Configuration</b>	Click the arrow to review the options and enable the types of logs you want to record to this storage location. For details, see <a href="#">“Choosing which events to log”</a> on page 271.

- Click *Create*.
- 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 42 and "About the management IP" on page 41) and static routes (see "Configuring static routes" on page 47), 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.



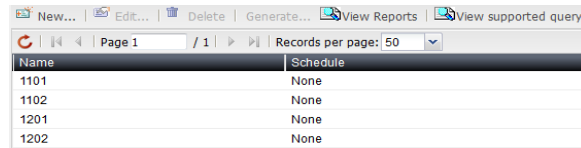
Generating reports can be resource intensive. To avoid phone processing performance impacts, you may want to generate reports during times with low traffic volume, such as at night. For more information on scheduling the generation of reports, see "Configuring report email notifications" on page 277.

---

### To view and configure report profiles

1. Go to *Log & Report > Call Report > Call Report*.

**Figure 2:** Configuration tab



Name	Schedule
1101	None
1102	None
1201	None
1202	None

<b>GUI field</b>	<b>Description</b>
<b>Generate</b>	Select a report and click this button to generate a report immediately. See <a href="#">“Generating a report manually” on page 278</a> .
<b>View Reports</b>	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 <a href="#">“Viewing generated reports” on page 32</a> .
<b>Report Name</b>	Displays the name of the report profiles.
<b>Schedule</b>	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 3:** 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:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for this query.
<b>Category</b>	Select a category for the report profile. The report chart will correspond to the category selected. <ul style="list-style-type: none"><li>• <i>Call Usage</i>: The number of calls.</li><li>• <i>Phone Bill</i>: The cost of making the phone calls.</li><li>• <i>Trunk Usage</i>: The status of the trunks being used.</li></ul>
<b>Subcategory</b>	Select to have a summary or detailed report on the report category you select.
<b>From</b>	Select to include the source of the incoming calls: <i>Internal</i> , <i>External</i> , or <i>Any</i> .
<b>To</b>	Select to include the source of the outgoing calls: <i>Internal</i> , <i>External</i> , or <i>Any</i> .
<b>Region</b>	Select the call region, such as international or long-distance.
<b>Report column</b>	Select the source of the call statistics: from caller or receiver. For details, see <a href="#">Figure 4 on page 277</a> .
<b>Sort column</b>	Select the value for filtering the call information. The caller or receiver with the higher value moves to the top of the table.  If you select <i>Report column</i> , the sort column value is equal to what you select in the <i>Report column</i> field.  For details, see <a href="#">Figure 4 on page 277</a> .
<b>Separate table</b>	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.  You can select to enable or disable the pre-defined table settings of the query values, although this is not recommended.

5. Click *Create*.

**Figure 4:** 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	fcc60	00:00:02	0.00
	2012-11-27 / Tue	10:23	7817	fcc60	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 call report and notification email templates](#)” on page 109.

### 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 278](#).

### To configure the report schedule

1. Go to *Log & Report > Call Report > Call Report*.
2. Expand *Schedule*.
3. Configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Type</b>	<ul style="list-style-type: none"><li>• <i>None</i>: Select if you do <b>not</b> 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 <a href="#">“Generating a report manually” on page 278</a>.</li><li>• <i>Daily</i>: Select to generate the report each day. Also configure <i>Hour</i>.</li><li>• <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>.</li><li>• <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>.</li></ul>

## 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 279](#).

### 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 32](#).

## 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:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for the rating profile.
<b>Trunk</b>	Select the trunk that will use the rates.
<b>Local</b>	Enter the rate for local phone calls.
<b>Long distance</b>	Enter the rate for long-distance phone calls.
<b>International</b>	Enter the rate for international phone calls.
<b>Other rate</b>	Enter the rate for other types of phone calls.
<b>Comment</b>	Enter any notes you have for this rating profile.

3. Click *Create*.

## Submitting CDRs to a database

If you have a remote third party database, you may submit the Call Detail Records (CDR) to the database. Each CDR contains the full life cycle of a call. Using the database's interface, you can display and review the CDRs.



To enable CDR submission, make sure to select *Remote CDR name*. For more information, see [“Setting up an IVR” on page 208](#).

This section includes the following topics:

- [Configuring CDR submission](#)
- [Modifying CDR templates](#)
- [Creating CDR filters](#)

## Configuring CDR submission

The *Log & Report > CDR > Submit CDR* submenu lets you configure sending CDR to a database. The configuration values should match those of the database server.

