FortiVoice™ Gateway 6.0.0
Administration Guide

FortiVoice™ Gateway 6.0.0 Administration Guide

November 14, 2019

2nd Edition

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

Table of Contents

Introduction

Welcome, and thank you for selecting Fortinet products.

The FortiVoice Gateway is a simple solution for adding analog phone lines (GO08 and GS16) or PRI lines (GT01 and GT02) to your SIP server enabled PBX. With the easy to use and intuitive web interface, you can quickly create rules that allow calls from analog/PRI lines, connected to the FortiVoice Gateway FXO/PRI ports, to communicate directly to your SIP server enabled PBX. The FortiVoice Gateway also offers various usage tracking options, such as call statistics and call detail records, so you can monitor the calls coming through the system.

This document describes how to configure and use the FortiVoice Gateway through the web-based manager.

This topic includes:

Registering your Fortinet product

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

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

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

Customer service & technical support

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

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

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

Training

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

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

Documentation

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

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

Fortinet Tools & Documentation CD

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

Fortinet Knowledge Base

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

Comments on Fortinet technical documentation

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

Scope

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

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

Conventions

Fortinet technical documentation uses the following conventions:

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

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

Cautions and notes

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

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

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

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographical conventions in Fortinet technical documentation

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

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

CLI output	`FGT-602803030703 # get system settings`
	`comments  : (null)`
	`opmode  : nat`

Emphasis	HTTP connections are ***not*** secure and can be intercepted by a third party.
File content	`<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>` `<BODY><H4>You must authenticate to use this service.</H4>`
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com.
Keyboard entry	Type a name for the remote VPN peer or client, such as `Central_Office_1`.

Table 1: Typographical conventions in Fortinet technical documentation

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

Command syntax conventions

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

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

Table 2: Command syntax notation

Convention	Description

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

Table 2: Command syntax notation

Angle brackets < >	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: `<retries_int>` indicates that you should enter a number of retries, such as `5`. Data types include: • `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`. • `<xxx_index>`: An index number referring to another part of the configuration, such as `0` for the first static route. • `<xxx_pattern>`: A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`. • `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`. • `<xxx_email>`: An email address, such as `admin@mail.example.com`. • `<xxx_url>`: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as `http://www.fortinet.com/`. • `<xxx_ipv4>`: An IPv4 address, such as `192.168.1.99`. • `<xxx_v4mask>`: A dotted decimal IPv4 netmask, such as `255.255.255.0`. • `<xxx_ipv4mask>`: A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`. • `<xxx_ipv4/mask>`: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as `192.168.1.99/24`. • `<xxx_ipv6>`: A colon(`:`)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`. • `<xxx_v6mask>`: An IPv6 netmask, such as `/96`. • `<xxx_ipv6mask>`: An IPv6 address and netmask separated by a space. • `<xxx_str>`: A string of characters that is ***not*** another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. • `<xxx_int>`: An integer number that is ***not*** another data type, such as `15` for the number of minutes.

Table 2: Command syntax notation

Curly braces `{ }`		A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].
	Options delimited by vertical bars |	Mutually exclusive options. For example: `{enable | disable}` indicates that you must enter either `enable` or `disable`, but must not enter both.

	Options delimited by spaces	Non-mutually exclusive options. For example:
		`{http https ping snmp ssh telnet}`
		indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
		`ping https ssh`
		To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type:
		`ping https snmp ssh`
		If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Connecting to the FortiVoice Gateway System

After physically installing the FortiVoice Gateway, you need to connect to its management tools to configure, maintain, and administer the unit.

This topic includes:

Connecting to the web-based manager or CLI

There are two methods to connect to the FortiVoice Gateway:

- 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 17.

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

This topic includes:

Connecting to the web-based manager

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

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

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

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

To connect to the web-based manager

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 with a netmask of 255.255.255.0.
2. Using the Ethernet cable, connect your computer's Ethernet port to the FortiVocieGateway'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 Gateway ships with a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiVocieGateway. When you connect, depending on your web browser and prior access of the FortiVocieGateway, 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 FortiVocieGateway. If your login is successful, the web UI appears. To continue by updating the firmware, see "System Information widget" on page 17. Otherwise, to continue by following the configuration wizard.

Connecting to the CLI

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

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

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

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

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

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

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

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

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

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 FortiVocieGateway's console port.
2. Verify that the FortiVocieGateway 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 FortiVocieGateway.
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:

   `FortiVocieGateway #`
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 FortiVocieGateway's port1.
3. Verify that the FortiVocieGateway 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 FortiVocieGateway.

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

Using the dashboard

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

This section includes:

Viewing the dashboard

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

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

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

This topic includes:

Hiding, showing and moving widget

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

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

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

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

System Information widget

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

In addition to displaying basic system information, the *System Information* widget lets you change the firmware. To change the firmware, click *Update* for *Firmware version*. For more information, see "Installing firmware" on page 64.

