



FortiVoice™ 200D v2.0
Setup and Administration Guide



FortiVoice 200D v2.0 Setup and Administration Guide

September 21, 2012

2nd Edition

Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance 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 the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

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

Table of Contents

Setting Up the FortiVoice System	7
Connecting to the web-based manager or CLI	7
Connecting to the web-based manager	8
Connecting to the CLI	9
Setting up the system using the wizard	11
Using the express mode	11
Using the advanced mode	12
Testing the setup	13
Monitoring the FortiVoice System	14
Viewing overall system status	14
Viewing the dashboard	14
Viewing the Call Statistics	17
Using the CLI Console	17
Viewing PBX status	17
Viewing active calls	17
Viewing parked calls	17
Viewing conference calls	17
Viewing extension status	18
Viewing trunk status	18
Viewing DHCP client list	18
Viewing call records	20
Viewing log messages	20
Displaying and arranging log columns	22
Using the right-click pop-up menus	23
Searching log messages	24
Viewing generated reports	25
Playing recorded calls	26
Configuring System Settings	27
Configuring network settings	27
About IPv6 Support	27
About the management IP	28
About FortiVoice logical interfaces	28
Configuring the network interfaces	29
Configuring static routes	33
Configuring DNS	35
Configuring DHCP server	35

Configuring voice	38
Configuring SIP settings	38
Configuring SIP phone auto-provisioning.....	40
Managing phone configurations	42
Configuring voicemail settings.....	42
Configuring system capacity	42
Configuring system time, system options, email setting, and GUI appearance....	43
Configuring the time and date	43
Configuring system options	44
Configuring email settings	46
Customizing the GUI appearance.....	49
Configuring administrator accounts and access profiles	51
Configuring administrator accounts.....	51
Configuring access profiles	54
Managing certificates.....	54
Managing local certificates	55
Obtaining and installing a local certificate	56
Managing certificate authority certificates.....	61
Managing the certificate revocation list.....	62
Maintaining the system	62
Maintaining the system configuration	62
Downloading a trace file	63
Configuring PBX	64
Configuring PBX settings.....	64
Setting PBX location and contact information.....	64
Configuring PBX options.....	65
Configuring number settings.....	65
Mapping speed dials.....	66
Scheduling the FortiVoice unit.....	67
Customizing notification email templates	68
Managing sound files.....	70
Managing music on hold.....	71
Configuring class of services.....	71
Configuring account codes.....	74
Working with SIP profiles and caller IDs.....	74
Configuring SIP profiles	75
Modifying caller IDs	76
Configuring Extensions.....	79
Setting up local extensions.....	79
Configuring IP extensions	79
Setting up remote extensions	83
Setting extension user preferences	84

Creating extension groups.....	87
Creating user groups	87
Creating ring groups	88
Configuring Trunks.....	90
Setting up SIP trunks	90
Configuring office peers.....	94
Configuring Dial Plans	95
Configuring outbound dial plans.....	95
Creating dialed number match	96
Configuring inbound dial plans	98
Configuring direct inward dialing	103
Mapping DIDs	104
Configuring Phone Services.....	105
Configuring auto attendants	105
Viewing auto attendant hierarchies.....	107
Configuring key actions	109
Configuring conference calls	111
Creating page groups	112
Configuring call parking	113
Recording calls	113
Modifying feature access codes.....	113
Configuring Logs and Reports.....	115
About FortiVoice logging	115
FortiVoice log types	115
Log message severity levels	116
Configuring logging.....	116
Configuring logging to the hard disk.....	117
Choosing which events to log.....	118
Configuring logging to a Syslog server or FortiAnalyzer unit.....	118
Configuring report profiles and generating reports	121
Configuring the report query selection	122
Configuring the report time period.....	123
Configuring report email notifications.....	124
Configuring the report schedule	124
Generating a report manually.....	125
Setting call rates	125
Installing firmware.....	126
Testing firmware before installing it	126

Installing firmware	128
Reconnecting to the FortiVoice unit.....	130
Restoring the configuration.....	131
Verifying the configuration	132
Upgrading	132
Clean installing firmware.....	133
Setup for phone users.....	136
Accessing the user web portal	136
Changing the voicemail PIN.....	136
Setting user preferences.....	136
Index	137

Setting Up the FortiVoice System

After physically installing the FortiVoice unit, you need to set up the unit by performing some basic configurations so that you can make and receive phone calls using the FortiVoice unit.

This setup serves as a road map for making the FortiVoice unit up and running. Detailed configuration is described in the other sections of this guide.

Only the configuration procedures through the web-based manager are provided.

This topic includes:

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

Connecting to the web-based manager or CLI

To configure, maintain, and administer the FortiVoice unit, you need to connect to it. There are two methods:

- 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 15.



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.

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 1: Default settings for connecting to the web-based manager

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

To connect to the web-based manager

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

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

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

Both warnings are normal for the default certificate.

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

Login credentials entered are encrypted before they are sent to the FortiVoice unit. If your login is successful, the web UI appears. To continue by updating the firmware, see "[System Information widget](#)" on page 15. Otherwise, to continue by following the configuration wizard, see "[Setting up the system using the wizard](#)" on page 11.

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 2: Default settings for connecting to the CLI by SSH

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



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



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

To connect to the CLI using a local serial console connection

1. Using the RJ-45-to-DB-9 or null modem cable, connect your computer's serial communications (COM) port to the FortiVoice unit's console port.
2. Verify that the FortiVoice unit is powered on.
3. On your management computer, start HyperTerminal.
4. On *Connection Description*, enter a *Name* for the connection and select *OK*.

5. On *Connect To*, from *Connect using*, select the communications (COM) port where you connected the FortiVoice unit.
6. Select *OK*.
7. Select the following *Port* settings and select *OK*.

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

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



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

To connect to the CLI using an SSH connection

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

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

The CLI displays the following text:

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

You can now enter commands.

Setting up the system using the wizard

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

The wizard has two modes:

- *Express mode*: Configure the system settings and extensions for internal calls.
- *Advanced mode*: Configure the system settings, extensions, trunks, dial plans, and auto attendants for internal, external, and office peer calls.

While all settings in each mode 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 *Configuration Wizard* in the top-right button row.

Using the express mode

1. Start the wizard, select *Express mode* and click *Next*.
2. Read the overview information and click *Next* to configure the system settings:
 - a. Enter the *Time Settings* and click *Next*. For more information, see “[Configuring the time and date](#)” on page 43.
 - b. Enter the *IP Setting*, *Route Setting*, and *DNS Setting* and click *Next*. For more information, see “[Configuring network settings](#)” on page 27.
 - c. Enter your main phone number/ID provided by your phone company or ISP and click *Next*.

This caller ID will appear on the phone of an outbound call receiver. In addition to a phone number, it can also contain a name. For example, ABC Inc. <111-222-1234>.
 - d. Configure the *Location Setting* and *Contact Information* and click *Next*. For more information, see “[Setting PBX location and contact information](#)” on page 64.
 - e. Configure the following optional settings:
 - i. For *Extension pattern*, see “[Configuring number settings](#)” on page 65.
 - ii. For *Default user password and voicemail PIN*, see “[Setting up local extensions](#)” on page 79.
 - iii. For *Add/Edit business hours*, see “[Scheduling the FortiVoice unit](#)” on page 67.
 - iv. For *Add administrator*, see “[Configuring administrator accounts and access profiles](#)” on page 51.

3. Click *Next* to configure the settings for making internal calls:
 - a. Click *Import/Add/Edit*.
 - i. If you had exported/saved a copy of your extensions from your previous PBX system into a CSV file, click *Import extensions* to upload the file. Review the imported extensions and click *Next*.
 - ii. Click *Add/Edit extensions* to create or modify extensions and click *Next*. For more information, see “[Configuring IP extensions](#)” on page 79.
 - b. Click *Other Operations*.
 - i. Configure *Add/Edit ring groups* to redirect incoming calls to each extension in a ring group and click *Next*. For more information, see “[Creating ring groups](#)” on page 88.
 - ii. Click *Specify extension for operator/manager* to add extensions of your operator and VoIP network support desk. Click *Next*, *Next*.
4. Click *Finish*.

Using the advanced mode

1. Start the wizard, select *Advanced mode* and click *Next*.
2. Repeat steps 2 to 3 of “[Using the express mode](#)” on page 11.
3. Configure SIP or office trunks as required:
 - a. Click *Trunk Configuration > SIP* to add one or more SIP service providers to the FortiVoice unit trunk configuration and click *Next*.

The service providers deliver telephone services to customers equipped with SIP-based PBX (IP-PBX).

For more information, see “[Setting up SIP trunks](#)” on page 90.
 - b. Click *Trunk Configuration > PSTN trunk* to connect your PBX or VoIP network to your phone companies and through them to the outside world and click *Next*. These trunks can be analog or digital phone lines.
4. Click *Next* to auto-generate dial plans based on the configuration made so far. Do one of the following:
 - a. If you need basic dial plans, click *Auto generation > Choose method > Auto generation - Easy*. When the auto-generation is complete, click *OK*. Click *Next* and then an item to view or edit the generated *Auto attendants*, *Inbound dialplans*, and *Outbound dialplans*. Click *Next*, *Next* to finish the basic auto-generation.

For more information, see “[Configuring auto attendants](#)” on page 105, “[Configuring inbound dial plans](#)” on page 98, and “[Configuring outbound dial plans](#)” on page 95.
 - b. If you need advanced dial plans, click *Auto generation > Choose method > Auto generation - Advanced*.
 - i. Configure the country, area code, and trunks for the dial plans.
 - ii. Click *Next* and then an item to view or edit the generated *Auto attendants*, *Inbound dialplans*, and *Outbound dialplans*. Click *Next*, *Next* to finish the advanced auto-generation.

For more information, see “[Configuring auto attendants](#)” on page 105, “[Configuring inbound dial plans](#)” on page 98, and “[Configuring outbound dial plans](#)” on page 95.
5. Click *Finish*.

Testing the setup

Once you complete the FortiVoice setup using the wizard, you can connect a SIP phone to your VoIP network and have a test call.

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:

- If the SIP phone and the FortiVoice unit (PBX) are on different subnets, proper routing should be set to make them reachable.
- Enter the IP address of the phone if it is not DHCP-enabled.
- Enter the SIP server IP address and port number (5060 by default) of the FortiVoice unit.
- Enter the extension number and SIP password you have configured and make sure the extension is enabled. You can find the information by opening any mode of the *Configuration Wizard* and going to *Internal Setting > Import/Add/Edit > Add/Edit extensions*.

If you have not imported or added any extensions, do it first. For more information, see [“Configuring IP extensions” on page 79](#). The extension number on the FortiVoice unit and your phone should match.

Monitoring the FortiVoice System

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

This topic includes:

- Viewing overall system status
- Viewing PBX status
- Viewing call records
- Viewing log messages
- Viewing generated reports
- Playing recorded calls

Viewing overall system status

Monitor > System Status 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

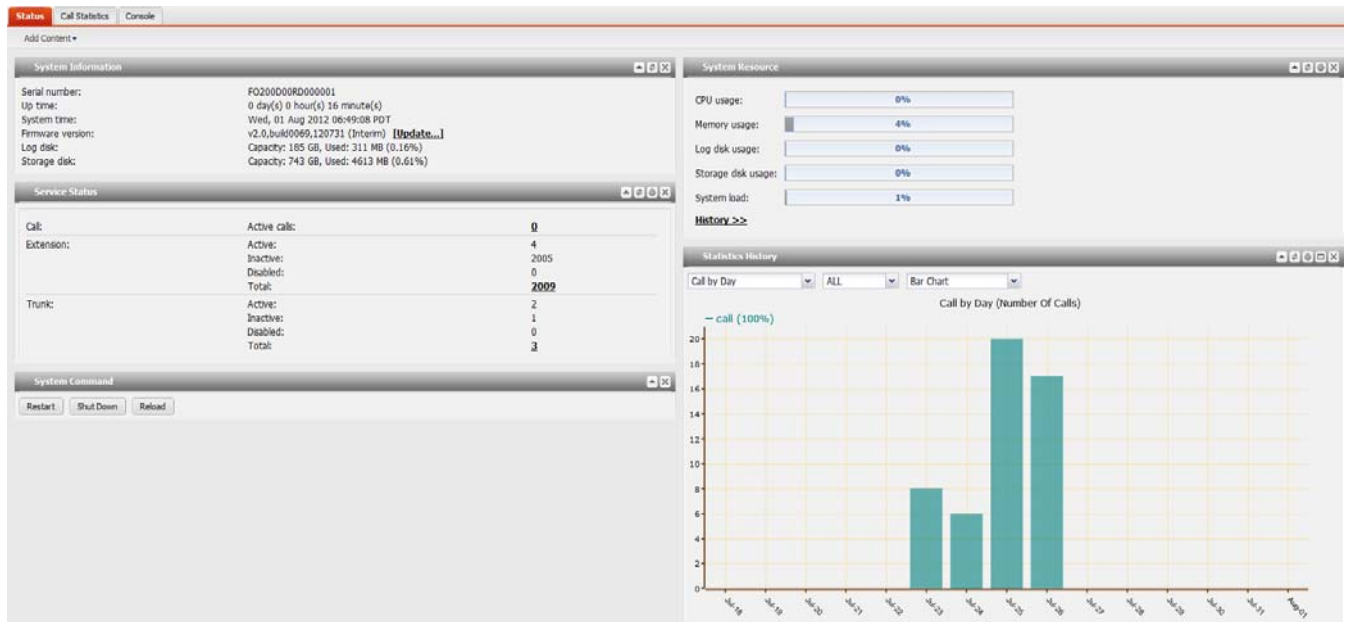
Viewing the dashboard

Monitor > System Status > Status displays first after you log in to the web-based manager. It contains a dashboard with widgets that each indicates performance level or other statistics.

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

To view the dashboard, go to *Monitor > System Status > Status*.

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



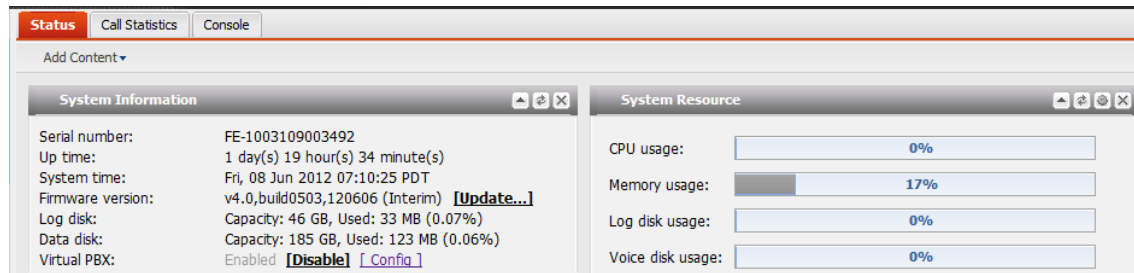
System Information widget

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 126.

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

Figure 3: Virtual PBX enabled



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 *Monitor > System Status > Status*. If the widget is not currently shown, click *Add Content*, and mark the check box for the widget.

Device 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 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 *Monitor > System Status > Status*. 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.

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 *Monitor > System Status > Status*. 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 *Monitor > System Status > Status*. 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 17.

Viewing the Call Statistics

The *Call Statistics* tab contains summaries of the number of calls in each time period that the FortiVoice unit recorded.

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

Using the CLI Console

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

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

Viewing PBX status

Monitor > PBX Status displays all the ongoing phone calls in realtime, parked calls, conference calls, extensions, trunks, and DHCP client list.

Viewing active calls

Monitor > PBX Status > 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 voice mail.

Viewing parked calls

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

To view parked calls, go to *Monitor > PBX Status > Parked Calls*.

For more information on call parking, see “[Configuring call parking](#)” on page 113.

Viewing conference calls

Monitor > PBX Status > 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 clicking the *Kick* icon.

For more information on call conference calls, see “[Configuring conference calls](#)” on page 111.

Viewing extension status

Monitor > PBX Status > Extensions displays all the extensions in realtime, including their names, numbers, statuses, display names, types, and IPs for SIP extensions.

You can select to view the extensions by categories:

- *All*: All extensions are displayed.
- *Active*: All extensions in use are displayed.
- *Inactive*: All extensions not in use are displayed.
- *Disable*: All disabled extensions are displayed.

The extension statuses include:

- *Idle*: The extension is not in use.
- *In Use*: The extension is in use.
- *Busy*: The extension is busy.
- *Ringing*: The extension is ringing.
- *On Hold*: The extension has an on-hold call.
- *Other*: The status other than the above.

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

For more information, see [“Configuring Extensions” on page 79](#).

Viewing trunk status

Monitor > PBX Status > Trunks displays all the trunks in realtime, including their names, IPs, types, and statuses.

The trunk statuses include:

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

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

Registry/Connected indicates if a trunk has been registered with or connected to the service provider.

For more information, see [“Configuring Trunks” on page 90](#).

Viewing DHCP client list

When you connect a phone using DHCP to the FortiVoice unit, it registers with the FortiVoice DHCP server and obtains an IP address from the SIP server.

Monitor > PBX Status > DHCP displays all the phones using DHCP in realtime.

Figure 4: DHCP client list

Mac	Interface	IP	VCI	Expired	Factory	Extension	Configuration Status
00:30:4f:88:7f:fe	port1	172.20.190.152	udhcp 1.10.3	2012-08-17 13:02:22	fortiphone-planet	00304f887ffe	Not assigned
00:15:65:1b:1f:ce	port1	172.20.190.217	udhcp 1.9.1	2012-08-17 12:46:03	fortiphone-210	7580	Misconfigured
00:15:65:1f:20:cc	port1	172.20.190.140	udhcp 1.10.3	2012-08-17 12:23:20	fortiphone-210	0015651f20cc	Not assigned
00:30:4f:74:5d:bd	port1	172.20.190.188	voip	2012-08-17 11:12:15	fortiphone-planet	7517	Misconfigured
00:0b:82:0e:f8:9c	port1	172.20.190.203	GXP	2012-08-17 09:47:28	grandstream	7817	OK

Action

- *Assign to new extension*
Select a DHCP client in *Not assigned* status and click this option to add an extension and assign this client to the user at the same time. The information of the phone is automatically populated. For more information, see “[To assign a DHCP client to a new extension user](#)” on page 20.
- *Apply to existing extension*
Select a DHCP client in *Not assigned* status and click this option to assign this client to an existing user. For more information, see “[To assign a DHCP client to an existing extension user](#)” on page 20.
- *Edit the existing extension*
Select a DHCP client in *Conflicted* status and click this option to modify an existing extension which will override the extension in conflict. The conflict is caused by two extensions sharing the same IP address. For more information, see “[Configuration Status](#)” on page 20 and “[To override a DHCP client in conflict](#)” on page 20.