### To submit a CDR

1. Go to *Log & Report > CDR > Submit CDR*.

- Click *New* and configure the following:

<b>GUI field</b>	<b>Description</b>
<b>Name</b>	Enter a name for the configuration.
<b>Status</b>	Select to enable the configuration.
<b>Description</b>	Click to enter any notes you have for the configuration.
<b>Remote RESTful Server</b>	Configure the database to which CDRs are submitted.
<b>Protocol</b>	Select the protocol used for information transmission between the FortiVoice unit and the database server.
<b>Http headers</b>	Select <i>Click to edit</i> to enter a HTTP header for sending information to the database server.
<b>Http timeout</b>	Enter the time allowed for the submission to be processed. The range is 1-60 minutes.
<b>URI</b>	Enter the Uniform Resource Identifier to represent the CDR to be submitted.
<b>Authentication</b>	Select to enter the user name and password for logging onto the database server.
<b>SSL verification</b>	Select if required.
<b>Options</b>	
<b>Retry</b>	Enter the times to retry submission. The range is 1-10 times.
<b>Retry interval</b>	Enter the retry interval in minutes (5-60).
<b>CDR template</b>	Click <i>Edit</i> to customize the default CDR submission template based on the requirements of the database server. Click <i>OK</i> when it is done. For more information, see <a href="#">“Modifying CDR templates” on page 280</a> .
<b>CDR filter</b>	Choose or create a new CDR filter to screen CDRs submitted to the database. For more information, see <a href="#">“Creating CDR filters” on page 281</a> .
<b>Custom value</b>	Click <i>New</i> to add a custom value (a token, for example) that is required by the database server for information exchange.

- Click *Create*.

## Modifying CDR templates

When configuring CDR submission, you need to customize the default CDR submission template based on the requirements of the database server.

### To modify a CDR template

- Go to *Log & Report > CDR > CDR Template*.
- Select the default CDR template and click *Edit*.



3. Modify the template and click *OK*.

## Creating CDR filters

You can use filters to limit the amount of CDRs submitted to the database.

### To create a CDR filter

1. Go to *Log & Report > CDR > CDR Filter*.
2. Click *New*.
3. Enter a name for the filter.
4. Using XML, enter the CDR filters based on the values you want, such as call queues or call IDs and so on.
5. For *Description*, enter any notes you have for the filter.
6. Click *OK*.

## Configuring Station Messaging Detail Record (SMDR)

FortiVoice SMDR component provides FortiVoice call detail records to third party devices on certain communication and format protocols based on third party's device requirements. For example, Property Management System (PMS) uses the FortiVoice SMDR to manage hotel guest call charges.



Configuring FortiVoice SMDR requires advanced SMDR knowledge and should be performed by advanced administrative users and field engineers.

---

This section contains the following topics:

- [Configuring SMDR settings](#)
- [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 282.
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 5:** 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 *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 XML types* to view the Fortinet SMDR format file and correct your format file accordingly.

## Configuring alert email

The *Alerts* submenu lets you configure the FortiVoice unit to notify selected users (including administrators) by email when specific types of events occur and are logged. For example, if you require notification about system activity event detections, you can have the FortiVoice unit send an alert email message whenever the FortiVoice unit detects a system activity event.

To set up alerts, you must configure both the alert email recipients (see [“Configuring alert recipients”](#) on page 283) and which event categories will trigger an alert email message (see [“Configuring alert categories”](#) on page 283).

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 48](#).

You can customize the alert email. For more information, see [“Customizing call report and notification email templates” on page 109](#).

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*.

<i>GUI field</i>	<i>Description</i>
<b>Test</b> (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.
<b>Alert Email Account</b>	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 283](#)).

### 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 10:** Alert email category choices

<i>GUI field</i>	<i>Description</i>
<b>Critical events</b>	Send an alert email message when the FortiVoice unit detects a system error that may affect its operation.
<b>Disk is full</b>	Send an alert email message when the hard disk of the FortiVoice unit is full.
<b>HA events</b>	Send an alert email message when any high availability (HA) event occurs.
<b>Archive quota is exceeded</b>	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 <a href="#">“Archiving recorded calls” on page 247</a> .