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

System Resource widget

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

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

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

Statistics History widget

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

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

Also see "Viewing Call Statistics" on page 18.

Service Status widget

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

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

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

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

Viewing Call Statistics

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

Using the CLI Console

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

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

For more information about CLI commands, see the *FortiVoice CLI Reference*.

Monitoring the FortiVoice Gateway System

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

This topic includes:

Viewing phone system status

Monitor > *Phone System* displays all the ongoing phone calls and trunks.

This topic includes:

Viewing active calls

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

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

The call statuses include:

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

Viewing trunk status

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

The trunk statuses include:

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

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

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

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

For more information, see “Configuring FortiVoice Gateway” on page 44.

Viewing call records

Monitor > *Call History* displays all the phone calls made during a certain time period, including time of the call, caller and receiver, call duration, call status, and call direction.

Double-clicking a record displays the detailed call information, including the call detail records (CDR) flow.

You can filter the call history 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 FortiVocieGateway 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 FortiVocieGateway. If you want to view logs from the web-based manager, also enable local storage. For details, see “Configuring Logs” on page 60.

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

To view the list of log files and their contents

1. Go to *Monitor* > *Log* > *System/Voice/Fax.*

   The list of log files appears with the beginning and end of a log file’s time range and the size of a log file in bytes. The queue log files display more information.
2. To search the log files, click the *Search* button and enter criteria that records must match in order to be visible.

   Unlike the search when viewing the contents of an individual log file, this search displays results regardless of which log file contains them. For more information, see “Searching log messages” on page 21.
3. To view messages contained in logs, double-click a log file.

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 21.

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

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

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

   The log messages are sorted in ascending order.
2. To sort in descending order, click the column heading again.

   Depending on your currently selected theme:

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

To display or hide columns

1. Go to *Monitor* > *Log* > *System/Voice/Fax*.
2. Click the *Configure View* icon.
3. Click *Show/Hide Columns*.
4. Select the columns you want to show or hide.
5. Click *OK*.

To change the order of the columns

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

Using the right-click pop-up menus

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

View Details	Select to display the log details.
Select All	Select to select all log messages in the current page, so that you can export all messages.
Clear Selection	Select to deselect one or multiple log messages.
Export	Select to open or save the log file.

Searching log messages

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

To search log messages

1. Go to *Monitor* > *Log* > *System/Voice/Fax*.
2. Click *Search*.

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

GUI field	*Description*
Keyword	Enter any word or words to search for within the log messages. For example, you might enter GUI session to locate all log messages containing that exact phrase in any log field.
Message	Enter all or part of the *Message* log field.
Log ID	Enter all or part of the log ID in the log message.
Match condition	• *Contain*: searches for the exact match. • *Wildcard*: supports wildcards in the entered search criteria.
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.

4. Click *Search*.

   The FortiVocieGateway unit searches for log messages that match your search criteria, and displays any matching log messages.

Configuring System Settings

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

This topic includes:

Configuring network settings

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

This topic includes:

About FortiVoice Gateway logical interfaces

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

VLAN subinterfaces

A Virtual LAN (VLAN) subinterface, also called a VLAN, is a virtual interface on a physical interface. The subinterface allows forwarding 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 24.

Redundant interfaces

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

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

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

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

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

For information about adding redundant interfaces, see “Configuring the network interfaces” on page 24.

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 Gateway’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 Gateway.

For information about adding a loopback interface, see “Configuring the network interfaces” on page 24.

Configuring the network interfaces

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

You must configure at least one network interface for the FortiVoice Gateway to connect to your network. Depending on your network topology and other considerations, you can connect the FortiVoice Gateway 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 Gateway logical interfaces” on page 23, and “Editing network interfaces” on page 25.

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

GUI field	***Description***
Name	Displays the name of the network interface, such as *port1*.
Type	Displays the interface type: physical, VLAN, redundant, or loopback. For details, see “About FortiVoice Gateway logical interfaces” on page 23.

IP/Netmask	Displays the IP address and netmask of the network interface.
IPv6/Netmask	Displays the IPv6 address and netmask of the network interface.
Access	Displays the administrative access and phone user access that are enabled on the network interface, such as HTTPS for the web-based manager.
Status	Indicates the ***up*** (available) or ***down*** (unavailable) administrative status for the network interface. • *Green up arrow*: The network interface is up and can receive traffic. • *Red down arrow*: The network interface is down and cannot receive traffic. To change the administrative status (that is, bring up or down a network interface), see "Editing network interfaces" on page 25.

Editing network interfaces

You can edit FortiVoice Gateway'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 Gateway.

You can restrict which IP addresses are permitted to log in as a FortiVoice Gateway administrator through network interfaces. For details, see "Configuring administrator accounts" on page 31.

To create or edit a network interface

1. Go to *System* > *Network* > *Network*.
2. Double-click a network interface to modify it or select the interface and click *Edit*. If you want to create a logical interface, click *New*.