Export

Select to save the DHCP client list in `csv` format.

Mac

The Media Access Control address (MAC address) of the DHCP client.

Interface

The FortiVoice unit port to which the DHCP client connects. For information on FortiVoice interfaces, see “[Configuring network settings](#)” on page 27.

IP

The IP address of the DHCP client assigned by the FortiVoice DHCP server.

VCI

Vendor Class Identifier is used by the DHCP clients to identify their vendor type and configuration.

Expired

The expiration time of the DHCP client IP address.

Factory

The brand names of the DHCP clients.

Extension	The name of the extension if the DHCP client is associated with an extension user.
Configuration Status	<ul style="list-style-type: none"> • <i>OK</i>: The DHCP client is assigned to a new or an existing extension user. • <i>Not assigned</i>: The DHCP client is not assigned to a new or an existing extension user. This happens when an unmanaged phone is auto provisioned. For more information, see “Auto provisioning unmanaged SIP phones” on page 41. • <i>Conflicted</i>: There is another extension sharing the same IP address with the extension associated with this DHCP. This could happen when manually entering a MAC address for an extension.

To assign a DHCP client to a new extension user

1. Go to *Monitor > PBX Status > Trunks*.
2. Select a DHCP client in *Not assigned* status.
3. Collapse *Action* and select *Assign to new extension*.
4. Configure the extension associated with the DHCP client following [“Configuring IP extensions” on page 79](#).

To assign a DHCP client to an existing extension user

1. Go to *Monitor > PBX Status > Trunks*.
2. Select a DHCP client in *Not assigned* status.
3. Collapse *Action* and select *Assign to existing extension*.
4. Select the extensions to associate with the DHCP client.
5. Click *Apply to existing extension*.

To override a DHCP client in conflict

1. Go to *Monitor > PBX Status > Trunks*.
2. Select a DHCP client in *Conflicted* status.
3. Collapse *Action* and select *Edit existing extension*.
4. Modify the extension associated with this DHCP client to override the one in conflict. For more information, see [“Configuring IP extensions” on page 79](#).

Viewing call records

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

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 log messages

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

Logs stored remotely cannot be viewed from the web-based manager of the FortiVoice unit. If you want to view logs from the web-based manager, also enable local storage. For details, see [“Configuring Logs and Reports” on page 115](#).

Monitor > Log displays the logs of administrator activities and system events as well as voice.

To view the list of log files and their contents

1. Go to *Monitor > Log > Event/Voice*.

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.

2. To download an event 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 24](#).

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 5](#).

Figure 5: Log message view

The screenshot shows a log message view interface. At the top, there are filters for 'Level: Information', 'Sub type: All', and a 'Go to line:' field. Below the filters, there are navigation controls for 'Page 1 / 4', 'Records per page: 25', and a 'Save View' button. The main area displays a table of log messages with columns for '#', 'Date', 'Time', 'Subtype', and 'Message'. A blue box highlights a specific log message in the 'raw format' column, showing its details: Date=2012-05-29, Time=15:46:18, Subtype=admin, Message=User admin login successfully from SSH(172.20.110.135), Level=information, Log ID=0001002535. The 'columnar format' column shows the same message in a structured, key-value format.

#	Date	Time	Subtype	Message
1	2012-05-30	09:02:55	admin	GUI session failed to get cookie info from (172.20.120.36)
2	2012-05-29	15:53:33	admin	User admin logout from ssh(172.20.110.135).
3	2012-05-29	15:46:18	admin	User admin login successfully from SSH(172.20.110.135)
4			min	User admin login failed from SSH(172.20.110.135)
5			min	User admin login failed from SSH(172.20.110.135)
6			min	User admin login successfully from GUI(172.20.120.36)
7			min	GUI session failed to get cookie info from (172.20.120.36)
8			min	GUI session failed to get cookie info from (172.20.120.36)
9			min	User admin login successfully from GUI(172.20.120.36)
10			min	GUI session failed to start verify password from (172.20.120.36)
11			min	GUI session failed to get cookie info from (172.20.120.36)
12			min	User admin login successfully from GUI(172.20.120.36)

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 115](#).

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 24](#).

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

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

1. Click the column heading by which you want to sort.

The log messages are sorted in ascending order.

2. To sort in descending order, click the column heading again.

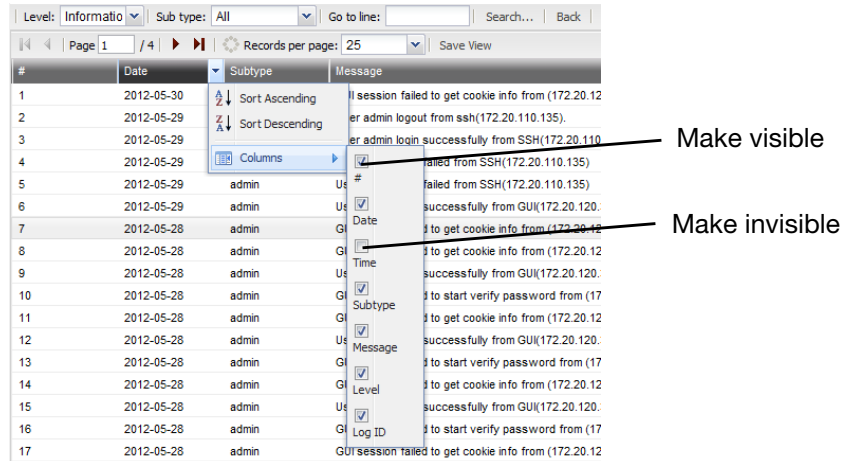
Depending on your currently selected theme:

- the column heading may darken in color to indicate which column is being used to sort the page
- a small upwards- or downwards-pointing arrow may appear in the column heading next to its name to indicate the current sort order.

To display or hide columns

1. Go to *Monitor > Log > Event/Voice*.
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 6: Hiding and showing log columns



4. Click *Save View*.

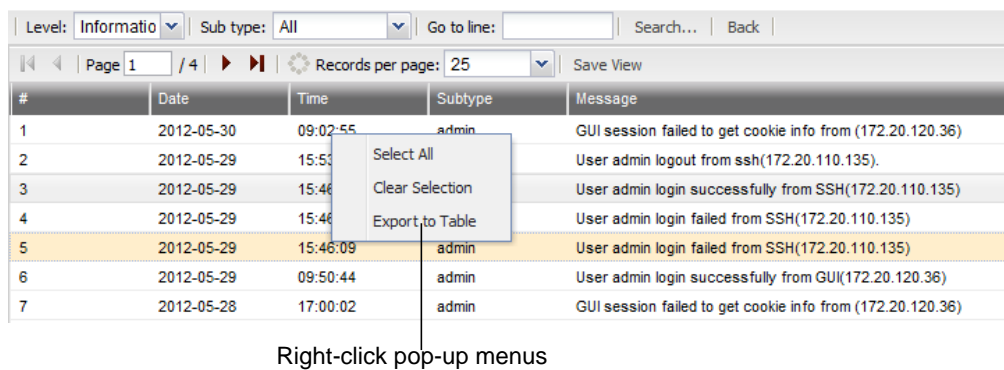
To change the order of the columns

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

Using the right-click pop-up menus

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

Figure 7: Using the right-click menus on log reports



Log report right-click menu options

Select All	Select to select all log messages in the current page, so that you can export all messages to a table.
Clear Selection	Select to deselect one or multiple log messages.
Export to Table	Select to export the selected log messages to a table format. A new tab named <i>Exported Table</i> appears, displaying the exported information. The table format allows you to copy the information and paste it elsewhere.

Searching log messages

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

To search log messages

1. Go to *Monitor > Log > Event/Voice*.
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 8: Log search dialog

FortiVoice
Event Log Search

Keyword:

Message:

Log ID:

Time: Zero day and 12 hour(s) before

05/30/12 10

Match condition: Contain

Apply Cancel

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

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

Time	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.
-------------	---

Match condition	<ul style="list-style-type: none"> • <i>Contain</i>: searches for the exact match. • <i>Wildcard</i>: supports wildcards in the entered search criteria.
------------------------	--

5. Click *Apply*.

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

Viewing generated reports

The *Report* tab displays the list of 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 reports](#)” on page 609.

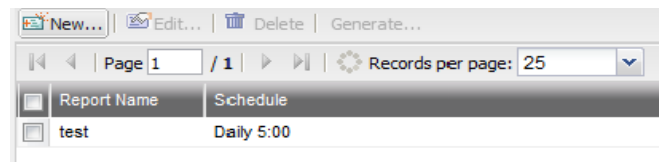


To reduce the amount of hard disk space consumed by reports, regularly download then delete generated reports from the FortiVoice unit.

To view and generate reports

1. Go to *Monitor > Report*.

Figure 9: Report tab



Download	Click to create a PDF or HTML version of the report.
-----------------	--

Report File Name	Lists the name of the generated report, and the date and time at which it was generated. For example, <i>Report 1-2012-03-31-2112</i> is a report named <i>Report 1</i> , generated on March 31, 2012 at 9:12 PM.
-------------------------	--

Last Access Time	Lists the date and time when the FortiVoice unit completed the generated report.
-------------------------	--

Size	Lists the file size of the report in HTML format, in bytes.
-------------	---

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

Playing recorded calls

The *Recorded Calls* tab lists the calls including conference calls recorded by the FortiVoice unit. You can listen to a call by selecting a call record and clicking the *Play* button. You can also save a record by selecting a call record and clicking the *Download* button.

To see the recorded call list, go to *Monitor > Recorded Calls*.

For information on recording calls, see “[Recording calls](#)” on page 113.

Configuring System Settings

The *System* menu lets you set up administrator accounts, and configure network settings, system time, SIP settings, system maintenance, and more.

This topic includes:

- [Configuring network settings](#)
- [Configuring voice](#)
- [Configuring system time, system options, email setting, and GUI appearance](#)
- [Configuring administrator accounts and access profiles](#)
- [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](#)

About IPv6 Support

IP version 6 (IPv6) handles issues that weren't 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 v2.0 release 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 8.

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 29.

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 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 > Interfaces* page. You cannot configure the interface anymore.

For information about adding redundant interfaces, see “[Configuring the network interfaces](#)” on page 29.

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 29.

Configuring the network interfaces

The *System > Network > Interfaces* 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 28, and “[Editing network interfaces](#)” on page 30.

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

Figure 1: Interface tab



Name	Type	IP/Netmask	IPv6/Netmask	Access	Status	
port1	Physical	172.20.120.165/24	:::0	HTTPS,PING,SSH	+	•
port2	Physical	192.168.2.99/24	:::0	HTTPS,PING,SSH	+	•
port3	Physical	255.255.255.255/32	:::0		+	•
port4	Physical	0.0.0.0/0	:::0		+	•
port5	Physical	0.0.0.0/0	:::0		+	•
port6	Physical	0.0.0.0/0	:::0		+	•

Table 1: Interface tab

Name	Displays the name of the network interface, such as <i>port1</i> .
Type	Displays the interface type: physical, VLAN, redundant, or loopback. For details, see “ About FortiVoice logical interfaces ” on page 28.
IP/Netmask	Displays the IP address and netmask of the network interface.
IPv6/Netmask	Displays the IPv6 address and netmask of the network interface. For more information about IPv6 support, see “ About IPv6 Support ” on page 27.
Access	Displays the administrative access and phone user access that are enabled on the network interface, such as HTTPS for the web-based manager.
Status	Indicates the up (available) or down (unavailable) administrative status for the network interface. <ul style="list-style-type: none">• <i>Green up arrow</i>: The network interface is up and can receive traffic.• <i>Red down arrow</i>: The network interface is down and cannot or receive traffic. To change the administrative status (that is, bring up or down a network interface), see “ Editing network interfaces ” on page 30.

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 51.

To create or edit a network interface

1. Go to *System > Network > Interfaces*.
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 2: Edit Interface dialog

Edit Interface

Interface name: port1 (00:25:90:3c:6d:cc)

Addressing Mode

Manual

IP/Netmask: 172.20.140.60 / 24

IPv6/Netmask: :: / 0

DHCP

Retrieve default gateway and DNS from server

Connect to server

Access

HTTPS PING HTTP

SSH SNMP TELNET

MTU

Override default MTU value (1500)

1500 (bytes)

Administrative status Up Down

OK Cancel

Table 2: Creating or editing a network interface

Interface Name	<p>If you are editing an existing interface, this field displays the name (such as port2) and media access control (MAC) address for this network interface.</p> <p>If you are creating a logical interface, enter a name for the interface.</p>
Type	<p>If you are creating a logical interface, select which type of interface you want to create. For information about logical interface types, see “About FortiVoice logical interfaces” on page 28.</p> <ul style="list-style-type: none">• <i>VLAN</i>: If you want to create a VLAN subinterface, select the interface for which you want to create the subinterface for. Then specify a VLAN ID. Valid VLAN ID numbers are from 1 to 4094, while 0 is used for high priority frames, and 4095 is reserved.• <i>Redundant</i>: If you want to create a redundant interface, select the interface members from the available interfaces. Usually, you need to include two or more interfaces as the redundant interface members.• <i>Loopback</i>: If you want to add a loopback interface, select the Loopback type and the interface name will be automatically reset to “loopback”. You can only add one loopback interface on FortiVoice.
Addressing Mode	<ul style="list-style-type: none">• <i>Manual</i>: Select to enter the IP address or IPv6 address and netmask for the network interface in <i>IP/Netmask</i> or <i>IPv6/Netmask</i>.• <i>DHCP</i>: Select to retrieve a dynamic IP address using DHCP.<ul style="list-style-type: none">• <i>Retrieve default gateway and DNS from server</i>: Enable to retrieve both the default gateway and DNS addresses from the DHCP server, replacing any manually configured values.• <i>Connect to server</i>: Enable for the FortiVoice unit to attempt to obtain DNS addressing information from the DHCP server. Disable this option if you are configuring the network interface offline, and do not want the unit to attempt to obtain addressing information at this time.

Access	<p>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.)</p> <ul style="list-style-type: none"> • <i>HTTPS</i>: Enable to allow secure HTTPS connections to the web-based manager and extension user account through this network interface. • <i>HTTP</i>: Enable to allow HTTP connections to the web-based manager, and extension user account through this network interface. <i>PING</i>: Enable to allow ICMP ECHO (ping) responses from this network interface. <i>SSH</i>: Enable to allow SSH connections to the CLI through this network interface. • <i>SNMP</i>: 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 29. • <i>TELNET</i>: 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 51.
MTU	<p><i>Override default MTU value (1500)</i>: Enable to change the maximum transmission unit (MTU) value, then enter the maximum packet or Ethernet frame size in bytes.</p> <p>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.</p> <p>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.</p>
Administrative status	<p>Select either:</p> <ul style="list-style-type: none"> • <i>Up</i>: Enable (that is, bring up) the network interface so that it can send and receive traffic. • <i>Down</i>: Disable (that is, bring down) the network interface so that it cannot send or receive traffic.

Configuring static routes

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

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

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

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

To determine which route a packet will be subject to, the FortiVoice unit compares the packet's destination IP address to those of the static routes and forward 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*.

Destination IP/Netmask	Gateway
0.0.0.0/0	172.20.140.2
172.20.140.0/24	172.20.190.2
172.20.110.0/24	172.20.190.2
192.168.110.0/24	192.168.110.5

Destination IP/Netmask	Displays the destination IP address and subnet of packets subject to the static route. A setting of 0.0.0.0/0.0.0.0 indicates that the route matches all destination IP addresses.
Gateway	Displays the IP address of the next-hop router to which packets subject to the static route will be forwarded.

2. Either click *New* to add a route or double-click a route to modify it.
A dialog appears.
3. In *Destination IP/netmask*, enter the destination IP address and netmask of packets that will be subject to this static route.
To create a default route that will match all packets, enter 0.0.0.0/0.0.0.0.
4. 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.
5. 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 hosts on the network connected to the interface. The host extensions must be configured to obtain their IP addresses using DHCP.

The FortiVoice unit can auto provision the SIP phones that it supports if the phones use the FortiVoice unit as the DHCP server, or if other existing DHCP server is used, then the DHCP server option 66 should be set to the FortiVoice unit. In case 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.

For more information about auto provisioning, see [“Configuring SIP phone auto-provisioning” on page 40](#).

To configure the DHCP server

1. Go to *System > Network > DHCP*.
2. Click *New*.

Figure 3: DHCP server configuration

The screenshot displays the DHCP server configuration interface, organized into several sections:

- Network Interface Setting:** Contains fields for ID (0), Status (checked), Interface (port1), Gateway (192.168.2.99), DNS options (Default), Primary DNS server (0.0.0.0), Secondary DNS server (0.0.0.0), Domain, and Netmask (255.255.255.0).
- Advanced Setting:** Contains fields for TFTP server (Opt66) (192.168.2.99), Conflicted IP timeout (Seconds) (604800), Device/Port type (Normal), Vender Class Identifier option (unchecked), and VCI string.
- DHCP IP Range:** A section with a toolbar (New..., Edit..., Delete) and a table with columns for Start and End.
- DHCP Excluded IP Range:** A section with a toolbar (New..., Edit..., Delete) and a table with columns for Start and End.
- Reserved IP Address:** A section with a toolbar (New..., Edit..., Delete) and a table with columns for IP and Mac.

At the bottom of the interface are 'Create' and 'Cancel' buttons.