**Table 10:** Alert email category choices

<b>GUI field</b>	<b>Description</b>
<b>Deferred emails # over</b>	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.
<b>Daily call summary</b>	Send an alert email with a daily call summary including the number of total calls, long distance calls, and international calls.  You need to enter the time for generating the summary which is for the 24 hours period prior to the time you set. For example, if you set 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.
<b>PRI alarm</b>	Send an alert email when the PSTN digital line has a problem. This option is not available for FortiVoice 200D.
<b>FXO alarm</b>	Send an alert email when the PSTN analog line has a problem. This option is not available for FortiVoice 200D.
<b>Trunk lines are saturated</b>	Send an alert email when the SIP/PSTN/PRI trunk lines are fully occupied.  SIP trunk alert only works if you select <i>Overflow check</i> when configuring SIP trunk. See <a href="#">“Setting up VoIP trunks” on page 173</a> .
<b>Massive SIP authentication failure</b>	Send an alert email when big scale SIP authentication sessions fail.
<b>Trunk alert</b>	Select the trunks of which an alert email is sent when a trunk has an issue.  Also set the time interval for sending alert email in seconds.

3. Click *Apply*.

# Installing firmware

Fortinet periodically releases FortiVoice firmware updates to include enhancements and address issues. After you have registered your FortiVoice unit, FortiVoice firmware is available for download at <http://support.fortinet.com>.

New firmware can also introduce new features which you must configure for the first time.

***For information specific to the firmware release version, see the Release Notes available with that release.***



In addition to major releases that contain new features, Fortinet releases patch releases that resolve specific issues without containing new features and/or changes to existing features. It is recommended to download and install patch releases as soon as they are available.



Before you can download firmware updates for your FortiVoice unit, you must first register your FortiVoice unit with Fortinet Technical Support. For details, go to <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 units 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 287.
  - 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 291.

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 103.

### 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 289](#) and [“Restoring the configuration” on page 290](#).

If you have upgraded the firmware version, to verify the conversion of the configuration file, see [“Verifying the configuration” on page 291](#). 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 292](#).

### 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 11:** Port settings

<b>Bits per second</b>	9600
<b>Data bits</b>	8
<b>Parity</b>	None
<b>Stop bits</b>	1
<b>Flow control</b>	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 290](#).

## 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 103](#).

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 291](#).

### 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 291](#).

## 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 103. For information on reconnecting to a FortiVoice unit whose network interface configuration has been reset, see “[Reconnecting to the FortiVoice unit](#)” on page 289.

---



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 units starts, a series of system startup messages are displayed.  

```
Press any key to display configuration menu.....
```

9. Immediately press a key to interrupt the system startup.



You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiVoice unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appear:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[I]: Configuration and information.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

Enter G,F,B,I,Q, or H:

**10.** If the firmware version requires that you first format the boot device before installing firmware, type F. (Format boot device) before continuing.

**11.** Type G to get the firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.2.99]:
```

**12.** Type the IP address of the TFTP server and press Enter.

The following message appears:

```
Enter Local Address [192.168.1.188]:
```

**13.** Type a temporary IP address that can be used by the FortiVoice unit to connect to the TFTP server.

The following message appears:

```
Enter File Name [image.out]:
```

**14.** Type the firmware image file name and press Enter.

The FortiVoice unit downloads the firmware image file from the TFTP server and displays a message similar to the following:

```
Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]
```

**15.** Type D.

The FortiVoice unit downloads the firmware image file from the TFTP server. The FortiVoice unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.

The FortiVoice unit reverts the configuration to default values for that version of the firmware.

**16.** Clear the cache of your web browser and restart it to ensure that it reloads the web-based manager and correctly displays all tab, button, and other changes.

**17.** To verify that the firmware was successfully installed, log in to the CLI and type:

```
get system status
```

The firmware version number appears.

**18.** Either reconfigure the FortiVoice unit or restore the configuration file from a backup. For details, see [“Restoring the configuration”](#) on page 290.

# 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 42.
  - **User Extension #:** Enter the user ID of the extension. For details, see “Configuring IP extensions” on page 134.
  - **Password:** Enter the password used for configuring your SIP phone from the phone or the Web. For details, see “Configuring IP extensions” on page 134.
-

# Index

## A

- active-passive HA 58
- address bar 21
- administrative access 43
- administrator
  - "admin" account 16, 17, 287, 288, 290, 291, 292
  - log messages 272
- alert email 59, 282
  - recipients 283
- appearance, web-based manager 91
- authentication 16
  - LDAP 125

## B

- backup unit 56
- bandwidth 24
- Base64 100, 101
- bind DN 126, 127, 128
- boot interrupt 292
- browser 15, 16, 20
  - warnings 16
- Buffalo TeraStation 94

## C

- cable
  - null modem 17
- call statistics 25
- certificate
  - backup 102
  - default 16
  - mismatch 16
  - options 98
  - self-signed 16
  - server 96
  - warning 16
- certificate authority (CA) 16, 97, 98, 100, 101, 102, 103
- certificate request
  - downloading and submitting 100
- certificate revocation list (CRL) 103
- certification 9
- CIDR 13
- clean install firmware 292
- CLI 46
  - connecting to 17
- column view
  - logs 35
- command line interface (CLI) 10, 12, 15
- comma-separated value (CSV) 273
- common name (CN) field 16
- communications (COM) port 17
- configuration, verifying the 291
- configured operating mode 60
- connecting
  - web UI 16
- conventions 10

- CPU 24, 84
- CSV import 142

## D

- dashboard 22
- date 76
- daylight savings time (DST) 76, 77
- default
  - administrator account 16, 17, 287, 288, 290, 291, 292
  - bridge configuration 41
  - certificate 16
  - gateway 47
  - password 16, 17, 18, 19
  - route 47
  - settings 17
- DHCP 45
- DNS server 48, 282
- documentation 10
  - conventions 10
  - Release Notes 292
- domain name
  - certificate 16
- DOS 15
- dotted decimal 13
- downgrade 287
- download
  - report 32
- dynamic DNS (DDNS) 99
- dynamic IP address 45

## E

- effective operating mode 62
  - HA 60
- \_email 13
- end-user guide 20
- Ethernet 16, 17
- expected input 12
- extended unique identifier (EUI) 95

## F

- factory default settings 17
- failover 63, 65, 66, 83
  - HA 69
- FAQ 10
- Fedora 94
- firmware 287
  - change 23
  - clean install 292
  - downgrade 287
  - upgrade 287
  - version 22
- formatted view
  - logs 35
- formatting the boot device 292

FortiAnalyzer 94, 270, 272

Fortinet

Knowledge Base 10

MIB 87, 88

Technical Documentation 10

conventions 10

Technical Support 9

Technical Support, registering with 9

Technical Support, web site 9

Training Services 9

\_fqdn 13

frame size 46

FreeNAS 94

fully qualified domain name (FQDN) 13, 99

fully-qualified domain name (FQDN) 99

## G

gateway 47

glossary 10

graphical user interface (GUI) 15

## H

HA

active-passive 58

alert email 59

backup unit 56

configuration not synchronized 57

configuration options 58, 62

configured operating mode 60

effective operating mode 60, 62

failover 63, 65, 66, 69, 83

forcing configuration synchronization 61

forcing data synchronization 61

heartbeat 57, 59

interface configuration synchronization 58

log messages 59

mail queue sync after a failover 58

master 56

monitoring 57, 68

MTA spool directory sync after a failover 58

network interface 58

primary unit 56

service monitoring 58, 59

slave 56

synchronization 57, 59

virtual IP 68

wait for recovery then assume slave role 64, 71

wait for recovery then restore original role 64, 71

halt 24

hard disk

logging to 270

heartbeat 59

HA 57

high availability (HA) 55

log messages 272

host name 16

in HA 57

how-to 10

HA 58

HTTP

web-based manager 46

HTTPS 16, 46, 96, 99

HyperTerminal 17

## I

ICMP ECHO 46

idle timeout 81

import

user in CSV 142

\_index 13

index number 13

InetOrgPerson 128

input constraints 12

\_int 13

Internet service provider (ISP) 48

IP address 16, 17, 21

private network 10