   The *Edit Interface* dialog appears.
3. Configure the following:

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

Type	If you are creating a logical interface, select which type of interface you want to create. For information about logical interface types, see "About FortiVoice Gateway logical interfaces" on page 23. • *VLAN*: If you want to create a VLAN subinterface, select the interface for which you want to create the subinterface. Then specify a port and VLAN ID. Valid VLAN ID numbers are from 1 to 4094, while 0 is used for high priority frames, and 4095 is reserved. • *Redundant*: If you want to create a redundant interface, select the interface members from the available interfaces. Usually, you need to include two or more interfaces as the redundant interface members. • *Loopback*: If you want to add a loopback interface, select the Loopback type and the interface name will be automatically reset to "loopback". You can only add one loopback interface on the FortiVoice Gateway.
Addressing Mode	• *Manual*: Select to enter the IP address or IPv6 address and netmask for the network interface in *IP/Netmask* or *IPv6/Netmask*. • DHCP: Select and click *Update Request* to retrieve a dynamic IP address using DHCP.

Advanced Settings	Enable protocols that this network interface should accept for connections ***to*** the FortiVoice Gateway itself. (These options do not affect connections that will travel ***through*** the FortiVoice Gateway.) • *HTTPS*: Enable to allow secure HTTPS connections to the web-based manager, and extension user account through this network interface. • *HTTP*: Enable to allow HTTP connections to the web-based manager, and extension user account through this network interface. • *PING*: Enable to allow ICMP ECHO (ping) responses from this network interface. • *SSH*: Enable to allow SSH connections to the CLI through this network interface. • *SNMP*: Enable to allow SNMP connections (queries) to this network interface. For information on further restricting access, or on configuring the network interface that will be the source of traps, see "Configuring the network interfaces" on page 24. • *TELNET*: Enable to allow Telnet connections to the CLI through this network interface. • *TFTP*: Enable to allow TFTP connections to the CLI through this network interface. The SIP phones connect to this server to receive the PBX setup information. • *NTP:* Enable to allow SIP phones to connect to this server to synchronize time. • *LDAP*: Enable to allow SIP phones to connect to this server to retrieve phone directories. • *SIPPNP*: Enable SIPPNP multicast function for the connected phones to find the provisioning server contained in its message for the phones. • *MDNS*: Enable MDNS multicast function for the connected phones to find the TFTP provisioning server contained in its message for the phones. This is mainly for backward support of legacy FortiFones. **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 Gateway. For information on further restricting access of administrative connections, see "Configuring administrator accounts" on page 31.

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

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

  The default value is 1500 bytes. The MTU size must be between 576 and 1500 bytes. Change this if you need a lower value; for example, RFC 2516 prescribes a value of 1492 for the PPPoE protocol.
- *Administrative status*: Select either:
  - *Up*: Enable (that is, bring up) the network interface so that it can send and receive traffic.
  - *Down*: Disable (that is, bring down) the network interface so that it cannot send or receive traffic.

4. Click *Create* or *OK*.

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 Gateway.

Static routes direct traffic exiting the FortiVoice Gateway. 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 Gateway compares the packet's destination IP address to those of the static routes and forwards the packet to the route with the large prefix match.

When you add a static route through the web-based manager, the FortiVoice Gateway 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 Gateway adds the static route.

To view or configure static routes

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

GUI field	*Description*
Destination IP/Netmask	Displays the destination IP address and subnet of packets subject to the static route. A setting of 0.0.0.0/0.0.0 indicates that the route matches all destination IP addresses.
Interface	The interface that this route applies to.
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. Select *Enable* to activate the static route.
4. In *Destination IP/netmask*, enter the destination IP address and netmask of packets that will be subject to this static route.

   To create a default route that will match all packets, enter `0.0.0.0/0.0.0.0`.
5. Select the interface that this route applies to.
6. In *Gateway*, type the IP address of the next-hop router to which the FortiVoice Gateway will forward packets subject to this static route. This router must know how to route packets to the destination IP addresses that you have specified in *Destination IP/netmask*. For an Internet connection, the next hop routing gateway routes traffic to the Internet.
7. Enter any notes you have for the route.
8. Click *Create* or *OK*.

Configuring DNS

FortiVoice Gateways 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 Gateway performance, use DNS servers on your local network.

The *DNS* tab lets you configure the DNS servers that the FortiVoice Gateway 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*.

Capturing voice and fax packets

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

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

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

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

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

To capture voice and fax packets

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

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

2. Click *New*.
3. Enter a prefix for the file generated from the captured traffic. This will make it easier to recognize the files.
4. Enter the time period for performing the packet capture.
5. If you choose *SIP* or *Use protocol* for *Filter*, from the *Available peers* field, select the extension or trunk of which you want to capture the voice packets and click -> to move them into the *Selected peers* field. You can select up to 3 peers.
6. If you want to limit the scope of traffic capture, in the *IP/Host* field, enter a maximum of 3 IP addresses or host names for the extensions and trunks you selected. Only traffic on these IP addresses or host names is captured.