Table 3: DHCP server configuration

ID	The system will generate an ID for this configuration. This is view only.
Status	Select to enable the DHCP server.
Interface	Select an interface from the drop-down list.
Gateway	Enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
DNS options	Select to use either a specific DNS server or the system's DNS settings. If you select a specific DNS server, enter the <i>Primary DNS server</i> and the <i>Secondary DNS server</i> fields. For more information, see “Configuring DNS” on page 35 .
Domain	Enter the domain that the DHCP server assigns to clients.
Netmask	Enter the netmask of the addresses that the DHCP server assigns.
Advanced Setting	<ul style="list-style-type: none">• <i>TFTP server (Opt66)</i>: The default TFTP server (192.168.2.99) is where the configuration profiles for some vendors' phone models are stored. This is also the IP address of the default gateway that the DHCP server assigns to DHCP clients. If you have your own TFTP server for such information, enter its IP address in this field. However, SIP phone auto provisioning will not work in this case. For more information, see “Configuring SIP phone auto-provisioning” on page 40.• <i>Conflicted IP timeout</i>: If an IP address assigned by the DHCP server to a client conflicts with the IP address of another client, the assigned IP address will be released after the timeout and a new IP address will be assigned.• <i>Vender Class Identifier option</i>: Select this option to apply the DHCP configuration to the phones of a specific vendor identified by the VCI string supplied by the vendor or by checking <i>Monitor > PBX Status > DHCP > VCI</i>.• <i>VCI string</i>: Enter the phone VCI string supplied by the vendor.
DHCP IP Range	Click <i>New</i> to enter the start and end for the range of IP addresses that this DHCP server assigns to DHCP clients.
DHCP Excluded IP Range	Click <i>New</i> to enter a range of IP addresses from the IP range that should not be assigned.
Reserved IP Address	Click <i>New</i> to enter an IP address from the DHCP server to match it to a specific client using its MAC address. In a typical situation, an IP address is assigned ad hoc to a client, and that assignment times out after a specific time of inactivity from the client, known as the lease time. To ensure a client always has the same IP address, that is, there is no lease time, use this option.

3. Click *Create*.

Configuring voice

The *System > Voice* submenu lets you configure the SIP setting, SIP phone auto provisioning, phone management, voicemail, and system capacity.

This topic includes:

- [Configuring SIP settings](#)
- [Configuring SIP phone auto-provisioning](#)
- [Managing phone configurations](#)
- [Configuring voicemail settings](#)
- [Configuring system capacity](#)

Configuring SIP settings

FortiVoice units support SIP communications.

The Session Initiation Protocol (SIP) is an IETF application layer signaling protocol used for establishing, conducting, and terminating multiuser multimedia sessions over TCP/IP networks using any media. SIP is often used for Voice over IP (VoIP) calls but can be used for establishing streaming communication between end points.

SIP employs a request and response transaction model similar to HTTP for communicating between endpoints. SIP sessions begin with a SIP client sending a SIP request message to another client to initiate a multimedia session. The other client responds with a SIP response message. Using these request and response messages, the clients engage in a SIP dialog to negotiate how to communicate and then start, maintain, and end the communication session.

SIP 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).

Devices involved in SIP communications are called SIP User Agents (UAs) (also sometimes called a User Element (UE)). UAs include User Agent Clients (UACs) that communicate with each other and User Agent Servers (UASs) that facilitate communication between UACs. For a VoIP application, an example of a UAC would be a SIP phone and an example of a UAS would be a SIP proxy server.

A SIP message contains headers that include client and server names and addresses required for the communication sessions. The body of a SIP message contains Session Description Protocol (SDP) statements that establish the media communication (port numbers, protocols and codecs) that the SIP UAs use. SIP VoIP most commonly uses the Real Time Protocol (RTP) and the Real Time Control Protocol (RTCP) for voice communication. Once the SIP dialog establishes the SIP call, the VoIP stream can run independently, although SIP messages can affect the VoIP stream by changing port numbers or addresses and by ending it.

Once SIP communication and media settings are established, the UAs communicate with each other using the established media settings. When the communication session is completed, one of the UAs ends the session by sending a final SIP request message and the other UA sends a SIP response message and both UAs end the SIP call and stop the media stream.

To configure SIP settings

1. Go *System > Voice > SIP Setting*.

Figure 4: SIP settings

SIP Setting

SIP server:

RTP timeout: (Seconds)

RTP hold timeout: (Seconds)

Re-register interval: (Minutes)

Transport Setting

Enable UDP UDP port:

Enable TCP TCP port:

Enable TLS TLS port:

TLS Client Setting

Server certificate verification

TLS protocol:

OK Cancel

2 Configure the following:

SIP Setting

- *SIP server*: Enter the current public IP address or public domain name of the SIP server.
- *RTP timeout*: Enter the amount of time in seconds during an active call that the extension will wait for RTP packets before hanging up the call. 0 means no time limit. The default is 60.
- *RTP hold timeout*: Enter the amount of time in seconds that the extension will wait on hold for RTP packets before hanging up the call. 0 means no time limit. The default is 300.
- *Re-register interval*: If this is a dynamic account with the VoIP provider, enter the registration interval as required by the VoIP provider. After each registration interval the FortiVoice unit renews the registration of the account with the VoIP provider.

Transport Setting

SIP 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).

Enable the ports as required.

TLS Client Setting

If you have enabled TLS, configure the following:

- *Server certificate verification*: Select this option for the TLS clients to confirm the validity of a server's credentials with a trusted root certification authority's (CA's) certificates. For information on uploading a CA certificate, see ["Managing certificate authority certificates"](#) on page 61.
- *TLS protocol*: Select the TLS protocol version.

3 Click **OK**.

Configuring SIP phone auto-provisioning

You can configure the FortiVoice unit to auto-provision SIP phones on your network. The SIP phones must support auto-provisioning using TFTP. The FortiVoice unit can auto provision the following SIP phones:

- Fortifone-110
- Fortifone-210
- Fortifone-350i/450i/550i
- Fortifone-video
- Cisco 7912s
- Grandstream

With auto-provisioning configured, when a supported SIP phone is connected to the network and powered on, it automatically receives all of its PBX setup information from the FortiVoice unit. In most cases the administrator does not have to make configuration changes to the SIP phone itself.

Auto provisioning managed SIP phones

When configuring phone extensions, you can create a managed phone by associating an extension number with a phone's type and MAC address. For more information, see "Configuring IP extensions" on page 79.

To auto provision a managed phone

1. 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 35.

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.

2. 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 35.
3. 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.
4. Make sure to select the *Auto provisioning* option in the class of service configuration added to the managed phone settings. For more information, see "Configuring class of services" on page 71 and "Configuring IP extensions" on page 79.
5. Connect the phone to the network and power it on.
6. Go to *System > Voice > Auto Provisioning*.
7. Select *Enabled* to enable SIP phone auto provisioning.
8. Click *OK*.

The phone will reboot and receive the PBX configuration from the FortiVoice unit.

Auto provisioning unmanaged SIP phones

If you have a large number of SIP phones and do not want to manually enter their MAC addresses and types on the FortiVoice unit, you can still auto provision the phones except that you need to assign extension numbers to the phones afterwards.



To auto provision an unmanaged phone, you must use the FortiVoice unit as your DHCP server. Otherwise the FortiVoice unit will not be able to get the phone's MAC address and generate a PBX configuration file for the phone accordingly.

Once you have configured the FortiVoice unit as your DHCP server, disable your own DHCP server to avoid any IP address conflicts.

To auto provision an unmanaged phone

1. 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 35.

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](#).

2. Use the FortiVoice unit as your DHCP server. For more information, see [“Configuring DHCP server”](#) on page 35.
3. Make sure to select the *Auto provisioning* option in the class of service configuration added to the managed phone settings. For more information, see [“Configuring class of services”](#) on page 71 and [“Configuring IP extensions”](#) on page 79.
4. Connect the phone to the network and power it on.
5. Go to *System > Voice > Auto Provisioning*.
6. Select *Enabled* to enable SIP phone auto provisioning.
7. Select *Generate configuration for unmanaged phone*.
8. Click *OK*.

The phone will reboot and receive the PBX configuration from the FortiVoice unit. The phone gets a temporary number which is its MAC address.

To assign an extension number to an unmanaged phone

1. Go to *Monitor > PBX Status > DHCP*.
2. In the *Extension* column, find the temporary extension number that matches the MAC address of the phone to which you want to assign an extension number.

Figure 5: DHCP client list

Mac	Interface	IP	VCI	Expired	Factory	Extension	Configuration Status
00:30:4f:88:7f:fe	port1	172.20.190.152	udhcp 1.10.3	2012-08-17 13:02:22	fortiphone-planet	00304f887ffe	Not assigned
00:15:65:1b:1f:ce	port1	172.20.190.217	udhcp 1.9.1	2012-08-17 12:46:03	fortiphone-210	7580	Misconfigured
00:15:65:1f:20:cc	port1	172.20.190.140	udhcp 1.10.3	2012-08-17 12:23:20	fortiphone-210	0015651f20cc	Not assigned
00:30:4f:74:5d:bd	port1	172.20.190.188	voip	2012-08-17 11:12:15	fortiphone-planet	7517	Misconfigured
00:0b:82:0e:f8:9c	port1	172.20.190.203	GXP	2012-08-17 09:47:28	grandstream	7817	OK

3. Right-click the temporary extension number.
4. Select *Assign to new extension* or *Apply to existing extension* to assign an extension to the phone. For more information, see [“Viewing DHCP client list”](#) on page 18.

Managing phone configurations

The FortiVoice unit provides the default configuration templates for the phone types it supports. 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 phone. Otherwise, phone auto provisioning will not be possible. This is because the template is part of the configuration file generated for the phone. For more information on auto provisioning, see “[Auto provisioning unmanaged SIP phones](#)” on page 41.

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 79.

To modify a configuration template

1. Go to *System > Voice > Phone Management*.
2. Select the phone type of which you want to modify the configuration template.
3. Click *Edit*.
4. In the pop-up window, click *Configuration Template*.
5. Make changes as required.
6. Click *Save*, or if you want to give up the changes, click *Reset to default*.

To manage phone firmware

1. Go to *System > Voice > Phone Management*.
2. Select the phone type of which you want to manage the firmware.
3. Click *Edit*.
4. In the pop-up window, click *Firmware*.
5. Remove, rename, or save an existing firmware, or upload a new firmware.

Configuring voicemail settings

The *System > Voice > Voicemail* tab lets you set voicemail greeting and message length.

To configure voicemail settings

1. Go to *System > Voice > Voicemail*.
2. Enter the maximum message and greeting length you want.
3. Click *OK*.

Configuring system capacity

The *System > Voice > System Capacity* tab lets you set the number of currently connected calls allowed on the FortiVoice unit.

To configure system capacity

1. Go to *System > Voice > System Capacity*.
2. Enter the outbound and inbound concurrent call limits you want.
3. Click *OK*.

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

The *System > Configuration* submenu lets you configure the virtual PBX, system time, system options, SIP setting, system capacity, email setting, auto provisioning, and GUI appearance.

This topic includes:

- Configuring the time and date
- Configuring system options
- Configuring email settings
- Customizing the GUI appearance

Configuring the time and date

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

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



For many features to work, including scheduling, logging, and certificate-dependent features, the FortiVoice system time must be accurate.

FortiVoice units support daylight savings time (DST), including recent changes in the USA, Canada and Western Australia.

To configure the system time

1. Go to *System > Configuration > Time*.

Figure 6: Time Settings tab

Time Settings

System time: 06/11/2012 11:30:27 Refresh

Time zone: (GMT-8:00)Pacific Time(US&Canada) v

Automatically adjust clock for daylight saving time changes

Set date 06/11/12 Time 11 30 27

Synchronize with NTP Server

Server: pool.ntp.org +

Sync Interval: 60 (minutes)

Apply Cancel

2. Configure the following:

Table 4: Configuring the date and time

System time	Displays the date and time according to the FortiVoice unit's clock at the time that this tab was loaded, or when you last selected the <i>Refresh</i> button.
Time zone	Select the time zone in which the FortiVoice unit is located. <ul style="list-style-type: none">• <i>Automatically adjust clock for daylight saving 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.
Set date	Select this option to manually set the date and time of the FortiVoice unit's clock, then select the <i>Year, Month, Day, Hour, Minute,</i> and <i>Second</i> fields before you click <i>Apply</i> . Alternatively, configure <i>Synchronize with NTP server</i> .
Synchronize with NTP Server	Select to use a network time protocol (NTP) server to automatically set the system date and time, then configure <i>Server</i> and <i>Syn Interval</i> . <ul style="list-style-type: none">• <i>Server</i>: Enter the IP address or domain name of an NTP server. You can add a maximum of 10 NTP servers. The FortiVoice unit uses the first NTP server based on the selection mechanism of the NTP protocol. Click the plus sign to add more servers. Click the minus sign to remove servers. Note that you cannot remove the last server. To find the NTP servers that you can use, see http://www.ntp.org.• <i>Sync Interval</i>: Enter how often in minutes the FortiVoice unit should synchronize its time with the NTP server. For example, entering 1440 causes the FortiVoice unit to synchronize its time once a day.

3. Click *Apply*.

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*.

Figure 7: Options tab

The screenshot shows a 'Configuration Options' dialog box. At the top, there is an 'Idle timeout' field set to '45' with a note '(1-480 minutes)'. Below this is a section titled 'Password Policy' with an expandable arrow. Inside this section, there is an 'Enable' checkbox which is unchecked. Below it, 'Minimum password length' is set to '8'. Under 'Password must contain:', there are four unchecked checkboxes: 'Uppercase letter', 'Lowercase letter', 'Number (0-9)', and 'Non alphanumeric character'. At the bottom of this section, 'Apply password policy to:' has three unchecked checkboxes: 'Administrators', 'Local mail users', and 'IBE users'. Below the Password Policy section is another section titled 'Administration Ports' with an expandable arrow. It contains four input fields: 'HTTP port number' (80), 'HTTPS port number' (443), 'SSH port number' (22), and 'TELNET port number' (23). At the bottom of the dialog are 'Apply' and 'Cancel' buttons.

2. Configure the following:

Table 5: Configuring system options

Idle timeout	Enter the amount of time that an administrator may be inactive before the FortiVoice unit automatically logs out the administrator. For better security, use a low idle timeout value.
Password Policy	Displays the password policy for administrators and extension users. <ul style="list-style-type: none">• <i>Enable</i>: Select to enable the password policy.• <i>Minimum password length</i>: Set the minimum acceptable length (8) for passwords.• <i>Password must contain</i>: Select any of the following special character types to require in a password. Each selected type must occur at least once in the password.<ul style="list-style-type: none">• <i>Uppercase letters</i> — A, B, C, ... Z• <i>Lowercase letters</i> — a, b, c, ... z• <i>Number</i> — 0 ... 9• <i>Non alphanumeric character</i> — punctuation marks, @, #, ... %• <i>Apply password policy to</i>: Select where to apply the password policy:<ul style="list-style-type: none">• <i>Administrators</i> — Apply to administrator passwords. If any password does not conform to the policy, require that administrator to change the password at the next login.• <i>Extension users</i> — Apply to FortiVoice extension users' passwords. If any password does not conform to the policy, require that user to change the password 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

3 Click *Apply*.

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.



For phone users to receive the notifications, you need to add their email addresses when configuring the extensions. See [“Configuring Extensions” on page 79](#).

To configure email settings

1. Go to *System > Configuration > Mail Server Settings*.

Figure 8: Mail server settings

The screenshot shows a 'Local Host Setting' dialog box with the following sections and fields:

- Local Host:**
 - Host name: FVC400C
 - Local domain name: (empty)
- Mail Queue:**
 - Maximum time for email in queue (1-240 hours): 24
 - Time interval for retry (10-120 minutes): 15
- Relay Server:**
 - Relay server name: (empty)
 - Relay server port: 25
 - Use SMTPs:
 - Authentication Required**
 - User name: (empty)
 - Password: (empty)
 - Authentication type: AUTO (dropdown menu)

Buttons: Apply, Cancel

2. Configure the following:

Table 6: Configuring email settings

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

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

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*.

Figure 9: Appearance tab

3. Configure the following to change appearance:

Administration Interface

Product name	Enter the name of the product. This name will precede <i>Administrator Login</i> in the title on the login page of the web-based manager.
Top logo	<p>Select <i>change</i> to upload a graphic that will appear at the top of all pages in the web-based manager. The image's dimensions must be 460 pixels wide by 36 pixels tall.</p> <p>For best results, use an image with a transparent background. Non-transparent backgrounds will not blend with the underlying theme graphic, resulting in a visible rectangle around your logo graphic.</p> <p>Note: Uploading a graphic overwrites the current graphic. The FortiVoice unit does not retain previous or default graphics. If you want to revert to the current graphic, use your web browser to save a backup copy of the image to your management computer, enabling you to upload it again at a later time.</p>
Default language	<p>Select the default language for the display of the web-based manager.</p> <p>You can configure a separate language preference for each administrator account. For details, see “Configuring administrator accounts” on page 51.</p>

Voicemail interface

Voicemail login	Enter a word or phrase that will appear on top of the voicemail login page, such as Voicemail Login.
------------------------	--

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

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

Configuring administrator accounts and access profiles

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

This topic includes:

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

Configuring administrator accounts

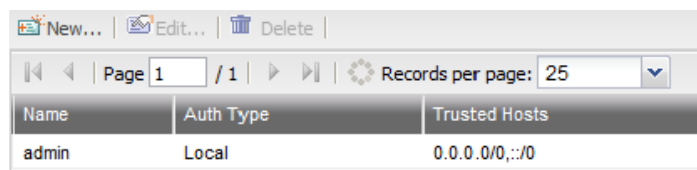
The *Administrator* tab displays a list of the FortiVoice unit's administrator accounts and the trusted host IP addresses administrators use to log in (if configured).

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

To view and configure administrator accounts

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

Figure 10:Administrator tab



Name	Auth Type	Trusted Hosts
admin	Local	0.0.0.0/0,::/0

Table 7: Viewing the list of administrator accounts

Name	Displays the name of the administrator account.
Auth Type	Displays the local or remote type of authentication that the administrator can use.
Trusted Hosts	Displays the IP address and netmask from which the administrator can log in.