\_ipv4 13

\_ipv4/mask 13

\_ipv4mask 13

\_ipv6 13

\_ipv6mask 13

iSCSI

qualified name (IQN) 95

## K

Knowledge Base 10

## L

language

web-based manager 92

LDAP

bind 126

bind DN 127, 128

cache 129

password 126

profile 125

query 128

schema 128

timeout 129

TTL 129

LDAPS 126

Linux 94

local certificate

options 98

location 21

log

column view 35

formatted view 35

FortiAnalyzer 272

rotate 271

search 37

severity level 269

storage 270

storing 270

Syslog 272

to the hard disk 270



## M

- management IP 41
- master 56
- master, HA mode 64
- maximum transmission unit (MTU) 46
- media access control (MAC) 44
- memory usage 24
- MIB 88
  - Fortinet 87
  - RFC 1213 87
  - RFC 2665 87
- Microsoft
  - Internet Explorer 16
- Microsoft Active Directory 128
- Microsoft Windows Service for NFS 94
- mode
  - HA 56
- monitor
  - HA 57
- monitoring services
  - for HA 58
- Mozilla Firefox 16

## N

- \_name 13
- network
  - interface 17
- network address authority (NAA) 95
- network attached storage (NAS) 93
  - server 94
- network file system (NFS) 93, 95
- network interface
  - in HA 58
- network time protocol (NTP) 76, 77
- next-hop router 47, 48
- null modem cable 17

## O

- objectClass 128
- on HA failure
  - wait for recovery then assume slave role 64, 71
  - wait for recovery then restore original role 64, 71
- Openfiler 94
- OpenSUSE 94

## P

- password 16, 17, 18, 19
  - administrator 54
  - certificate 102
  - LDAP bind 126
- \_pattern 13
- pattern 13
- PDF report 222, 277
- ping 46
- PKCS #10 100
- PKCS #12 101, 102
- port1 17
- primary unit 56

- privacy-enhanced email (PEM) 101
- product registration 9
- profile
  - administrator access 55
  - LDAP 125
- protocol 129
  - administrative access 54
- public key 101

## Q

- query
  - cache 129
  - filter 128
  - LDAP 128
  - report 221, 275
  - SNMP 86, 87

## R

- reachable 47
- read & write
  - administrator 54
- reconnecting to the FortiMail unit 289
- RedHat 94
- registering
  - with Fortinet Technical Support 9
- regular expression 13
- Release Notes 292
- report
  - configure 220, 274
  - download 32
  - HTML format 222, 277
  - on demand 220, 274
  - PDF format 222, 277
  - periodically generated 220, 274
  - query 221, 275
  - subject matter 221, 275
  - time span 222, 277
  - view 32
- reset
  - effective operating mode for HA 61
- restart 24
- restore
  - factory defaults 40
  - previous configuration 290
- RFC
  - 1213 83, 87
  - 1918 11
  - 2665 83, 87
- RJ-45 16, 17
- route
  - default 47
  - static 47

## S

- secure (S/MIME) 102
- Secure Shell (SSH) 15
- secure shell (SSH) 46
- security certificate 16
- self-signed 16

- services
  - monitoring for HA 58
- severity level 269
- shut down 24
- slave 56
- slave, HA mode 64
- SMB 95
- SNMP 46
  - community 85, 86
  - event 86, 87
  - manager 85, 86, 87, 88
  - MIB 88
  - MIBs 87
  - query 86, 87
  - RFC 12123 87
  - RFC 2665 87
  - traps 88
- SSL 126
- static route 47
- static routing 47
- storing logs 270
- \_str 13
- string 13
- subject matter 221, 275
- synchronization 57
- syntax 12
- Syslog 270, 272
- system options
  - changing 80
  - data and time 76
- system resource usage 22
- system time 22

## T

- T11 network address authority (NAA) 95
- technical
  - documentation 10
  - notes 10
- Telnet 15
- telnet 46
- terminal 15, 17
- time 76
- time to live (TTL)
  - cache 129
  - LDAP 129
- time zone 77
- timeout 129

- Training Services 9
- transport layer security (TLS) 102
- traps, SNMP 88
- troubleshooting 129
  - Syslog 274
- trust certificate 16
- trusted host 54

## U

- Ubuntu 94
- UNIX 15
- update 287
  - verify 291
- uptime 22
- URL 16, 21
- \_url 13
- Use secure connection 126
- user
  - group 125
  - query 128
- user guide 20

## V

- \_v4mask 13
- \_v6mask 13
- value parse error 13
- variable
  - Predefined 109
- virtual IP
  - HA 68

## W

- wait for recovery then assume slave role
  - on HA failure 64, 71
- wait for recovery then restore original role
  - on HA failure 64, 71
- web browser 15, 16, 20
  - warnings 16
- web UI 16
- web-based manager
  - customizing appearance 91
  - HTTP 46
  - HTTPS 46
  - language 92
- widget 22
- wild cards 13
- Windows share 95