7. Select the filter for the traffic capture:
   - *SIP*: Only SIP traffic of the peers you select will be captured.
   - *Use Protocol*: Only UDP or TCP traffic of the peers you select will be captured.
   - *Capture All*: All network traffic will be captured.
8. For *Exclusion*, enter the IP addresses/host names and port numbers of which you do not want to capture voice traffic.
9. Click *Create*.

Configuring administrator accounts

The *Administrator* submenu configures administrator accounts.

Configuring administrator accounts

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

By default, FortiVoice Gateway has 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*.
2. Either click *New* to add an account or double-click an account to modify it.

   A dialog appears.
3. Configure the following:

GUI field	*Description*
Enable	Click to activate the administrator status. By default, this is enabled.
Administrator	Enter the name for this administrator account. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), hyphens (-), and underscores (_). Other special characters and spaces are not allowed.
Email address	Enter the administrator's email address.
Single sign-on manager	Select the extension for the administrator account. If you add an extension, a *User portal* icon appears at the top of the web-based manager when you log into the FortiVoice unit. Clicking the icon opens the user web portal. Click *Edit* to modify the selected extension or click *New* to configure a new one. For more information on extensions, see *FortiVoice Phone System Administration Guide*.
Admin profile	Select the name of an admin profile that determines which functional areas the administrator account may view or affect. Click *New* to create a new profile or *Edit* to modify the selected profile.

Authentication type	Select an administrator authentication type: *Local* or *LDAP*.
New password	Enter this account's password. The password can contain any character except spaces. This field does not appear if *Authentication type* is *LDAP*. **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.
Confirm password	Enter this account's password again to confirm it. This field does not appear if *Authentication type* is *LDAP*.
LDAP profile	If you select *LDAP* for *Authentication type*, select an LDAP authentication profile. For more information, see "Configuring LDAP profiles" on page 119.
Trusted Hosts	Enter an IPv4 or IPv6 address or subnet from which this administrator can log in. If you want the administrator to access the FortiVoice unit from any IP address, use `0.0.0.0/0.0.0.0`. Enter the IP address and netmask in dotted decimal format. For example, you might permit the administrator to log in to the FortiVoice unit from your private network by typing `192.168.1.0/255.255.255.0`. **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 *Trusted Host #1*, *Trusted Host #2*, and *Trusted Host #3* fields. **Note:** For information on restricting administrative access protocols that can be used by these hosts, see "Editing network interfaces" on page 25. Click the + sign to add additional IP addresses or subnets from which the administrator can log in.
Select language	Select this administrator account's preference for the display language of the web-based manager.
Select theme	Select this administrator account's preference for the display theme or click *Use Current* to choose the theme currently in effect. The administrator may switch the theme at any time during a session by clicking *Next Theme*.
Department only	Select the checkbox if this is a department administrator.
Description	Select *Click to edit* to enter any comments for the administrator account.

Departments	Select the department to which the administrator belongs. This option is only available if you select *Department only*.

4. Click *Create*.

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

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

This topic includes:

Configuring the time and date

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

You can either manually set the FortiVoice Gateway system time or configure the FortiVoice Gateway 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 Gateway system time must be accurate.
FortiVoice Gateway supports daylight savings time (DST), including recent changes in the USA, Canada and Western Australia.

To configure the system time

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

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

Time zone	Select the time zone in which the FortiVoice Gateway is located. • *Automatically adjust clock for daylight saving time changes*: Enable to adjust the FortiVoice Gateway system clock automatically when your time zone changes to daylight savings time (DST) and back to standard time. When selecting time zone in CLI, use the command `config system time manual` and enter the code before the time zone in Table 1 on page 34.
Set date	Select this option to manually set the date and time of the FortiVoice Gateway's clock, then select the *Year*, *Month*, *Day, Hour*, *Minute*, and *Second* fields before you click *Apply*. Alternatively, configure *Synchronize with NTP server*.
Synchronize with NTP Server	Select to use a network time protocol (NTP) server to automatically set the system date and time, then configure *Server* and *Sync Interval*. • *Server*: Enter the IP address or domain name of an NTP server. You can add a maximum of 10 NTP servers. The FortiVoice Gateway uses the first NTP server based on the selection mechanism of the NTP protocol. Click the + sign to add more servers. Click the - sign to remove servers. Note that you cannot remove the last server. To find the NTP servers that you can use, see http://www.ntp.org. • *Sync Interval*: Enter how often, in minutes, the FortiVoice Gateway should synchronize its time with the NTP server. For example, entering 1440 causes the FortiVoice Gateway to synchronize its time once a day. Depending on your network traffic, it may take some time for the FortiVoice unit to synchronize its time with the NTP server.