2. Either click *New* to add an account or double-click an account to modify it. A dialog appears.

Figure 11: New Administrator dialog

The screenshot shows the 'New Administrator' dialog box. It includes the following fields and controls:

- Administrator:** A text input field.
- Create password** (with a dropdown arrow)
- Password:** A text input field.
- Confirm password:** A text input field.
- Trusted hosts:** Two rows of IP/netmask inputs. The first row shows '0.0.0.0 / 0' and the second row shows ':: / 0'. There are expand/collapse icons to the right of each row.
- Access profile:** A dropdown menu currently showing 'super_admin_prof', with 'New...' and 'Edit...' buttons to its right.
- Language:** A dropdown menu currently showing 'English'.
- Theme:** A dropdown menu currently showing 'Red Grey', with a 'Use Current' button to its right.
- Create** and **Cancel** buttons at the bottom left.

3. Configure the following:

Table 8: Configuring an administrator account

Administrator	<p>Enter the name for this administrator account.</p> <p>The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), hyphens (-), and underscores (_). Other special characters and spaces are not allowed.</p>
Create password	<ul style="list-style-type: none">• <i>Password:</i> Enter this account's password. The password can contain any character except spaces. This field does not appear if <i>Auth Type</i> is not <i>Local</i> or <i>RADIUS+Local</i>. Caution: Do not enter a FortiVoice administrator password less than six characters long. For better security, enter a longer password with a complex combination of characters and numbers, and change the password regularly. Failure to provide a strong password could compromise the security of your FortiVoice unit.• <i>Confirm password:</i> Enter this account's password again to confirm it. This field does not appear if <i>Auth Type</i> is not <i>Local</i> or <i>RADIUS+Local</i>.
Trusted Hosts	<p>Enter an IPv4 or IPv6 address or subnet from which this administrator can log in.</p> <p>If you want the administrator to access the FortiVoice unit from any IP address, use 0 . 0 . 0 . 0 / 0 . 0 . 0 . 0 .</p> <p>Enter the IP address and netmask in dotted decimal format. For example, you might permit the administrator to log in to the FortiVoice unit from your private network by typing 192 . 168 . 1 . 0 / 255 . 255 . 255 . 0 .</p> <p>Note: For additional security, restrict all trusted host entries to administrative hosts on your trusted private network. For example, if your FortiVoice administrators log in only from the 10.10.10.10/24 subnet, to prevent possibly fraudulent login attempts from unauthorized locations, you could configure that subnet in the <i>Trusted Host #1</i>, <i>Trusted Host #2</i>, and <i>Trusted Host #3</i> fields.</p> <p>Note: For information on restricting administrative access protocols that can be used by these hosts, see “Editing network interfaces” on page 30.</p> <p>Click the + sign to add additional IP addresses or subnets from which the administrator can log in.</p>
Access profile	<p>Select the name of an access profile that determines which functional areas the administrator account may view or affect.</p> <p>Click <i>New</i> to create a new profile or <i>Edit</i> to modify the selected profile. For details, see “Configuring access profiles” on page 54.</p>

Language	Select this administrator account's preference for the display language of the web-based manager.
Theme	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 access profiles

The *Access Profile* tab displays a list of access profiles.

Access 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 accounts

1. Go to *System > Administrator > Access Profile*.
2. Either click *New* to add an account or double-click an access profile to modify it. A dialog appears.

Figure 12:Access Profile dialog

Access Control	None	Read Only	Read-Write
--Select All--	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
monitor	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Others	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. In *Profile Name*, enter the name for this access profile.
4. In the *Access Control* 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*.

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 9: Certificate types

Certificate type	Usage
CA certificates	The FortiVoice unit uses CA certificates to authenticate the PKI users, including administrators and phone users. For details, see “Managing certificate authority certificates” on page 61.
Server certificates	The FortiVoice unit must present its local server certificate for the following secure connections: <ul style="list-style-type: none"> the web-based manager (HTTPS connections only) phone user web interface (HTTPS connections only) For details, see “Managing local certificates” on page 55.
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 13: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

Table 10:Managing local certificates

View	Select a certificate and click <i>View</i> to display its issuer, subject, and range of dates within which the certificate is valid.
Generate	Click to generate a local certificate request. For more information, see “Generating a certificate signing request” on page 56 .
Download	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">• <i>Download</i>: Download a certificate (.cer) or certificate request (.csr) file. You can send the request to your certificate authority (CA) to obtain a signed certificate for the FortiVoice unit. For more information, see “Downloading a certificate signing request” on page 59.• <i>Download PKCS12 File</i>: Download a PKCS #12 (.p12) file. For details, see “Downloading a PKCS #12 certificate” on page 61.
Set status	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.”
Import	Click to import a signed certificate for local use. For more information, see “Importing a certificate” on page 60 .

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 60](#).
- 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 56](#).

To generate a certificate request

1. Go to *System > Certificate > Local Certificate*.

2. Click *Generate*.
A dialog appears.
3. Configure the following:

Figure 14: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:

Table 11: Generating a certificate signing request

Certification name	Enter a unique name for the certificate request, such as <code>fvlocal</code> .
---------------------------	---

Subject Information	<p>Information that the certificate is required to contain in order to uniquely identify the FortiVoice unit.</p> <ul style="list-style-type: none">• <i>ID type</i>: select the type of identifier to be used in the certificate to identify the FortiVoice unit:<ul style="list-style-type: none">• Host IP• Domain name• E-mail<p>Which type you should select varies by whether or not your FortiVoice unit has a static IP address, a fully-qualified domain name (FQDN), and by the primary intended use of the certificate.</p><p>For example, if your FortiVoice unit has both a static IP address and a domain name, but you will primarily use the local certificate for HTTPS connections to the web-based manager by the domain name of the FortiVoice unit, you might prefer to generate a certificate based on the domain name of the FortiVoice unit, rather than its IP address.</p><ul style="list-style-type: none">• <i>Host IP</i> requires that the FortiVoice unit have a static, public IP address. It may be preferable if clients will be accessing the FortiVoice unit primarily by its IP address.• <i>Domain name</i> requires that the FortiVoice unit have a fully-qualified domain name (FQDN). It may be preferable if clients will be accessing the FortiVoice unit primarily by its domain name.• <i>E-mail</i> does not require either a static IP address or a domain name. It may be preferable if the FortiVoice unit does not have a domain name or public IP address.• <i>IP</i>: Enter the static IP address of the FortiVoice unit.<p>This option appears only if <i>ID type</i> is <i>Host IP</i>.</p>• <i>Domain name</i>: Type the fully-qualified domain name (FQDN) of the FortiVoice unit.<p>The domain name may resolve to either a static or, if the FortiVoice unit is configured to use a dynamic DNS service, a dynamic IP address. For more information, see “Configuring the network interfaces” on page 29 and “Configuring DNS” on page 35.</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>• <i>E-mail</i>: Type the email address of the owner of the FortiVoice unit.<p>This option appears only if <i>ID type</i> is <i>E-mail</i>.</p>
----------------------------	--

Optional Information	<p>Information that you may include in the certificate, but which is not required.</p> <ul style="list-style-type: none"> • <i>Organization unit</i>: Type the name of your organizational unit, such as the name of your department. (Optional) To enter more than one organizational unit name, click the + icon, and enter each organizational unit separately in each field. • <i>Organization</i>: Type the legal name of your organization. (Optional) • <i>Locality(City)</i>: Type the name of the city or town where the FortiVoice unit is located. (Optional) • <i>State/Province</i>: Type the name of the state or province where the FortiVoice unit is located. (Optional) • <i>Country</i>: Select the name of the country where the FortiVoice unit is located. (Optional) • <i>E-mail</i>: Type an email address that may be used for contact purposes. (Optional)
Key type	<p>Displays the type of algorithm used to generate the key.</p> <p>This option cannot be changed, but appears in order to indicate that only RSA is currently supported.</p>
Key size	<p>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.</p>

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 59.

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 56.

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 have 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 56.

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 60](#).

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 56](#).

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 56.
 - *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 60.

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.

Backup and restore

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 backup system configuration or user configuration. System configuration includes the configurations that make the FortiVoice unit work. User configuration includes phone user voicemails and call data recordings in addition to system configuration.

To back up the configuration file

1. Go to *System > Maintenance > Configuration*.
2. In the *Backup Configuration* area, select *System configuration* or *User configuration*.
If you choose to backup user configuration and the user configuration files are not updated, select the files to be updated and click *Update* 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 91](#).

Restoring the configuration

In the *Restore Configuration* area under *System > Maintenance > Configuration*, you can restore the backup FortiVoice configuration from your local PC.

Restoring the firmware

In the *Restore Firmware* area under *System > Maintenance > Configuration*, you can install a FortiVoice firmware from your local PC.

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 PBX

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

This topic includes:

- Configuring PBX settings
- Configuring class of services
- Configuring account codes
- Working with SIP profiles and caller IDs

Configuring PBX settings

PBX > Setting lets you configure a PBX's location, number management, schedule, and much more.



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

This topic includes:

- Setting PBX location and contact information
- Configuring PBX options
- Configuring number settings
- Mapping speed dials
- Scheduling the FortiVoice unit
- Customizing notification email templates
- Managing sound files
- Managing music on hold

Setting PBX location and contact information

Identify the PBX location and its number.

To set PBX location

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

Country	Select the country name.
Emergency number	Click the default number (911) to enter the emergency call number of the selected country.
Long-distance prefix	Click the default number (1) to enter the prefix for dialing long distance calls.

International prefix	Click the default number (011) to enter the prefix for dialing international calls.
Outside line prefix	Click the default number (9) to enter the prefix for making outbound calls.
Area code	Click <i>Click to edit</i> to enter the <i>Area code</i> for the main number of the PBX. This code is provided by your phone company or ISP.
Area code is required when dialing local numbers	Select this option if the area code needs to be dialed for local numbers.
System Main caller ID	Enter the <i>Main number</i> of the PBX. This number is provided by your phone company or ISP.
Default prompt language	Select a new default prompt language for the PBX. The default is English. This setting affects all of the PBX'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.

3. Optionally, enter your *Contact Information*.
4. Click *OK*.

Configuring PBX options

Configure the default FortiVoice system settings.

To configure PBX options

1. Go to *PBX > Setting > Options*.
2. For *Default SIP user password*, enter a password for the PBX. The password is used to log into the PBX user web portal. 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.
3. For *Ring duration*, enter the time in seconds for the PBX to ring before it responds to a call.
4. Click *OK*.

Configuring number settings

The *PBX > Setting > Number Management* tab lets you configure the pattern and number of digits you want the FortiVoice unit to use for phone numbers, speed dials, and prefixes.

The FortiVoice unit support the following pattern-matching syntax:

Table 1: Pattern-matching syntax

Syntax	Description
X	Matches any single digit from 0 to 9.
Z	Matches any single digit from 1 to 9.

Table 1: Pattern-matching syntax

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

Table 2: Pattern-matching examples

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

To configure number settings

1. Go to *PBX > Setting > Number Management*.
2. Enter the extension *Number pattern*. For example, NXXX is any four digit number as long as the first digit is 2 or higher and 7XXX is a four digit number that always starts with 7. This pattern will be followed when creating extensions. See [“Configuring IP extensions” on page 79](#).
3. Enter the *Speed dial pattern*. For example, *3XX is any three digit number that starts with 3. This pattern will be followed when configuring speed dials. See [“Mapping speed dials” on page 66](#).
4. In the *System prohibited prefix* field, enter the phone number prefix that you want to ban, such as 900. Click the + sign to add up to 10.
5. In the *System unrestricted prefix* field, enter the allowed phone number prefix, such as 800. Click the + sign to add up to 10.
6. Enter the *Operator extension* of the PBX.
7. Enter the *Supporting extension* for technical support of the PBX.
8. Click **OK**.

Mapping speed dials

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

For information on setting speed dial pattern, see “Configuring number settings” on page 65.

To map speed dials

1. Go to *PBX > Setting > Speed Dial*.
2. Enter a name for the speed dial mapping.
3. For *Code*, enter the number based on the speed dial pattern you set. For example, 333.
4. Enter the phone *Number* to map to the speed dial code. For example, 222-1234.
5. Optionally, enter a note for the mapping, such as “This is for customer A”.
6. Click *Create*.

Scheduling the FortiVoice unit

You can schedule the FortiVoice operation time and use the schedules when configuring dial plans. There are three default schedules, namely *after_hour*, *any_time*, and *business_hour*. You can modify the default schedules, but cannot delete them.

For information on dial plan, see “Configuring Dial Plans” on page 95.

To schedule the operation time

1. Go to *PBX > Setting > Schedule* and click *New*.

Figure 1: PBX scheduling

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

Holiday

New... | Edit... | Delete

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

Create Cancel

2. Configure the following:

Table 3: PBX scheduling

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

3. Click *Create*.

Customizing notification email templates

Go to *PBX > Setting > Custom Message* to view and reword the default notification email templates.

The FortiVoice unit sends out notification email when you have a new voicemail in your mailbox or missed a call. You can customize the email templates for the email notifications.

You can change the content of the email template by editing the text and HTML codes and by working with email template variables. For descriptions of the default email template variables, see "Default email template variables" on page 69.

To customize email templates

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

8. Click *OK*, or click *Reset To Default* to revert the replacement message to its default text.

Table 4: Default email template variables

Variable	Description
%%CONTENT%%	The notification message content.
%%ENVELOP_FROM%%	The mail sender's address. This is the address for bounce messages.
%%NOTIFY_FROM%%	The email address, such as <code>notify@example.com</code> , used to send notifications.
%%SUBJECT%%	The subject of the notification.
%%DATE%%	The date and time when the notification is sent.
%%NOTIFY_TO%%	The email address of the notification receiver in the header of the notification.
%%MISSED_CALLERID%%	The phone number of the caller whose call was missed.
%%MISSED_DATE%%	The date and time when a call was missed.

Creating variables

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

To create a new variable

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

4. Configure the following:

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

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

5. Click OK.

Table 5: Default replacement message variables

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

Managing sound files

The *PBX > Setting > Sound File* tab lets you upload, record, and play phone sound files such as voicemail greetings. These files can be used when configuring music on hold, conference calls, and auto attendants. See [“Managing music on hold” on page 71](#) and [“Configuring Phone Services” on page 105](#).

To manage a sound file

1. Go to *PBX > Setting > Sound File*.
2. Click *New*.
3. Enter a name for the file.
4. Optionally, enter a description for the file.
5. Click *Upload* to get an existing sound file, *Record* to make a sound file (with a microphone), and *Play* to listen to a uploaded or recorded file (with speakers or earphones) for the language you select.
6. Click *OK*.

Managing music on hold

The *PBX > Setting > Music On Hold* tab lets you choose the sound files to play while a call is on hold. For information on sound files, see “Managing sound files” on page 70.

To choose sound files

1. Go to *PBX > Setting > Music On Hold*.
2. Click *New*.
3. Enter a name for the configuration.
4. Select the *Available* sound files and click *->* to move them into the *Selected* field. You can use the *Up* and *Down* buttons to reorder the fiels.
5. For *Mode*, if you want to play the sound files randomly, select *Random*. If you want to play the files according to the order in the *Selected* field, select *Sequential*.
6. Optionally, enter a description for the file.
7. Click *Create*.

Configuring class of services

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

There is a default class of service configuration that can be edited but not be deleted.

For information on extensions, see “Configuring Extensions” on page 79.

To configure a class of service

1. Go to *PBX > Class of Service > Class of Service* and click *New*.

Figure 2: Class of service configuration

The screenshot shows the 'Class of Service' configuration window. At the top, there is a 'Name:' text box. Below it is a section titled 'Basic settings' with a list of options, each with a checked checkbox: Auto provisioning, Call waiting, Call queue, Follow me, Feature codes, List in directory, Call transfer, Call forwarding, Call park, Do not disturb, and Dial local extension. The next section is 'Voice Mail' with 'Enabled' checked, 'Maximum messages' set to 1000, and 'Voicemail retention days' set to 60. There are three collapsed sections: 'Call Restriction', 'Monitor/Recording', and 'Advanced'. At the bottom are 'Create' and 'Cancel' buttons.

2. Configure the following:

Table 6: Class of service configuration

Name	Enter a name for this class of service.
Basic settings	
Auto provisioning	Select to enable auto provisioning for the extension. For more information, see “Configuring SIP phone auto-provisioning” on page 40.
Call waiting	Select to enable the FortiVoice unit to sound a tone if an incoming call reaches a busy line.
Call queue	Select to enable placing multiple callers on hold at your extension while you are on an existing call.
Follow me	Select to enable ringing all the numbers provided to the FortiVoice unit when a call comes in. These numbers are where you can be reached.
Feature codes	Select to enable using feature codes, such as dialing *79 to turn Do Not Disturb off.
List in directory	Select to put the user’s name in the dial-by-name directory which allows a caller to find a user’s extension number, and connect to their local extension or remote extension. This way the caller can reach their party without speaking to the receptionist.
Call transfer	Select to enable transferring an ongoing phone call to another extension.
Call forwarding	Select to enable forwarding incoming calls to another phone number.
Call park	Select to enable putting a call on hold and then retrieving it from another extension.
Do not disturb	Select to enable playing a DND message instead of phone ringing when a call comes in.
Dial local extension	Select to enabling calling local extensions.
Voice Mail	
Enabled	Select to enable the voicemail service.
Maximum messages	Enter the number of voice mails allowed.
Voicemail retention days	Enter the number of days to keep the voicemails.
Call Restriction	
Allow long distance call	Select to allow long distance direct dialing. If required, select the account code that needs to be dialed before making a long distance call. For information on account code, see “Configuring account codes” on page 74.