3. Click *Apply*.

Table 1: Time zone codes for CLI configuration

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

Table 1: Time zone codes for CLI configuration

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

Table 1: Time zone codes for CLI configuration

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

Table 1: Time zone codes for CLI configuration

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

Configuring system options

The *System* > *Configuration* > *Option* 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* > *Option*.
2. Configure the following:

GUI field	*Description*
Idle timeout	Enter the amount of time that an administrator may be inactive before the FortiVoice Gateway automatically logs out the administrator. For better security, use a low idle timeout value.
Web action host/IP	Enter the host name or IP address from where a email notification is sent to you when a voice mail or fax is delivered to your extension. This IP address is included in the email notification. You can open the link to view or manage the voice mail or fax. If you leave this field empty, port1 IP will be used instead. The value entered here replaces the default *Url host* variable for customizing messages. See "Customizing call report and notification email templates" on page 105.
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 Gateway to send email notifications to phone users when they miss a phone call or receive a voicemail or fax.

For phone users to receive the notifications, you need to add their email addresses when configuring the extensions. See "Configuring Extensions" on page 153.

To configure email settings

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

GUI field	*Description*
Local Host	
Host name	Enter the host name of the FortiVoice Gateway, such as `FortiVoice Gateway GT02`.
Local domain name	Enter the local domain name of the FortiVoice Gateway, such as `example.com`.
Mail Queue	
Maximum time for email in queue (1-240 hours)	Enter the maximum number of hours that deferred email messages can remain in the deferred email queue, during which the FortiVoice Gateway periodically retries to send the message. After it reaches the maximum time, the FortiVoice Gateway 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 Gateway will relay outgoing email. This is typically provided by your Internet service provider (ISP), but could be a mail relay on your internal network.
Relay server name	Enter the domain name of an SMTP relay.
Relay server port	Enter the TCP port number on which the SMTP relay listens. This is typically provided by your Internet service provider (ISP).

Use SMTPs	Enable to initiate SSL- and TLS-secured connections to the SMTP relay if it supports SSL/TLS. When disabled, SMTP connections from the FortiVoice unit's built-in MTA or proxy to the relay will occur as clear text, unencrypted. This option must be enabled to initiate SMTPS connections.

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

Customize email template	View and reword the default email history report and notification email templates.

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. Expand *Administration interface*.
3. Configure the following to change appearance:

GUI field	***Description***
Product name	Enter the name of the product. This name will precede *Administrator Login* in the title on the login page of the web-based manager.
Product icon	Click *Change* to browse for the product icon. The icon should be in .ico format, and 16 pixels wide x16 pixels tall in size. Click *Reset* to return to the default setting.

Top logo	Click *Change* to upload a graphic that will appear at the top of all pages in the web-based manager. The image's dimensions must be 460 pixels wide by 36 pixels tall. For best results, use an image with a transparent background. Non-transparent backgrounds will not blend with the underlying theme graphic, resulting in a visible rectangle around your logo graphic. **Note:** Uploading a graphic overwrites the current graphic. The FortiVoice Gateway does not retain previous or default graphics. If you want to revert to the current graphic, use your web browser to save a backup copy of the image to your management computer, enabling you to upload it again at a later time. Click *Reset* to return to the default setting.
Default UI language	Select the default language for the display of the web-based manager. You can configure a separate language preference for each administrator account. For details, see "Configuring administrator accounts" on page 31.
Default theme	Select the default theme for the web-based manager GUI.

4. Click *Apply*.

Configuring advanced system settings

The *System* > *Advanced Settings* submenu lets you configure the FortiVoice Gateway location and SIP setting.

This topic includes:

Setting FortiVoice Gateway location and contact information

Identify the FortiVoice Gateway's location and its number.

To set the location

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

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

Outside line prefix	Click the default number (9) to enter the prefix for making outbound calls.
Area code	Click the default number (613) to enter the *Area code* for the main number of the FortiVoice Gateway. This code is provided by your PSTN service provider.
Required when dialing local numbers	Select this option if the area code needs to be dialed for local phone calls.
Main display name	Enter the name displaying on the FortiVoice Gateway. This name is provided by your PSTN service provider.
Main number	Enter the main number of the FortiVoice Gateway. This number is provided by your PSTN service provider.
Default prompt language	Select a new default prompt language for the FortiVoice Gateway. The default is English. To add a prompt language, click *New*. In the *Upload* field, click *Browse* to upload the language file provided by Fortinet Technical Support. Click *OK*.
Default emergency zone	Select the default emergency contact or click + to add a new one.
Default time zone	Select a new default time zone for the FortiVoice unit.

3. Click *Apply*.

Configuring SIP settings

FortiVoice Gateway supports SIP communications.

To configure SIP settings

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

GUI field	***Description***
Transport Setting	SIP communication commonly uses TCP or UDP port 5060 and/or 5061. Port 5060 is used for nonencrypted SIP signaling sessions and port 5061 is typically used for SIP sessions encrypted with Transport Layer Security (TLS). Enable the ports as required.
RTP Setting	
RTP port start	Enter the starting Real-time Transport Protocol (RTP) port that the FortiVoice Gateway will use for phone call sessions. If the unit is behind a firewall, these ports should be open. Ensure there is a reasonable port range so that you have enough ports for all open calls. The default port is 5000.

RTP port end	Enter the end RTP port that the FortiVoice Gateway will use for phone call sessions. Ensure there is a reasonable port range so that you have enough ports for all open calls. The default port is 30000.
RTP timeout	Enter the amount of time in seconds during an active call that the extension will wait for RTP packets before hanging up the call. 0 means no time limit. The default is 60.
RTP hold timeout	Enter the amount of time in seconds that the extension will wait on hold for RTP packets before hanging up the call. 0 means no time limit. The default is 300.

3. Click *Apply*.

Maintaining the system

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

This topic includes:

Maintaining the system configuration

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

Backing up configuration

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

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

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

To back up the configuration file

1. Go to *System* > *Maintenance* > *Configuration*.
2. In the *Backup* area, select *System configuration* or *User data*.

   If you choose to back up user data and the user data files are not updated, select the files to be updated and click *Prepare* first before proceeding to the next step.
3. Click *Backup*.

   Your management computer downloads the configuration file. Time required varies by the size of the file and the speed of your network connection. You can restore the backup configuration later when required. For details, see "Restoring the configuration" on page 43.

To schedule a configuration backup

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

Downloading a trace file

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

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

To download a trace file

1. Go to *System* > *Maintenance* > *Configuration* > *Trace Log*.
2. Configure *Trace Log* settings.
3. Click *Prepare* to make the trace log file ready before downloading it.
4. Click *Download trace log*.

   Your web browser downloads trace.log.gz.

Restoring the configuration

Go to *System* > *Maintenance* > *Configuration* > *Restore Configuration to* restore the backup FortiVoice Gateway configuration from your local PC. For details, see “Restoring the configuration” on page 69.

Restoring the firmware

Go to *System* > *Maintenance* > *Configuration* > *Restore Firmware* to install a FortiVoice Gateway firmware from your local PC. For details, see “Installing firmware” on page 66.

Configuring FortiVoice Gateway

Configure the FortiVoice Gateway to connect your voice and data to the outside world.

This topic includes:

Creating SIP peer for IP-PBX

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

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

GUI field	*Description*
Test	Select to test if the trunk is created successfully. For more information, see "Testing SIP trunks" on page 48.
FortiCall	Select to create a SIP trunk with Fortinet's FortiCall service. You can only create one trunk with FortiCall and use it free for 30 days or 300 minutes, whichever comes first. Note that the trial account only allows outbound calling and no international calling is available. If you sign up for the service during a trial, the trial is closed and billing will start. For more information, see "Creating a SIP trunk with FortiCall service" on page 49.
Enabled	Select to activate this trunk.
Name	The name of the VoIP service provider.
Server	The VoIP provider's domain name or IP address. For example, `172.20.120.11` or `voip.example.com`.
Port	The port for SIP sessions.

SIP Setting	The SIP profile applied to this trunk.
Status	The status of the SIP trunk. • *Not registered*: The trunk is not registered with the VoIP service provider and is not in service. • *In service*: The trunk is registered with the VoIP service provider and is in service. • *Unavailable*: The trunk is not reachable. • *Alarm detected*: There is a problem with the phone line. • *Admin down*: The trunk is disabled. • *Unmonitored*: The trunk is unknown.

To create a VoIP trunk

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

GUI field	*Description*
Name	Enter the name of the VoIP service provider.
Status	Select to activate the SIP trunk.
Display name	Enter your caller ID that will appear on the called phone, such as Example Company.
Main number	Enter the phone number that will appear on the called phone.
SIP Setting	
SIP server	Enter the VoIP provider's IP address or domain name. For example, `172.20.120.11` or `voip.example.com`.
SIP port	Most SIP configurations use TCP or UDP port 5060 for SIP sessions. If your VoIP service provider uses a different port for SIP sessions, enter the port number. If you select the *Using DNS record* option, this field is greyed out.
Using SRV record	If you entered the VoIP provider's domain name in the *SIP server* field, select this option to translate the domain name and obtain the SIP port. You can only select this option if your VoIP provider uses the same setting.
User name	Enter the user name provided by the VoIP service provider for the FortiVoice Gateway to register with the SIP server.
Password	Enter the password provided by the VoIP service provider for the FortiVoice Gateway to register with the SIP server.