Allow international call	<p>Select to allow international direct dialing. If required, select the account code that needs to be dialed before making a long distance call. For information on account code, see “Configuring account codes” on page 74.</p> <p>There are phone numbers with certain calling services and likely higher calling rates such as 900 number in North America and 0990-5 number in Japan. These numbers do not belong to international calls or long distance calls and can be banned on a system-wide basis (see “Configuring number settings” on page 65). However, if you want to allow calling some of these numbers, click <i>New</i> and configure the following:</p> <ol style="list-style-type: none"> 1. Enter a name for this setting. 2. Select <i>Enabled</i> to activate this exemption. 3. Enter the area code/prefix of the number to be called, such as 900. 4. Select the account code that needs to be dialed before making a call with this prefix. For information on account code, see “Configuring account codes” on page 74. 5. Click Create.
Monitor/Recording	<p>Configure monitoring and recording outgoing and incoming calls of an extension to which this class of service is applied.</p>
Call barge	<p>Select to enable the supervisor to join an ongoing call for monitoring purpose.</p>
Personal recording	<p>Select to allow users to configure personal recording of their incoming and outgoing calls on the user web interface.</p>
Advanced	
Conference number	<p>Select the permission for conference calls:</p> <ul style="list-style-type: none"> • <i>Allow all</i>: Select to allow all extensions to join conference calls. • <i>Disallow all</i>: Select to prohibit all extensions to join conference calls. • <i>Allow all with exempt</i>: If you select this option, click <i>New</i> to enter the number(s) banned for joining conference calls. • <i>Disallow all with exempt</i>: If you select this option, click <i>New</i> to enter the number(s) allowed for joining conference calls. <p>For more information, see “Configuring auto attendants” on page 105.</p>

Paging number	<p>Select the permission for paging:</p> <ul style="list-style-type: none"> • <i>Allow all</i>: Select to allow all paging numbers to page. • <i>Disallow all</i>: Select to prohibit all paging numbers to page. • <i>Allow all with exempt</i>: If you select this option, click <i>New</i> to enter the number(s) disallowed to page. • <i>Disallow all with exempt</i>: If you select this option, click <i>New</i> to enter the number(s) allowed to page. <p>For more information on paging, see “Configuring auto attendants” on page 105.</p>
Trusted hosts	<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>
Permit outgoing rules	<p>Select the available outbound calling rules in the <i>Available rules</i> field and click <i>-></i> to move them to the <i>Selected rules</i> field. You can apply the rules to a user later. For more information on calling rules, see “Configuring outbound dial plans” on page 95.</p>

6. 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 class of services. For information on class of service, see [“Configuring class of services” on page 71](#).

To set an account code

1. Go to *PBX > Class of Service > Account Code*
2. Click *New*.
3. Enter a name for the account code.
4. Enter the access code, such as 69.
5. Click *Create*.

Working with SIP profiles and caller IDs

The *PBX > Profile* tab lets you create SIP profiles for configuring extensions and SIP trunks. It also lets you to modify caller IDs.

This topic includes:

- [Configuring SIP profiles](#)
- [Modifying caller IDs](#)

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 service provider. For example, if some of your features and Codecs are not supported by your service provider, they will not work even if they are enabled or selected in the SIP profile.

There is a default SIP profile that can be edited but not be deleted.

For information on extensions, see “Configuring Extensions” on page 79.

For information on SIP trunks, see “Configuring Trunks” on page 90.

To configure a SIP profile

1. Go to *PBX > Profile > SIP Profile* and click *New*.

Figure 3: SIP profile

SIP Profile	
Name:	<input type="text"/>
DTMF:	Auto <input type="button" value="v"/>
<input type="checkbox"/> NAT	
<input type="checkbox"/> Video	
<input type="checkbox"/> Direct media stream	

Transport	
<input checked="" type="checkbox"/> UDP	
<input type="checkbox"/> TCP	
<input checked="" type="checkbox"/> TLS	

Codec	
Supported	Preferred
<input checked="" type="checkbox"/> G711u	<input checked="" type="radio"/>
<input checked="" type="checkbox"/> G711a	<input type="radio"/>
<input checked="" type="checkbox"/> G729	<input type="radio"/>
<input checked="" type="checkbox"/> G722	<input type="radio"/>
<input checked="" type="checkbox"/> G723.1	<input type="radio"/>
<input checked="" type="checkbox"/> G726	<input type="radio"/>
<input checked="" type="checkbox"/> GSM	<input type="radio"/>

2. Configure the following:

Table 7: SIP profile

SIP Profile	<ul style="list-style-type: none">• <i>Name</i>: Enter a name for this profile.• <i>DTMF</i>: Select the DTMF method used by the VoIP provider. Options are RFC2833, Inband, Info, Shortinfo, and Auto. Auto means the VoIP provider's server and the FortiVoice unit will negotiate to select a DTMF method. You could also select a specific DTMF method if required.• <i>NAT</i>: Select if the service provider supports SIP NAT translation.• <i>Direct media stream</i>: Select if the service provider supports direct media transfer to extensions by bypassing the PBX in between.
Transport	<p>SIP 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 protocols as required.</p> <p>This option, if applied to a user, overrides the system-wide transport settings. For more information, see “Configuring SIP settings” on page 38.</p>
Codec	<p>Select the Codecs supported by the service provider. Among the selected ones, choose the preferred one for the VoIP provider. The preferred Codec is usually the most used one in your area and provides the best quality of communication.</p> <p>If your preferred Codec is different from that of your service provider, the service provider's Codec will be used as long as it is one of your supported Codecs.</p>

3. Click *Create*.

Modifying caller IDs

You can change the phone number, caller's name, or both that will appear on the other phone when the local extension is used to make a VoIP call.

Caller ID modifications are used when configuring outbound dial plans. For more information, see [“Configuring outbound dial plans” on page 95](#).

To modify a caller ID

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

Figure 4: Caller ID modification

3. Configure the following:

Name	Enter the name for this caller ID modification record.
Match number	Enter the extension number or number pattern you want to modify. For example, you can enter 8134 to modify a single extension, or 81xx to modify all the four-digit numbers starting with 81.
Number Modification	<p>If you have entered a <i>Match number</i>, configure the following values to modify it:</p> <ul style="list-style-type: none"> • <i>Strip</i>: Enter a number to hide the starting part of an extension from displaying. 0 means no action. For example, if your <i>Match number</i> is 8134 and <i>Strip</i> is 2, only 34 will be displayed as caller ID. • <i>Truncate</i>: Enter a number to hide the ending part of an extension from displaying. 0 means no action. For example, if your <i>Match number</i> is 8134 and <i>Truncate</i> is 2, only 81 will be displayed as caller ID. • <i>Prefix</i>: Add a number before an extension. For example, if your <i>Match number</i> is 8134 and <i>Prefix</i> is 5, the caller ID will be 58134. • <i>Postfix</i>: Add a number after an extension. For example, if your <i>Match number</i> is 8134 and <i>Postfix</i> is 5, the caller ID will be 81345.
Match caller ID name	Enter the caller ID that you want to map to another one. Caller IDs are created when configuring SIP extensions. See “Configuring IP extensions” on page 79 .
Map to new caller ID name	Enter the new caller ID name to which you want to map the one entered in the <i>Match caller ID name</i> field.

4. 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 ten extensions (8100-8110), instead of displaying each extension when making calls, you can display a caller ID name “Support” for the whole team.

To map a group of extensions to a caller ID name

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

Configuring Extensions

The *Extension* menu lets you configure local and remote extensions, ring groups, extension paging, and extension groups.

This topic includes:

- Setting up local extensions
- Creating extension groups

Setting up local extensions

You can configure IP phone extensions and choose extension preferences.

This topic includes:

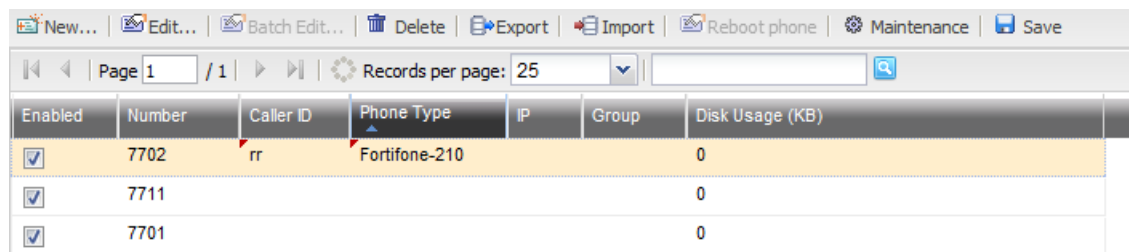
- Configuring IP extensions
- Setting up remote extensions
- Setting extension user preferences

Configuring IP extensions

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

To view the local IP extensions, go to *Extension > User > SIP*.

Figure 1: IP extensions



Enabled	Number	Caller ID	Phone Type	IP	Group	Disk Usage (KB)
<input checked="" type="checkbox"/>	7702	rr	Fortifone-210			0
<input checked="" type="checkbox"/>	7711					0
<input checked="" type="checkbox"/>	7701					0

Table 1: IP extensions

Batch Edit	If you want to apply the same changes to multiple extensions, select the extensions and click this option. Make the changes and click <i>Apply To All</i> .
Export	Select to save a copy of the extension list in CSV format.
Import	Select to upload a copy of the extension list in CSV format. For details, see “Importing a list of extensions” on page 83 .
Reboot phone	<p>If you have edited an extension configuration and want to apply it to the extension phone, select the extension and click this option.</p> <p>The selected phones will reboot and only the phones that meet the following conditions will receive the new configuration:</p> <ul style="list-style-type: none">• Phones supported by and registered to the FortiVoice unit. For the list of supported phones and auto provisioning prerequisites, see “Configuring SIP phone auto-provisioning” on page 40.• Phones types and MAC addresses are correctly configured. See “To create or edit an IP extension” on page 80.• Auto-provisioning is enabled for the phone through the class of service applied to it. See “Configuring class of services” on page 71.
Maintenance	<p>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.</p> <p>Click <i>Back</i> to return to the <i>SIP</i> tab.</p>
Save	Click an extension’s <i>Caller ID</i> or <i>Phone Type</i> to modify them and click this button to save the changes.
Enabled	Select to activate an extension.
Number	The extension number.
Caller ID	The name displaying on the extension. This is usually the name of the extension user.
Phone Type	The type of phone for this extension.
IP	The link to the IP address of the phone using the extension number. See “IP” on page 83 .
Group	<p>The link to the extension group of which this extension is a member. An extension can be used in multiple groups.</p> <p>An extension used in an extension group cannot be deleted.</p> <p>For information on extension group, see “Creating user groups” on page 87.</p>
Disk Usage (KB)	Displays the size of disk space used by voicemails for the user in kilobytes (KB).

To create or edit an IP extension

1. Go to *Extension > User > SIP*.
2. Click *New* or double-click an existing extension.

Figure 2: IP extension configuration

The screenshot displays a configuration window titled "Extension Setting". It contains the following fields and controls:

- Number:** An empty text input field.
- Enabled:** A checked checkbox.
- Caller ID:** An empty text input field.
- SIP password:** A text input field containing "voice#321".
- Voicemail PIN:** A text input field containing "123123".
- Prompt language:** A dropdown menu set to "English".

Below these fields is an expandable section titled "Advanced Setting" (indicated by a small upward-pointing triangle). This section contains:

- SIP setting:** A dropdown menu set to "--None--", with "Edit..." and "New..." buttons to its right.
- Class of service:** A dropdown menu set to "--None--", with "Edit..." and "New..." buttons to its right.
- Phone type:** A dropdown menu.
- MAC address:** An empty text input field.

At the bottom of the window are two buttons: "Create" and "Cancel".

3. Configure the following:

Table 2: IP extension configuration

Extension Setting	
User ID	This is the system-generated ID based on the extension number. This option is only available when you edit an extension and is view only.
Number	Enter the extension number following the extension number pattern. See “Configuring number settings” on page 65.
Enabled	Select to activate the extension.
Caller ID	Enter the name displaying on the extension. This is usually the name of the extension user.
SIP password	Enter the password used for configuring your SIP phone from the phone or the Web. You need the phone's IP to access it from the Web.
Voicemail PIN	Enter the password for the extension user to access voicemail.
Prompt language	Select the display language for the extension.
Preference	Select <i>Edit preference</i> to configure the extension user preferences. See “Setting extension user preferences” on page 84. This option is only available when you edit an extension.
Advanced Setting	
SIP setting	Select the SIP profile for the extension. Click <i>Edit</i> to modify the current profile or <i>New</i> to configure a new one. For more information, see “Working with SIP profiles and caller IDs” on page 74.
Class of service	Select the services for the extension. Click <i>Edit</i> to modify the current class of service or click <i>New</i> to configure a new one. For more information on class of service, see “Configuring class of services” on page 71.
Phone type	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.
MAC address	Enter the MAC address of the SIP phone using the extension number.
Extension Information	

IP	<p>The link to the IP address of the phone using the extension number. This address is retrieved from an 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 login.</p> <p>This option is only available when you edit an extension.</p>
Group	<p>The link to the extension group of which this extension is a member. Clicking the link opens the extension group setting page. For more information on extension group, see “Creating user groups” on page 87.</p> <p>An extension can be used in multiple groups.</p> <p>This option is only available when you edit an extension.</p>

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

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.

To import extension records

1. On the *SIP* 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.

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.

To configure a remote extension

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

Table 3: Adding a remote extension

Number	Enter the local extension number from which calls are transferred to a remote extension.
Enabled	Select to activate the remote extension.
Caller ID	The name displaying on the remote extension when a call is transferred. You can choose to display the caller ID differently than the one you entered here. See “ Modifying caller IDs ” on page 76.
Remote number	Enter the remote phone number to which a call to the local extension is transferred, using digits 0-9.
Trunk	Select the trunk for transferring the call. The FortiVoice unit will select a line from the trunk to reach the remote extension. For information on trunks, see “ Configuring Trunks ” on page 90.

4. Click *Create*.

Setting extension user preferences

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

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

Figure 3: Extension preferences

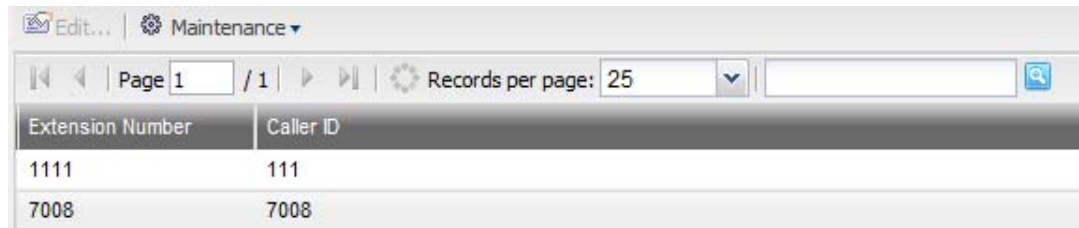


Table 4: Extension preferences

Edit	Select an extension and click this option to modify the user preferences.
Maintenance	Select an extension and click this option to reset the user preferences to the default values.
Extension Number	The extension number of which the user preferences can be edited.
Caller ID	The name displaying on the extension. This is usually the name of the extension user.

To edit extension user preferences

1. Go to *Extension > User > Preferences*.
2. Select an extension and click *Edit*.

Figure 4: Modifying extension user preferences

Extension User Preference

Voicemail setting

Extension:

Caller ID:

Ring duration: (Seconds)

Email notification option:

Email address:

Missed call email notification

Call forward Forward to:

Call waiting

Do not disturb

Message waiting indication

Display Preference

Web language:

Theme:

Time zone:

Account Management

Voicemail PIN: [[Change voicemail PIN](#)]

Speed Dial Setting

Follow Me

When I am not able to answer my phone:

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

Settings

Black list

New... | Delete |

Value

OK Cancel

3. Configure the following:

Table 5: Modifying extension user preferences

Voicemail setting	
Extension	The extension number. This is not editable.
Caller ID	Enter the name displaying on the extension. This is usually the name of the extension user.
Ring duration	Enter the phone ringing duration in seconds before an incoming call goes to voicemail.
Email notification option	Select the type of email notification when you have a voicemail. <ul style="list-style-type: none">• <i>None</i>: Do not send any notification.• <i>Simple</i>: Send an email notification.• <i>Attachment</i>: Send an email notification with the voicemail attached.
Email address	Enter the email address(es) to which the email notifications are sent.
Missed call email notification	Select to send an email when an incoming call is missed.
Call forward	Select to forward phone calls and enter the phone number to forward the calls. This function only works if call forwarding is enabled in the extension's class of service. See "Configuring class of services" on page 71.
Call waiting	Select to enable call waiting. This function only works if call waiting is enabled in the extension's class of service. See "Configuring class of services" on page 71.
Don not disturb	Select to enable DND. This function only works if DND is enabled in the extension's class of service. See "Configuring class of services" on page 71.
Message waiting indication	Select to enable phone indication that a message is received.
Display Preference	
Web language	Select the language for the FortiVoice user web interface.
Theme	Select the display theme for the FortiVoice user web interface.
Time zone	Select the time zone for the FortiVoice user web portal.
Account Management	Click <i>Change voicemail PIN</i> to change the password for accessing the voice mailbox and the FortiVoice user web interface.
Speed Dial Setting	Map a phone key to a phone number for speed dialing by clicking <i>Number</i> and enter the phone number.

Follow Me	This feature allows a call to an extension to be transferred to another destination when you are not available.
When I am not able to answer my phone	Select <i>Voicemail</i> to transfer the call to a user's voice mailbox; <i>Follow Me</i> to transfer the call to another phone; or <i>Hang up</i> to terminate the call.
Follow me setting	If you select <i>Follow Me</i> for <i>When I am not able to answer my phone</i> , click <i>New</i> to configure <i>Follow Me Setting</i> : <ol style="list-style-type: none"> 1. Enter a <i>Name</i> for this setting. 2. Click <i>New</i> to enter a phone number to which the call to your extension can be transferred and enter the phone ringing duration in seconds before the call goes to voicemail. 3. Click <i>Create</i>, then <i>Create</i>. 4. In the <i>Follow Me Setting</i> field, select the setting you've configured.
Black list	Click <i>New</i> to enter the phone number you want to block from calling this extension.

5. Click *OK*.

Creating extension groups

The *Extension > Group* submenu lets you create user and ring groups using the extensions created.

This topic includes:

- [Creating user groups](#)
- [Creating ring groups](#)

Creating user groups

You can create a user group and use it in a ring/page group configuration. User groups can simplify the creation of ring and page groups. 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 ring and page groups, see [“Creating ring groups” on page 88](#) and [“Creating page groups” on page 112](#).