Auth. user name	Some VoIP providers may provide you with an authentication user name that is different from your user name for the FortiVoice Gateway to register with the SIP server. If tat is the case, enter the authentication user name here.
Realm/domain	Some VoIP service providers' SIP servers authenticate the PBXes that register with them by requesting the name of the host performing the authentication. If this is the case with your VoIP service provider, enter the name of the host performing the authentication provided by your VoIP service provider.
SIP setting	Select the SIP profile to apply the supported phone features and codecs for the trunk. To match the information of the VoIP service provider, you can edit the existing profile or click *New* to add a new one. For more information, see "Configuring SIP profiles" on page 49.
Max channel	Each trunk contains multiple channels. The number of channels you can have in a trunk is controlled by your VoIP service provider. Consult your VoIP service provider for the maximum of channels that you can set to limit the number of concurrent calls. For example, if you want to allow six calls at a time, enter 6.
Overflow check	If selected, the phone calls exceeding the *Max channel* limit will be handled according to the call handling actions set in the dialplan applied to this trunk. If unselected, the phone calls exceeding the *Max channel* limit will be disconnected.
Max outgoing channel	With known max channels, if you need to reserve incoming channels, you may enter the number of outgoing channels allowed and the remaining channels are for incoming calls. For example, the max channel number is 10 and you want to reserve 4 channels for incoming calls, you can enter 6 for *Max outgoing channel*.
User=Phone in SIP URI	Select if your service provider requires this option to make the FortiVoice Gateway to be compatible with the VoIP service provider's configurations.
Caller ID modification	Select if you want the trunk main number to appear on the called phone. See "Main number" on page 45. Otherwise, the user name provided by the VoIP service provider for the FortiVoice Gateway to register with the SIP server will appear on the called phone. See "User name" on page 45.
Inband ringtone	Select to enable the FortiVoice Gateway to send ring tone to the caller of an incoming call before the establishment of a call connection.

Registration	Enter the SIP registration information from the VoIP service provider by selecting a registration method. You can receive calls after registering with the SIP server of the VoIP service provider.
	• *Disable*: Select to deactivate the registration with the VoIP service provider.
	• *Standard*: Select to use the standard registration method which automatically registers with the SIP server of the VoIP service provider.
	• *Registrar*: Select to enter the registration information from the VoIP service provider:
	  • *Registrar host/IP*: Enter the VoIP service provider's SIP registration server domain name or IP address. For example, `172.20.120.11` or `voip.example.com`.
	  • *Registrar port:* Most SIP configurations use TCP or UDP port 5060 for SIP sessions. If your VoIP service provider uses a different port for SIP sessions, enter the port number.
	  • *Transport protocol*: Select the transport protocol used for the registration.
	• *Registration URI*: Enter the registration string provided by the VoIP service provider in the *Registration URI* field.
	  The string usually has the following formats:
	  `register => user[:secret[:authuser]]@host [:port][/extension]`
	  or
	  `register => fromuser@fromdomain:secret@host`
	  or
	  `register => fromuser@fromdomain:secret: authuser@host:port/extension`
	  For example, a string could be: `register => 2345:password@mysipprovider.com/1234`
	• *Registration interval*: Enter the time interval in minutes to register with the SIP server of the VoIP service provider.

Outbound Proxy	Some VoIP service providers use proxy servers to direct its traffic. If this is the case, your registration request will go to the proxy server first before reaching the registration server. Configure the following: • Select to activate the proxy server settings. • *Proxy (Host/IP)*: Enter the proxy server's domain name or IP address. For example, `172.20.120.11` or `voip.example.com`. • *Proxy port*: Enter the port number of the proxy server. • *Transport protocol*: Select the transport protocol used for the registration.
Fax	Configure fax signal automatic detection and fax handling.

Automatic fax detection	Select for the FortiVoice Gateway to detect incoming fax signal on this trunk automatically. Selecting this option may delay the call response time on this trunk.
Forward fax to eFax account	Some incoming faxes' numbers do not match those of your eFax accounts. Selecting this option and a fax receiving account will send the faxes to the fax account. This option is only selectable if *Automatic fax detection* is selected.
Phone Number	Click *New* to add the phone number provided by your VoIP service provider. The VoIP service provider SIP server will direct calls from external callers directly to this number. You can add multiple numbers.

4. Click *Create*.

Testing SIP trunks

After you create a SIP trunk, you can select the trunk and click *Test* to see if the trunk works.

For more information, see "Test" on page 44.

To test a SIP trunk

1. Go to *Gateway* > *SIP* > *SIP.*
2. Select the trunk that you want to test and click *Test*.
   The *System Configuration Test* page appears.
3. Configure the following:

GUI field	*Description*
Test Call - Dry Run	Run a system SIP trunk test without making a real phone call.
Destination number	Enter a destination number to call.
From number	Enter the number from which you want to call the destination number. The FortiVoice Gateway will connect this number with the destination number for the test.
Test	Click to start the dry run test and check the *Test result*.
Reset	Click to remove the test result in order to start a new test.
Test Call	Test the SIP trunk by making a real phone call.
Destination number	Enter a destination number to call.