To create an user group

1. Go to *Extension > Group > User group*.
2. Click *New*.
3. Enter an ID 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 user and group* field.
5. Click *Create*.

Creating ring groups

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

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

To create or edit a ring group

1. Go to *Extension > Group > Ring Groups*.
2. Click *New* or double-click an existing group.

Figure 5: Creating a ring group

The screenshot shows the 'Extension Ring Group' configuration interface. It includes a 'Number' field, an 'Enabled' checkbox, and two lists for 'Members' and 'Selected user and group'. The 'Members' list contains 'admin (user)', 'jdoe (user)', and 'operator (user)'. Below these are 'External numbers' with a table, 'Trunk' set to '--None--', 'Ring mode' set to 'Sequential', and 'Timeout' set to 20 seconds. 'Create' and 'Cancel' buttons are at the bottom.

3. Configure the following:

Table 6: Creating a ring group

Group ID	<p>The system-generated ID for this ring group. This option is only available when you edit a ring group and is view only.</p> <p>The ID is identical to the ring group number you entered when creating a ring group for the first time. If you change the ring group number later, this ID will not change.</p>
Number	<p>Enter the ring group number following the extension number pattern. See “Configuring number settings” on page 65.</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>
Enabled	<p>Select to activate the ring group.</p>
Members	<p>Select the available extensions or extension groups that you want to include in the ring group and click -> to move them into the <i>Selected user and group</i> field.</p>
External numbers	<p>Click <i>New</i> to add an external phone number to the ring group. For example, you can add the number of a remote employee to a ring group.</p>
Ring mode	<p>Select how you want the ring group to be called.</p> <ul style="list-style-type: none">• All: All extensions in the group will ring when the ring group number is dialed.• Sequence: 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.
Time Out	<p>Set the amount of time in seconds allowing all extensions or each one to ring before going to voicemail.</p>

4. Click *Create* or *OK*.

Configuring Trunks

Setting up trunks enables the FortiVoice unit to connect to the outside world. You can configure trunks that go to your SIP service provider for long distance calls, 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 79 and “Configuring Dial Plans” on page 95.

This topic includes:

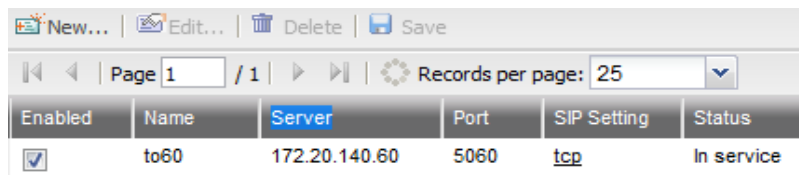
- Setting up SIP trunks
- Configuring office peers

Setting up SIP trunks

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

To view the list of service providers, go to *Trunk > SIP > SIP*.

Figure 1: SIP trunks



Enabled	Name	Server	Port	SIP Setting	Status
<input checked="" type="checkbox"/>	to60	172.20.140.60	5060	tcp	In service

Table 1: SIP trunks

Enabled	Select to activate this trunk.
Name	The name of the SIP service provider.
Server	The VoIP provider's domain name or IP address. For example, 172.20.120.11 or voip.example.com.
Port	The port for SIP sessions.
SIP Setting	The SIP profile applied to this trunk.
Status	The status of the SIP trunk. <ul style="list-style-type: none">• <i>Not registered:</i> The trunk is not registered with the service provider and is not in service.• <i>In service:</i> The trunk is registered with the service provider and is in service.• <i>Unavailable:</i> The trunk is not reachable.• <i>Alarm detected:</i> There is a problem with the phone line.• <i>Admin down:</i> The trunk is disabled.

To create a SIP trunk

1. Go to *Trunk > Trunk > SIP*.
2. Click *New*.

Figure 2: New SIP trunk

The screenshot shows the 'New SIP Trunk' configuration window. It is organized into three main sections: 'SIP Trunk', 'SIP Setting', and 'Trunk DID'.
1. **SIP Trunk:** Contains input fields for 'Name' and 'Caller ID', and an 'Enabled' checkbox which is checked.
2. **SIP Setting:** Contains input fields for 'SIP server', 'SIP port' (pre-filled with 5060), 'User name', and 'Password'. Below these is a dropdown menu for 'SIP setting' currently set to '--None--', and buttons for 'Edit...' and 'New...'. There are also expandable sections for 'Registration' and 'Proxy'.
3. **Trunk DID:** Features buttons for 'New...', 'Edit...', and 'Delete', and a table with a header 'DID Number'.
At the bottom of the window are 'Create' and 'Cancel' buttons.

3. Configure the following:

Table 2: New SIP trunk

SIP Trunk	
Name	Enter the name of the SIP service provider.
Caller ID	Enter your caller ID that will appear on the phone of an outbound call receiver.
Enabled	Select to activate the SIP trunk.
SIP Setting	
SIP server	Enter the VoIP provider's domain name or IP address. For example, 172.20.120.11 or voip.example.com.
SIP port	Most SIP configurations use TCP or UDP port 5060 for SIP sessions. If your provider uses a different port for SIP sessions, enter the port number.
User name	Enter the user name provided by the provider for the FortiVoice unit to register with the SIP server.
Password	Enter the password provided by the provider for the FortiVoice unit to register with the SIP server.
SIP setting	Select the SIP profile to apply the supported phone features and Codecs for the trunk. To match the information of the service provider, you can edit the existing profile or click <i>New</i> to add a new one. For more information, see "Configuring SIP profiles" on page 75.

Registration

Enter the SIP registration information from the service provider by selecting a method in the *Status* field. You can receive calls after registering with the SIP server of the service provider.

- *Disable*: Disables registration with the service provider. This trunk is not usable.
- *Standard*: Enter the standard registration information from the service provider:
 - *Remote SIP trunk host/IP*: Enter the VoIP provider's SIP registration server domain name or IP address. For example, 172.20.120.11 or voip.example.com.
 - *Remote SIP trunk port*: Most SIP configurations use TCP or UDP port 5060 for SIP sessions. If your provider uses a different port for SIP sessions, enter the port number.
 - *Transport protocol*: Select the transport protocol used for the registration.
- *User defined*: Enter the registration string provided by the service provider in the *User defined register string* 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`

Proxy

Some 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:

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

Trunk DID

Click *New* to add the Direct Inward Dial number provided by your service provider. DID allows the service provider SIP server to direct calls from external callers directly to the FortiVoice unit. You can add multiple DIDs.

4. Click *Create*.

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.

To set up an office peer

1. Go to *Trunk > Office > Office Peer*.
2. Click *New*.

Figure 3: Office peer trunk

The screenshot shows a configuration window for an office peer trunk. It is divided into two main sections: 'Trunk Settings' and 'Authentication Settings'. In the 'Trunk Settings' section, there are input fields for 'Name', 'Remote server', and 'Remote port' (set to 5060). There is a checked 'Enabled' checkbox, a 'Type' dropdown menu set to 'SIP', and a 'Sip setting' dropdown menu set to '--None--'. There are 'Edit...' and 'New...' buttons next to the 'Sip setting' dropdown. The 'Authentication Settings' section has two unchecked checkboxes: 'Incoming authentication' and 'Outgoing authentication'. At the bottom of the window are 'Create' and 'Cancel' buttons.

3. Configure the following:

Name	Enter a name for the trunk.
Enabled	Select to activate the trunk.
Type	Select the trunk type: SIP or IAX2.
Remote server	Enter the domain name or IP address of the remote office's PBX.
Remote port	Enter the port number for VoIP network on the remote office's PBX.
SIP setting	Select the SIP profile for the trunk. You can edit the existing profile or click <i>New</i> to add a new one. For more information, see "Configuring SIP profiles" on page 75.
Authentication settings	<p>If you want to authenticate incoming and outgoing calls, enable <i>Incoming authentication</i> and <i>Outgoing authentication</i> and enter the <i>Inbound name</i>, <i>outbound name</i>, and <i>Password</i>. These settings must be the same on both PBXes 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*.

Configuring Dial Plans

Dial plans define how calls flow into and out of a PBX. Without dial plans, telephone communications among PBXes are impossible.

This topic includes:

- Configuring outbound dial plans
- Configuring inbound dial plans
- Configuring direct inward dialing

Configuring outbound dial plans

The *Dial Plan > 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 set up an outbound dial plan

1. Go to *Dial Plan > Outbound*.
2. Click *New*.

Figure 1: Outbound dial plan

The screenshot shows the 'Dialplan Setting' configuration interface. It includes a 'Name' input field, an 'Enabled' checkbox, and a 'Dialed Number Match' table with columns for 'Match Pattern', 'Strip', 'Prefix', and 'Postfix'. Below this is a 'Caller ID Match' dropdown menu and a 'Call Handling Action' table with columns for 'Schedule', 'Trunk', and 'Caller ID manipulation'. The interface also features 'New...', 'Edit...', and 'Delete' buttons for each section, and 'Create' and 'Cancel' buttons at the bottom.

3. Configure the following:

Table 1: Outbound dial plan

Dialplan Setting	
Name	Enter a name for this plan.
Enabled	Select to activate this dial plan.
Dialed Number Match	<p>With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers.</p> <p>The numbers matching this pattern will follow this dial plan rule.</p> <p>For information on adding a dialed number match, see “Creating dialed number match” on page 96.</p>
Caller ID Match	<p>Click <i>New</i> to set the caller ID pattern following “Pattern-matching syntax” on page 97 and “Pattern-matching examples” on page 97 for this dial plan, and click <i>Create</i>.</p> <p>You can enter a caller’s display name string or the caller’ phone number string as the pattern.</p> <p>Callers with IDs under this pattern are subject to this plan.</p>
Call Handling Action	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 and click <i>Create</i> .
Schedule	Select the FortiVoice operation schedule to implement this plan. Click <i>Edit</i> to modify the selected schedule or click <i>New</i> to configure a new one. For more information on PBX schedule, see “Scheduling the FortiVoice unit” on page 67 .
Outgoing trunk	Select the trunk for the outbound calls. Click <i>Edit</i> to modify the selected trunk or click <i>New</i> to configure a new one. For more information on trunks, see “Configuring Trunks” on page 90 .
Caller ID modification	Select the caller ID modification configuration. Click <i>Edit</i> to modify the selected configuration or click <i>New</i> to configure a new one. For more information on caller ID modification, see “Modifying caller IDs” on page 76 .

4. Click *Create*.

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 support 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.

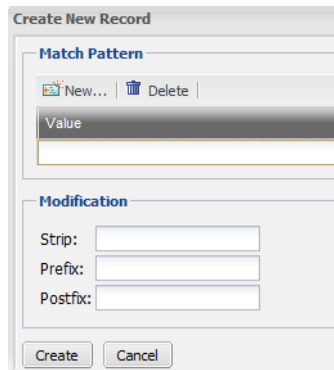
Table 3: Pattern-matching examples

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 *Dial Plan > Outbound*.
2. Click *New*.
3. In *Dialed Number Match*, click *New*.

Figure 2: Creating a number match



4. Configure the following:

Table 4: Creating a number match

Match Pattern	
New	Click to add the number pattern in the <i>Value</i> field following “Pattern-matching syntax” on page 97 and “Pattern-matching examples” on page 97 for this dial plan. Repeat to add more patterns.
Modification	You can manipulate the number patterns you entered.
Strip	Enter a number to omit dialing the starting part of a pattern. 0 means no action. For example, if your <i>Match Pattern</i> is 9XXX and <i>Strip</i> is 1, you only need to dial the last three digits for this pattern.
Prefix	Add a number before a pattern, such as area code. For example, if your <i>Match Pattern</i> is 123XXXX and its area code is 555, you can enter 555 for the <i>Prefix</i> . When you dial a number under this pattern, you do not need to dial the area code 555.
Postfix	Add a number after a pattern. For example, if your <i>Match Pattern</i> is 9XXX and the numbers under this pattern have been upgraded to have an additional digit 5 at the end, you can enter 5 for the <i>Postfix</i> . When you dial a number under this pattern, you do not need to dial the last digit - 5.

5. Click *Create*.

Configuring inbound dial plans

The *Dial Plan > 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 set up an inbound dial plan

1. Go to *Dial Plan > Inbound*.
2. Click *New*.

Figure 3: Inbound dial plan

Dialplan Inbound

Name:
Enabled:

From Trunk

Available : (4/4) Selected : (0/4)

line1
pri1
to93
tofr125

->
-<

Dialed Number Match

New... | Delete |

Value

Caller ID Match

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

Caller ID pattern

Call Handling

Action type: Dial local number

Dial Pattern

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

Match Pattern	Strip	Prefix	Postfix

Create Cancel

3. Configure the following:

Table 5: Creating inbound dial plan

Dialplan Inbound	
Name	Enter a name for this plan.
Enabled	Select to activate this dial plan.
From Trunk	<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 -> to move them into the <i>Selected</i> field.</p>
Dialed Number Match	<p>With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers.</p> <p>The called numbers matching this pattern will follow this dial plan rule.</p> <p>Create the number match following “Pattern-matching syntax” on page 97 and “Pattern-matching examples” on page 97.</p>
Caller ID Match	<p>Click <i>New</i> to set the caller ID pattern following “Pattern-matching syntax” on page 97 and “Pattern-matching examples” on page 97 for this dial plan, and click <i>Create</i>.</p> <p>You can enter an incoming call’s display name string or the caller’ phone number string as the pattern.</p> <p>Caller IDs under this pattern are subject to this plan.</p>
Call Handling	Select the actions to process the incoming calls with matched dialed numbers and/or caller IDs.

Action type

Select the type of action for the plan and configure the actions accordingly. See [“Action” on page 102](#).

- *Endpoint action*: Select if you want to send incoming calls to the local destinations according to operation schedules. For example, send calls to the voicemail after business hours.
 - *Dial local number*: Select if you want to send incoming calls to the local destinations at any time. For example, you can enter 222xxxx as a pattern and strip 222. The FortiVoice unit will only dial the last four digits for all called numbers matching the pattern.
 - *Call routing*: Select if you want to route incoming calls (to the FortiVoice unit) to an external phone system using an outbound dial plan.
-

Action

Depending on the selected *Action type*, click *New* to configure the actions:

- If you select the *Endpoint action* type:
 - a. Select the FortiVoice operation schedule for the action. Click *Edit* to modify the selected schedule or click *New* to configure a new one. For more information on PBX schedule, see “[Scheduling the FortiVoice unit](#)” on [page 67](#).
 - 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 97](#) and “[Pattern-matching examples](#)” on [page 97](#) 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. 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 before the number.
 - e. Click *Create*.
- If you select the *Call routing* type:
 - a. Select the available outbound dial plans and click -> to move them into the *Selected outbound dialplan* filed. 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 *Dial Plan > Direct Inward Dial* 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 an company's PBX system over limited rented physical lines (also called "trunk lines"). Depending on the phone numbers you rent, some workstations may not get DID numbers. Instead, they have extensions. In this case, you can map a DID number to the extensions based on the calling numbers.

To configure DID

1. Go to *Dial Plan > Direct Inward Dial*.
2. Click *New*.

Figure 4: DID setting

The screenshot shows a configuration window titled "Direct Inward Dial Setting". It is divided into two main sections. The top section, "Direct Inward Dial Setting", contains the following fields: "Name:" with an empty text box; "Enabled:" with a checked checkbox; "Incoming trunk:" with a dropdown menu showing "--None--"; and "Fall back action:" with a dropdown menu showing "Hang up". The bottom section, "DID Mapping", features a toolbar with "New...", "Edit...", and "Delete" buttons. Below the toolbar is a table with three columns: "Dialed Number", "Calling Number", and "Mapped Extension". At the very bottom of the window are "Create" and "Cancel" buttons.

3. Configure the following:

Table 6: DID settings

Direct Inward Dial Setting	
Name	Enter a name for this DID setting.
Enabled	Select to activate this DID setting.
Incoming trunk	Select the trunk used for dialing the DIDs.
Fall back action	Select the action to take if a caller not in the caller list dialed the DID number mapped to the extensions. For some actions, you need to enter the extension, such as <i>Dial voicemail</i> . For information on filtering callers, see "Mapping DIDs" on page 104.
DID Mapping	
	See "Mapping DIDs" on page 104.

4. Click *Create*.

Mapping DIDs

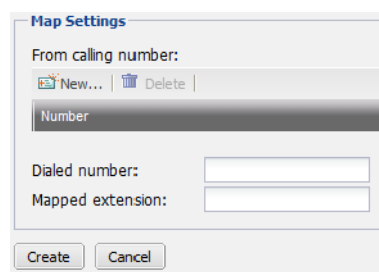
You can map a DID number to one or more extensions based on the callers' phone numbers. For example, calling numbers 123-4567, 123-4568, and 123-4569 can call the DID number 222-1000 to reach extension 1234. Calling numbers 234-4567, 234-4568, and 234-4569 can call the same DID number 222-1000 to reach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

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 ["Fall back action" on page 103](#).

To map DIDs

1. Go to *Dial Plan > Direct Inward Dial*.
2. In *DID Mapping*, click *New*.

Figure 5: DID mapping



3. Configure the following:

From calling number	Click <i>New</i> to add the caller's phone number in the <i>Value</i> field. Repeat to add more calling numbers. Only these callers will reach the mapped extension when they dial the DID number.
Dialed number	Enter the DID number that you want to map to an extension.
Mapped extension	Enter the extension that you want to map to the DID number.

4. Click *Create*.

Configuring Phone Services

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

This topic includes:

- Configuring auto attendants
- Configuring conference calls
- Creating page groups
- Configuring call parking
- Recording calls
- Modifying feature access codes

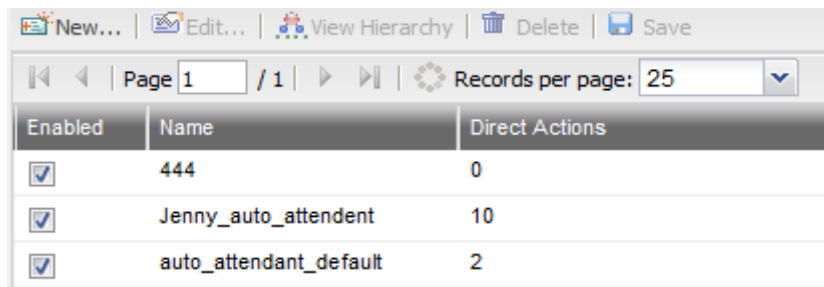
Configuring auto attendants

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 *Service > Auto Attendant > Auto Attendants*.

Figure 1: Auto Attendants list



Enabled	Name	Direct Actions
<input checked="" type="checkbox"/>	444	0
<input checked="" type="checkbox"/>	Jenny_auto_attendant	10
<input checked="" type="checkbox"/>	auto_attendant_default	2

Table 1: Auto attendant list

View Hierarchy	Click to view the hierarchical structure of the existing auto attendants. For more information, see “Viewing auto attendant hierarchies” on page 107.
Delete	Removes a selected auto attendant. You cannot remove an auto attendant that is used in another auto attendant configuration.
Enabled	Select to activate this auto attendant.
Name	The name of the auto attendant.
Direct actions	The number of key actions configured for the main auto attendant, excluding the key actions for the subsidiary auto attendants. For more information, see “Viewing auto attendant hierarchies” on page 107.

To create an auto attendant

1. Go to *Service > Auto Attendant > Auto Attendants* and click *New*.
2. Configure the following:

Figure 2: New auto attendant

Auto Attendant

Name:

Enabled:

Greeting:

Ringing for: seconds before answer

Time out after: seconds if no response

Timeout action:

Dial Pad Key Action

Key	Action	Target

Advanced

Dial local number

Call Bridge(DISA)

Outbound dialplans allowed for access:

Available : (5/5)

Selected : (0/5)

emergency
outgoing_default
to60
to64
toVM

Table 2: New auto attendant

Auto Attendant	<ul style="list-style-type: none">• <i>Name</i>: Enter a name for the auto attendant.• <i>Enabled</i>: Select to activate the auto attendant.• <i>Greeting</i>: Select a greeting message (sound file) for the auto attendant. You can edit a selected file or create a new one. For more information, see “Managing sound files” on page 70.• <i>Ringling for</i>: Enter the number of seconds for the phone to ring before the auto attendant answers with the greeting message.• <i>Timeout after</i>: 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.• <i>Timeout action</i>: Select the action when the auto attendant timeout is reached.<ul style="list-style-type: none">• <i>Dial operator</i>: The call is transferred to an operator.• <i>Start over</i>: The auto attendant will repeat the instructions for the caller.• <i>Hang up</i>: The call will be terminated.
Dial Pad Key Action	Configure the auto attendant keys for callers to use when navigating through the auto attendant hierarchy. For more information, see “Configuring key actions” on page 109 .
Advanced	Once configuring these functions, you need to inform the users on how to use them after they reach the auto attendant. <ul style="list-style-type: none">• <i>Dial local number</i>: Select to enable an external caller to dial local extensions.• <i>Call Bridge(DISA)</i>: Select an account code for dialing certain restricted outgoing calls. Callers must dial the code first before making the calls. You can edit a selected account code or create a new one. For more information, see “Configuring account codes” on page 74.• <i>Outbound dialplans allowed for access</i>: Select the outbound dial plan for users to call the FortiVoice unit and through it to make outbound calls. For details, see “Configuring outbound dial plans” on page 95.

3. Click *Create*.

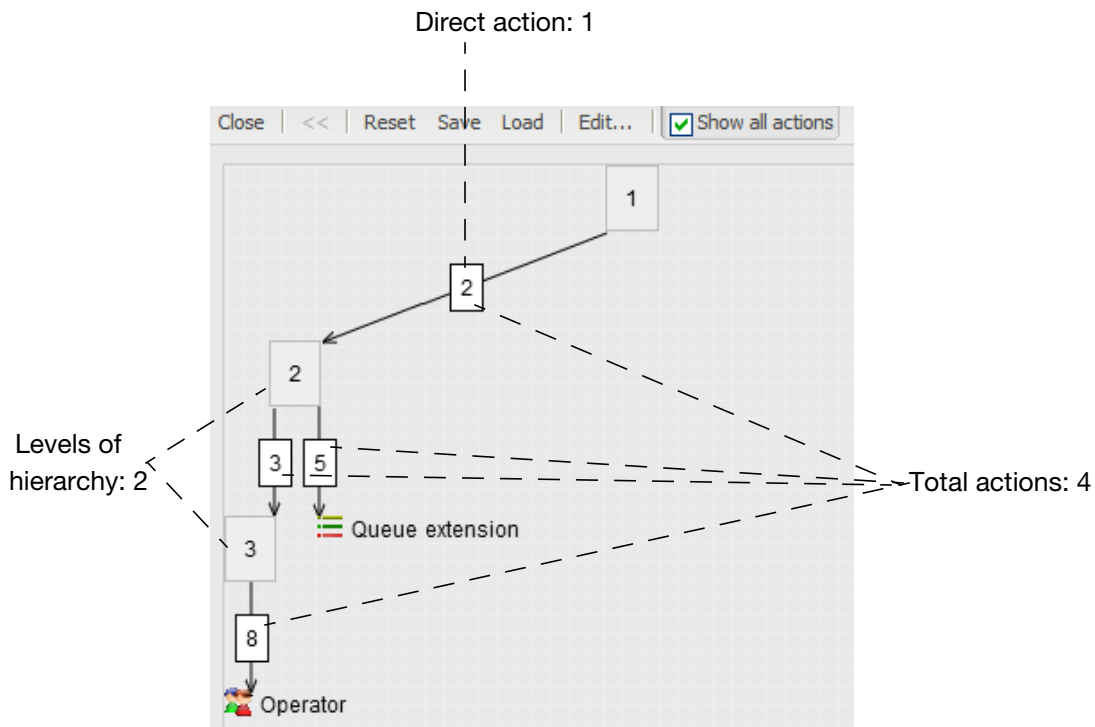
Viewing auto attendant hierarchies

The FortiVoice unit provides a chart based on your auto attendant configurations to display the levels 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 *Service > Auto Attendant > Auto Attendants*.
2. From the auto attendant list, select the one of which you want to view its hierarchy chart.
3. Click *View Hierarchy*.

Figure 3: Sample auto attendant hierarchy



This example shows the hierarchy of auto attendant 1.

- Based on the configuration, pressing 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 3: Sample auto attendant hierarchy

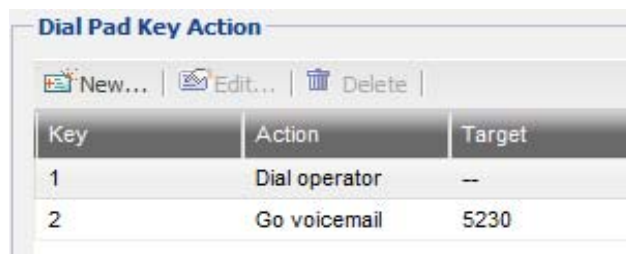
Close	Closes the chart.
<<	If you selected viewing the snapshot of an auto attendant (other than the main one) by right-clicking it and selecting <i>Drill down</i> on the chart, clicking << restores the full chart.
Reset	Sets the chart to its default view. All the saved and unsaved views will be lost.
Show all actions	Selection 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.

To view the key action list, go to *Service > Auto Attendant > Auto Attendants > Dial Pad Key Action*.

Figure 4: Key action list



Key	Action	Target
1	Dial operator	--
2	Go voicemail	5230

Table 4: Key action list

Key	The key that transfers a call to a resource, for example, voicemail, if pressed.
Action	The resource to which a call is transferred by pressing a key.
Target	The resource target if applicable. For example, an extension number, sound file, or external phone number that leads to a resource.

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:

Table 5: Key actions

No action	The call is not transferred to any resource.
Play announcement	<p>Play an announcement with directions, business hours, etc.</p> <ul style="list-style-type: none">• Select an action to follow the announcement:<ul style="list-style-type: none">• <i>No action</i>: The auto attendant takes no action.• <i>Start over</i>: The auto attendant will repeat the announcement.• <i>Hang up</i>: The call will be terminated.• Select the sound file for the announcement. You can click <i>Edit</i> to modify an existing one or <i>New</i> to add a new one. For information on sound files, see “Managing sound files” on page 70.
Dial operator	The call is transferred to the operator.
Dial extension	<p>The call is transferred to a specified local extension.</p> <p>Select the extension. You can click <i>Edit</i> to modify an existing one or <i>New</i> to add a new one. For more information, see “Configuring Extensions” on page 79.</p>
Go voicemail	<p>The call is transferred to a voice mailbox, allowing the caller to leave a message.</p> <p>Select the extension for the voice mailbox. You can click <i>Edit</i> to modify an existing one or <i>New</i> to add a new one. For more information, see “Configuring Extensions” on page 79.</p>
Dial ring group	<p>The call is transferred to the call queue of a ring group. The call is placed on hold. The system will ring the next available extension in the ring group.</p> <p>Select the ring group. You can click <i>Edit</i> to modify an existing one or <i>New</i> to add a new one. For more information, see “Creating ring groups” on page 88.</p>
Dial external number	<p>The call is transferred to a specified remote extension number.</p> <p>Enter the remote extension number. For more information, see “Setting up remote extensions” on page 83.</p>

Queue extension

Lookup name directory Access the dial-by-name directory so the caller can find a user's extension number by entering the user's name.

Auto attendant Route the call to another auto attendant, which allows actions to be nested into a powerful call routing system. For example, the main auto attendant can say "Press one for English. Oprima dos para Español." Option 1 goes to the English auto attendant and option 2 goes to the Spanish auto attendant.

Select an auto attendant. For information on creating auto attendants, see ["Configuring auto attendants" on page 105](#).

Start over The auto attendant will repeat the announcement.

Go back The auto attendant will repeat the previous level announcement.

Hang up The call is terminated.

4. Optionally, enter any comments about this key action.
5. Click *Create*.

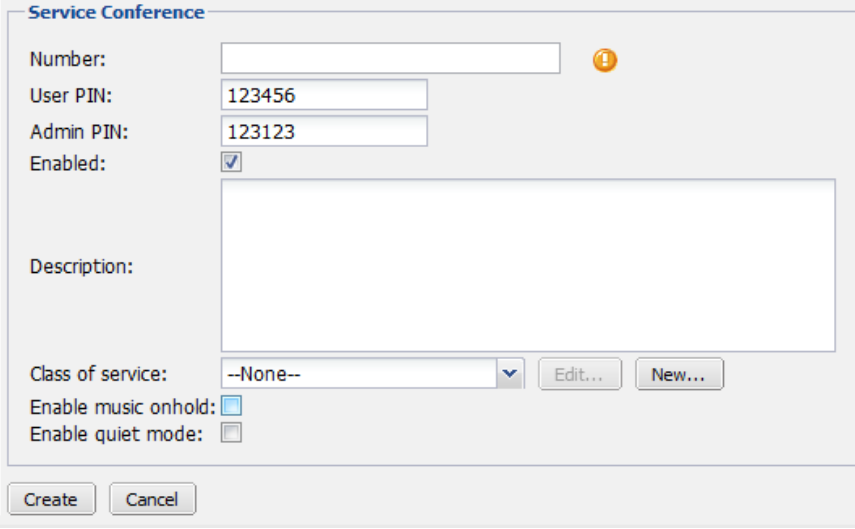
Configuring conference calls

The *Service > Conference > Conferences* tab lets you configure and enable conference call settings.

To configure a conference call

1. Go to *Service > Conference > Conferences* and click *New*.

Figure 5: Configuring conference call



The screenshot shows a configuration window titled "Service Conference". It contains the following fields and controls:

- Number:** An empty text input field with a yellow information icon to its right.
- User PIN:** A text input field containing "123456".
- Admin PIN:** A text input field containing "123123".
- Enabled:** A checked checkbox.
- Description:** A large empty text area.
- Class of service:** A dropdown menu currently set to "--None--".
- Enable music onhold:** A checked checkbox.
- Enable quiet mode:** An unchecked checkbox.
- Buttons for "Edit...", "New...", "Create", and "Cancel" are located at the bottom of the window.

2. Configure the following:

Table 6: Configuring conference call

Number	Select an extension number that callers can call and enter the user PIN to join a conference call.
User PIN	Enter a password for joining the conference call. A caller needs to dial the conference call number and enter this password to join the conference call.
Admin PIN	Enter the number to be entered by the conference host to be able to host a conference call.
Enabled	Select to activate this conference call.
Description	Enter any notes you have for this conference call.
Class of service	Select the service class for this conference call. You can click <i>Edit</i> to modify an existing one or <i>New</i> to add a new one. For information on class of service, see “ Configuring class of services ” on page 71.
Enable music onhold	Select to play background music that callers hear after the joining message and leaving message are played.
Quiet mode	Select to mute the background sound that callers hear after the joining message and leaving message are played.

3. 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 customer calls the sales group, the first available salesperson answers for the group.

To create a page group

1. Go to *Service > Paging > Paging*.
2. Click *New*.
3. Enter the page group number following the extension number pattern. See “[Configuring number settings](#)” on page 65.
This is the number that, once paged, will ring all the extensions in the group.
4. Select *Enabled* to activate this group.
5. Select the available extensions or extension groups that you want to include in the page group and click -> to move them into the *Selected user and group* field.
6. Click *Create*.

Configuring call parking

Call park is a feature for placing a call on hold and then retrieving it from any other local extension. By default, the FortiVoice unit has 20 park orbits, 101–120.

To view the parked calls, see [“Viewing parked calls” on page 17](#).

To configure call parking

1. Go to *Service > Call Parking > Call Parking*.
2. For *Park call number*, enter the number to dial to park a call.
For example, if you enter 100, depending on the phone, when a user receives a call and wants to park it, the user may:
 - a. press #100.
The FortiVoice unit selects the first available park orbit (101–120). The user hears a confirmation indicating the caller has been parked successfully and into which park orbit.
 - b. 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 101).
3. For *Park line start*, enter the starting park orbit. The default is 101.
4. For *Park line end*, enter the ending park orbit. The default is 120.
5. For *Parking time out*, enter the time in seconds to time out the parked call. The default is 80 seconds.
6. Click *OK*.

Recording calls

For supervising and monitoring purpose, 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 listen or save the recordings. For details, see [“Playing recorded calls” on page 26](#).

To configure call recording

1. Go to *Service > Recording > Recording*.
2. Click *New*.
3. Enter a *Name* for this configuration.
4. Select *Enabled* to activate this configuration.
5. For *Caller number pattern*, enter the number pattern to match the callers’ phone numbers following the pattern as configured in [“Configuring number settings” on page 65](#).
The phone calls from the numbers matching the pattern will be recorded.
6. For *Dialed number pattern*, enter the number pattern to match the dialed phone numbers following the pattern as configured in [“Configuring number settings” on page 65](#).
The phone calls to the numbers matching the pattern will be recorded.
7. Click *Create*.

Modifying feature access codes

By default, the FortiVoice unit has defined seven 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 example, if you change the DISA code from the default ** to 12, dialing 12 still accesses the DISA feature.

The features include:

- *Attended transfer*: During a call, dial *2 or the code you set and then the extension number of a second person to transfer the call to the person. Since you want to inform the second person about the call, you can have a private conversation with the person without the first person who made the call hearing it.
- *Blind transfer*: During a call, dial # 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.
- *DISA*: Direct Inward System Access (DISA) service allows external users to log into PBX and use PBX service just like the local extensions. To use DISA, dial the PBX main number and then ** or the code you set. The PBX will prompt you to enter the password (password set at *PBX > Class of Service > Account code*). Once you pass authorization, you can use PBX service just like a local extension.
- *DND off*: Dial *79 or the code you set to turn off the Do Not Disturb service. Otherwise, callers will hear the busy sound when they dial your number.
- *DND on*: Dial *78 or the code you set to turn on the Do Not Disturb service. Callers will hear the busy sound when they dial your number.
- *Voicemail direct*: Dial *97 or the code you set from your own phone and then enter your voicemail password to directly access your voice mailbox.
- *Voicemail prompt*: Dial *98 or the code you set from any extension and then enter your extension number and voicemail password to access your voice mailbox.

Configuring Logs and Reports

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

FortiVoice units provide extensive logging capabilities for voice incidents and system events. Detailed log information and reports provide 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.

This topic includes:

- [About FortiVoice logging](#)
- [Configuring logging](#)
- [Configuring report profiles and generating reports](#)
- [Setting call rates](#)

About FortiVoice logging

FortiVoice units can log:

- system-related events, such configuration change 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 116.

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 116. It can also use log messages as the basis for reports. For more information, see [“Configuring report profiles and generating reports”](#) on page 121.

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 *Log* submenu of the *Monitor* tab.

Table 1: Log types

Log type	Subtype	Description
Event	config admin system update ha voicemail	Includes system and administration events, such as downloading a backup copy of the configuration.
Voice		Includes phone calls 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 2: 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.

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.

See also 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 116](#).

For information on viewing locally stored log messages, see [“Viewing log messages” on page 20](#).

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 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 20](#).

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 43](#).

To configure logging to the local hard disk

1. Go to *Log and 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*, enable the types of logs that you want to record to this storage location. Click the arrow to review the options. For details, see “[Choosing which events to log](#)”.
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 3: Events logging options

Event Log	<p>Select this check box and then select specific events. No event types are logged unless you enable this option.</p> <ul style="list-style-type: none"> • <i>When configuration has changed:</i> Log configuration changes. • <i>Admin login/logout event:</i> Log all administrative events, such as logins, resets, and configuration updates. • <i>System activity event:</i> Log all system-related events, such as rebooting the FortiVoice unit. • <i>SMTP server event:</i> Log SMTP relay or proxy events. This option is for local log setting only. <i>DHCP event:</i> Log DHCP server events. This option is for local log setting only. • <i>Voice mail event:</i> Log voicemail events. This option is for remote log setting only.
Voice Log	Log phone call events. This option is for local log setting only.

Configuring logging to a Syslog server or FortiAnalyzer unit

Instead of or in addition to logging locally, you can store log messages remotely on a Syslog server or a FortiAnalyzer unit.

You can add a maximum of three remote Syslog servers.



Logs stored remotely cannot be viewed from the web-based manager of the FortiVoice unit. If you require the ability to view logs from the web-based manager, also enable local storage. For details, see “[Configuring logging to the hard disk](#)” on page 117.

Before you can log to a remote location, you must first enable logging. For details, see “[Choosing which events to log](#)” on page 118. 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 43.

To configure logging to a Syslog server or FortiAnalyzer unit

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

Figure 1: Remote Log Settings tab

Enabled	ID	Server	Port	Level	Facility
<input type="checkbox"/>	1	172.20.120.255	514	Emergency	kern
<input type="checkbox"/>	2	10.10.10.10	514	Notification	local1

Table 4: Viewing the list of remote logs

Enabled	Select to enable remote storage on the server. Clear to disable storage.
ID	Displays the remote host ID.
Server	Displays the IP of the Syslog server or FortiAnalyzer unit.
Port	Displays the port on the Syslog server or FortiAnalyzer unit.
Level	Displays the minimum severity level for logging purposes.
Facility	Displays the facility identifier the FortiVoice unit uses to identify itself.

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

Figure 2: Remote host configuration dialog

Log to Remote Host

Enable

IP: Port:

Level: ▼

Facility: ▼

CSV format: Enable

▲ **Logging Policy Configuration**

Event Log

- When configuration has changed
- Admin login/logout event
- System activity event
- Voice mail event

Create Cancel

Table 5: Remote host configuration

Enable	Select to allow logging to a remote host.
IP	Enter the IP address of the Syslog server or FortiAnalyzer unit where the FortiVoice unit will store the logs.
Port	If the remote host is a FortiAnalyzer unit, enter 514; if the remote host is a Syslog server, enter the UDP port number on which the Syslog server listens for connections (by default, UDP 514).
Level	Select the severity level that a log message must equal or exceed in order to be recorded to this storage location. For information about severity levels, see “Log message severity levels” on page 116 .
Facility	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
CVS format	Enable this option if you want to send log messages in comma-separated value (CSV) format. Do not enable this option if the remote host is a FortiAnalyzer unit. FortiAnalyzer units do not support CSV-formatted log messages.
Logging Policy Configuration	Click the arrow to review the options and enable the types of logs you want to record to this storage location. For details, see “Choosing which events to log” on page 118 .

- 3 Click *Create*.
- 4 If the remote host is a FortiAnalyzer unit, confirm with the FortiAnalyzer administrator that the FortiVoice unit was added to the FortiAnalyzer unit’s device list, allocated sufficient disk space quota, and assigned permission to transmit logs to the FortiAnalyzer unit. For details, see the [FortiAnalyzer Administration Guide](#).
- 5 To verify logging connectivity, from the FortiVoice unit, trigger a log message that matches the types and severity levels that you have chosen to store on the remote host. Then, on the remote host, confirm that it has received that log message.

For example, if you have chosen to record event log messages to the remote host and if they are more severe than information, you could log in to the web-based manager or download a backup copy of the FortiVoice unit’s configuration file in order to trigger an event log message.

If the remote host does not receive the log messages, verify the FortiVoice unit’s network interfaces (see [“Configuring the network interfaces” on page 29](#) and [“About the management IP” on page 28](#)) and static routes (see [“Configuring static routes” on page 33](#)), and the policies on any intermediary firewalls or routers. If ICMP ECHO (ping) is enabled on the remote host, you can use the execute traceroute command to determine the point where connectivity fails.

Configuring report profiles and generating reports

The *Log and Report > Report Settings > Configuration* 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 124.

To view and configure report profiles

- 1 Go to *Log and Report > Report Settings > Configuration*.

Figure 3: Configuration tab

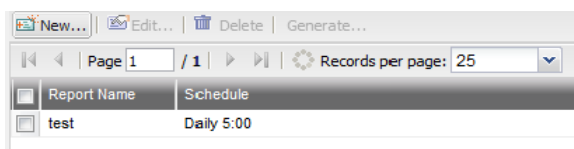


Table 6: Viewing the list of report profiles

Generate	Select a report and click this button to generate a report immediately. See “Generating a report manually” on page 125.
Report Name	Displays the name of the report profiles.
Schedule	Displays the frequency with which the FortiVoice unit generates a scheduled report. If the report is designed for manual generation, <i>Not Scheduled</i> appears in this column.

- 2 Click *New* to add a profile or double-click a profile to modify it. A multisection dialog appears.

Figure 4: New report configuration

The screenshot shows the 'Report Setting' configuration window. It includes a 'Name' field, a 'Query List' section with a toolbar and a table, a 'Period' section with date and value fields, an 'Email' section with recipient and format fields, a 'Schedule' section with a type dropdown, and a 'Rate Setting' section with two list boxes and navigation arrows. 'Create' and 'Cancel' buttons are at the bottom.

- 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](#)
 - [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 and Report > Report Settings > Configuration*.

- Expand *Query List* and click *New*.

Figure 5: Query selection

The screenshot shows a 'Query' configuration window with the following settings:

- Name: [Empty text box]
- Category: Call_Usage
- Subcategory: Summary
- From: Internal
- To: External
- Region: Any
- Order by: Caller
- Graph focus: Default
- Limited records: [Empty text box]

Buttons: Create, Cancel

- Configure the following:

Table 7: Report query selection options

Name	Enter a name for this query.
Category	Select a category for the report profile. The report chart will correspond to the category selected. <ul style="list-style-type: none"> • <i>Call Usage</i>: The number of calls. • <i>Phone Bill</i>: The cost of making the phone calls. • <i>Trunk Usage</i>: The status of the trunks being used.
Subcategory	Select to have a summary or detailed report on the report category you select.
Call from	Select to include the source of the incoming calls: internal, external, or any.
Call to	Select to include the source of the outgoing calls: internal, external, or any.
Region	Select the call region, such as international or long distance.
Order by	Select the order of statistics in the report, by caller, receiver, date, or hour of day.
Graph focus	Select the value for the X axis in the report chart.
Limited records	Enter the maximum number of records you want to appear in the generated report.

- Click *Create*.

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 and Report > Report Settings > Configuration*.
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*, chose 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.

To configure an email notification

1. Go to *Log and Report > Report Settings > Configuration*.
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 125.

To configure the report schedule

1. Go to *Log and Report > Report Settings > Configuration*.
2. Expand *Schedule*.
3. Configure the following:

Table 8: Report schedule options

Schedule	
	<ul style="list-style-type: none">• <i>None</i>: Select if you do not want the FortiVoice unit to generate the report automatically according to a schedule. If you select this option, the report can only be generated on demand. See “Generating a report manually” on page 125.• <i>Daily</i>: Select to generate the report each day. Also configure <i>Hour</i>.• <i>Weekdays</i>: Select to generate the report on specific days of each week, then select those days in <i>These weekdays</i>. Also configure <i>Hour</i>.• <i>These dates</i>: Select to generate the report on specific date of each month, then enter those date numbers in <i>These days</i>. Also configure <i>Hour</i>.

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 and Report > Report Settings > Configuration*.
- 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 25.

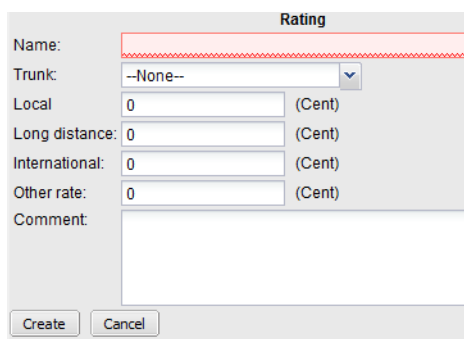
Setting call rates

The *Log and Report > Report Settings > Rate* tab lets you set call rates. The rates are used to calculate phone bills.

To set call rates

1. Go to *Log and Report > Report Settings > Rate* and click *New*.

Figure 6: Call rate



2. configure the following:

Table 9: Call rate configuration

Name	Enter a name for the rating profile.
Trunk	Select the trunk over which you want to rate the calls.
Local	Enter the rate for local phone calls.
Long distance	Enter the rate for long distance phone calls.
International	Enter the rate for international phone calls.
Other rate	Enter the rate for other types of phone calls.
Comments	Enter any notes you have for this rating profile.

3. Click *Create*.

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 a RJ-45 to DB-9 serial cable or a null-modem cable.
2. Initiate a connection from your management computer to the CLI of the FortiVoice unit.
3. Connect port1 of the FortiVoice unit directly or to the same subnet as a TFTP server.
4. Copy the new firmware image file to the root directory of the TFTP server.
5. Verify that the TFTP server is currently running, and that the FortiVoice unit can reach the TFTP server.

To use the FortiVoice CLI to verify connectivity, enter the following command:

```
execute ping 192.168.2.99
```

where 192.168.2.99 is the IP address of the TFTP server.

Enter the following command to restart the FortiVoice unit:

```
execute reboot
```

6. As the FortiVoice unit starts, a series of system startup messages are displayed.
Press any key to display configuration menu.....
Immediately press a key to interrupt the system startup.



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

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

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 128.
 - 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 132](#).

Therefore, no matter you are upgrading or downgrading, it is always a good practice to back up the configuration and call data. For details, see “[Backup and restore](#)” on [page 62](#). **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 a 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 message 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 130](#) and [“Restoring the configuration” on page 131](#).

If you have upgraded the firmware version, to verify the conversion of the configuration file, see [“Verifying the configuration” on page 132](#). 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 133](#).

To reconnect using the CLI

1. Connect your management computer to the FortiVoice console port using a 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*:

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

5. Press Enter to connect to the FortiVoice CLI.
The login prompt appears.
6. Type `admin` and press Enter twice.
The following prompt appears:
Welcome!

7. Enter the following command:

```
set system interface <interface_str> mode static ip <address_ipv4>
<mask_ipv4>
```

where:

- <interface_str> is the name of the network interface, such as `port1`
- <address_ipv4> is the IP address of the network interface, such as `192.168.1.10`
- <mask_ipv4> is the netmask of the network interface, such as `255.255.255.0`

Enter the following command:

```
set system interface <interface_str> config allowaccess
<accessmethods_str>
```

where:

- <interface_str> is the name of the network interface configured in the previous step, such as `port1`
- <accessmethods_str> is a space-delimited list of the administrative access protocols that you want to allow on that network interface, such as `ping ssh https`

The network interface's IP address and netmask is saved. You can now reconnect to either the web UI or CLI through that network interface. For information on restoring the configuration, see [“Restoring the configuration” on page 131](#).

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 [“Backup and restore” on page 62](#).

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 132](#).

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 132](#).

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 “Backup and restore” on page 62. For information on reconnecting to a FortiVoice unit whose network interface configuration has been reset, see “Reconnecting to the FortiVoice unit” on page 130.



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 a RJ-45 to DB-9 serial cable or a null-modem cable.
3. Initiate a **local console connection** from your management computer to the CLI of the FortiVoice unit, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
4. Connect port1 of the FortiVoice unit directly to the same subnet as a TFTP server.
5. Copy the new firmware image file to the root directory of the TFTP server.
6. Verify that the TFTP server is currently running, and that the FortiVoice unit can reach the TFTP server.

To use the FortiVoice CLI to verify connectivity, if it is responsive, enter the following command:

```
execute ping 192.168.2.99
```

where `192.168.2.99` is the IP address of the TFTP server.

7. Enter the following command to restart the FortiVoice unit:

```
execute reboot
```

or power off and then power on the FortiVoice unit.

8. As the FortiVoice unit starts, a series of system startup messages are displayed.
Press any key to display configuration menu.....
9. Immediately press a key to interrupt the system startup.



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

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

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

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

10. If the firmware version requires that you first format the boot device before installing firmware, type F. (Format boot device) before continuing.
11. Type G to get the firmware image from the TFTP server.
The following message appears:
Enter TFTP server address [192.168.2.99]:
12. Type the IP address of the TFTP server and press Enter.
The following message appears:
Enter Local Address [192.168.1.188]:
13. Type a temporary IP address that can be used by the FortiVoice unit to connect to the TFTP server.
The following message appears:
Enter File Name [image.out]:
14. Type the firmware image file name and press Enter.
The FortiVoice unit downloads the firmware image file from the TFTP server and displays a message similar to the following:
Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
15. Type D.
The FortiVoice unit downloads the firmware image file from the TFTP server. The FortiVoice unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.
The FortiVoice unit reverts the configuration to default values for that version of the firmware.
16. Clear the cache of your web browser and restart it to ensure that it reloads the web-based manager and correctly displays all tab, button, and other changes.
17. To verify that the firmware was successfully installed, log in to the CLI and type:
`get system status`
The firmware version number appears.
18. Either reconfigure the FortiVoice unit or restore the configuration file from a backup. For details, see [“Restoring the configuration” on page 131](#).

Setup for phone users

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

This topic includes:

- [Accessing the user web portal](#)
- [Changing the voicemail PIN](#)
- [Setting user preferences](#)

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 the call record for received, placed, or missed calls
- check the voicemail including playing, deleting, or saving the voicemails
- view the corporate phone directory
- check the feature codes that one can dial on the phone keypad
- configure the extension according to user's preferences.

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 voicemail PINs. With these 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 voicemail 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 voicemail PINs, see [“Configuring IP extensions”](#) on page 79.

Changing the voicemail PIN

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

Setting user preferences

The call features each phone user can use is controlled by the class of service settings associated with the user's extension. You may need to inform users of the features that they can use.

For information on class of service, see [“Configuring class of services”](#) on page 71.

Index

A

- address bar 136
- administrative access 30
- administrator
 - "admin" account 8, 9, 128, 129, 131, 132, 133
 - log messages 118
- appearance, web-based manager 49
- authentication 8

B

- bandwidth 16
- Base64 59, 60
- boot interrupt 133
- browser 7, 8, 136
 - warnings 8

C

- cable
 - null modem 9
- call statistics 17
- certificate
 - backup 61
 - default 8
 - mismatch 8
 - options 56
 - self-signed 8
 - server 55
 - warning 8
- certificate authority (CA) 8, 56, 59, 60, 61, 62
- certificate request
 - downloading and submitting 59
- certificate revocation list (CRL) 62
- clean install firmware 133
- CLI 33
 - connecting to 9
- column view
 - logs 22
- command line interface (CLI) 7
- comma-separated value (CSV) 120
- common name (CN) field 8
- communications (COM) port 9
- configuration, verifying the 132
- connecting
 - web UI 8
- CPU 16
- CSV import 83

D

- dashboard 14
- date 43, 44
- daylight savings time (DST) 43, 44

default

- administrator account 8, 9, 128, 129, 131, 132, 133
- bridge configuration 28
- certificate 8
- gateway 32, 33
- password 8, 9, 10, 11
- route 33, 34
- settings 9

default variables 69, 70

DHCP 32

DNS server 32, 35

documentation

- Release Notes 133

domain name

- certificate 8

DOS 7

downgrade 128

download

- report 25

dynamic DNS (DDNS) 58

dynamic IP address 32

E

- Ethernet 8, 9

F

- factory default settings 9
- firmware 128
 - change 15
 - clean install 133
 - downgrade 128
 - upgrade 128
 - version 14
- formatted view
 - logs 22
- formatting the boot device 133
- FortiAnalyzer 116, 118
- frame size 33
- fully qualified domain name (FQDN) 58
- fully-qualified domain name (FQDN) 58

G

- gateway 33, 34
- graphical user interface (GUI) 7

H

- halt 16
- hard disk
 - logging to 117
- host name 8
- HTTP
 - web-based manager 33
- HTTPS 8, 33, 55, 58
- HyperTerminal 9

I

- ICMP ECHO 33
- idle timeout 46
- import
 - user in CSV 83
- Internet service provider (ISP) 35
- IP address 8, 9, 136

L

- language
 - web-based manager 50
- local certificate
 - options 56
- location 136
- log
 - column view 22
 - formatted view 22
 - FortiAnalyzer 118
 - rotate 117
 - search 24
 - severity level 116
 - storage 116
 - storing 116
 - Syslog 118
 - to the hard disk 117

M

- management IP 28
- maximum transmission unit (MTU) 33
- media access control (MAC) 32
- memory usage 16
- Microsoft
 - Internet Explorer 8
- Mozilla Firefox 8

N

- network
 - interface 9
- network time protocol (NTP) 43, 44
- next-hop router 34
- null modem cable 9

P

- password 8, 9, 10, 11
 - administrator 53
 - certificate 61
- PDF report 124
- phone-user guide 136
- ping 33
- PKCS #10 59
- PKCS #12 60, 61
- port1 9
- privacy-enhanced email (PEM) 60
- profile
 - administrator access 54
- protocol
 - administrative access 53
- public key 60

Q

- query
 - report 122

R

- reachable 34
- read & write
 - administrator 53
- reconnecting to the FortiMail unit 130
- Release Notes 133
- report
 - configure 121
 - download 25
 - HTML format 124
 - on demand 121
 - PDF format 124
 - periodically generated 121
 - query 122
 - subject matter 122
 - time span 123
 - view 25
- restart 16
- restore
 - factory defaults 27
 - previous configuration 131
- RJ-45 8, 9
- route
 - default 34
 - static 33, 34

S

- secure (S/MIME) 61
- Secure Shell (SSH) 7
- secure shell (SSH) 33
- security certificate 8
- self-signed 8
- severity level 116
- shut down 16
- SNMP 33
- static route 34
- static routing 33
- storing logs 116
- subject matter 122
- Syslog 116, 118
- system options
 - changing 44
 - data and time 43
- system resource usage 14
- system time 14

T

- Telnet 7
- telnet 33
- terminal 7, 9
- time 43, 44
- time zone 44
- transport layer security (TLS) 61
- troubleshooting
 - Syslog 120

trust certificate 8
trusted host 53

U

UNIX 7
update 128
 verify 132
uptime 14
URL 8, 136
user guide 136

V

variable
 Predefined 68

variables
 predefined list 69, 70

W

web browser 7, 8, 136
 warnings 8
web UI 8
web-based manager
 customizing appearance 49
 HTTP 33
 HTTPS 33
 language 50
widget 14