After call is established	Select the FortiVoice Gateway action once it calls the destination number: • *Play welcome message*: The FortiVoice Gateway will play a message to the destination number. • *Connect test call to number*: In the *Number* field, enter the number from which you want to call the destination number. The FortiVoice Gateway will connect this number with the destination number to test the trunk.
Test	Click to start the test and check the *Test result*.
Reset	Click to remove the test result in order to start a new test.

Creating a SIP trunk with FortiCall service

You can create one trunk with FortiCall and use it free for 30 days or 300 minutes, whichever comes first. Note that the trial account only allows outbound calling and no international calling is available.

If you sign up for the service during a trial use, the trial is closed and billing will start.

To create a SIP trunk with FortiCall service

1. Go to *Trunk* > *VoIP* > *SIP.*
2. Click *FortiCall*.

   The *Create SIP Trunk* dialog box displays.
3. Note down the *MAC Address* and *System ID* for use if you decide to sign up for the service later.
4. Keep *Create dialplans for this trunk* selected unless you want to create the dialplans by yourself.

   The auto-generated dialplans will replace the default inbound, outbound, and emergency call dialplans. You can delete them if you do not choose to use the FortiCall service.
5. Click *OK*.
6. Enter your name, email address, and reseller or partner code.
7. Click *Create*.
8. Click *OK*.

   The FortiCall trunk is created.

Configuring SIP profiles

Configure the SIP related settings and codecs and apply them to SIP trunks.

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

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

To configure a SIP profile

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

GUI field	*Description*
Name	Enter a name for this profile.
DTMF	Select the dual-tone multi-frequency (DTMF) method used by the VoIP provider. Options are RFC2833, Inband, Info, Shortinfo, and Auto. Auto means the VoIP provider's server and the FortiVoice Gateway will negotiate to select a DTMF method. You could also select a specific DTMF method if required.
Monitor/Keep alive (SIP notify) interval	Enter the time interval in seconds for the FortiVoice Gateway to talk to the SIP server of your service provider to keep the connectivity and check its capability. 0 means no checking by the FortiVoice Gateway.
NAT	Select if the VoIP service provider supports SIP NAT translation.
Video	Select if the service provider supports video calling over SIP.
T.38	Select if the VoIP service provider supports fax over VoIP network.
Transport	*Transport*: SIP commonly uses TCP or UDP port 5060 and/or 5061. Port 5060 is used for non-encrypted SIP signaling sessions and port 5061 is typically used for SIP sessions encrypted with Transport Layer Security (TLS). Enable the protocols as required. *Secure RTP*: Select to provide encryption, message authentication and integrity, and replay protection to the FortiVoice Gateway Real-time Transport Protocol data.
Codec	Select the codecs supported by the VoIP service provider. Among the selected ones, choose the preferred one for the VoIP provider. The preferred codec is usually the most used one in your area and provides the best quality of communication. If your preferred codec is different from that of your VoIP service provider, the service provider's codec will be used as long as it is one of your supported codecs.

3. Click *Create*.

Modifying analog trunks (GO08 only)

The analog FXO (Foreign eXchange Office) ports connect your FortiVoice Gateway to your PSTN service providers and through them to the outside world.

To view the analog trunks, go to *Gateway* > *Analog.*

GUI field	*Description*
Enabled	Select to activate the trunk.
Name	The name of the trunk.
Status	The trunk statuses, including: • *In service:* The trunk is currently in use. • *Not activated:* The trunk is not enabled. • *Idle*: The trunk is not in use. • *Unavailable*: The trunk is not reachable. • *Conflict*: The trunk conflicts with another one. • *Alarm detected*: There is a problem with the trunk. • *Admin down*: The trunk is disabled.
Type	The trunk type: analog.

To add an analog trunk

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

GUI field		*Description*
Trunk Setting		
	Name	Enter a name for the trunk.
	Enable	Select to activate the trunk.
	Display name	Enter your caller ID that will appear on the called phone, such as Example Company.
	Number	Enter the phone number that will appear on the called phone.
	Relay FAX	Select if you want the extension to relay fax.
Hardware Property		
	analog1	Use this option to configure the analog trunk. Click *Edit* to configure the PSTN analog settings to match the same settings of your PSTN service provider. Click *OK* after finishing the configuration.
	Port	Select the FXO ports you want for this trunk and click -> to move them into the *Selected ports* field. Each FXO port selected provides a connection for this particular analog trunk profile. For example: if 4 FXO ports have been selected, this particular profile could allow up to 4 PSTN connections.
	Max channel	Displays the number of FXO ports that have been selected, and are available to receive incoming and outgoing calls.

	Max outgoing channel	Defines how many of the FXO ports available can be used for outbound calls at one time.
Fax		Configure fax signal automatic detection and fax handling.
	Automatic fax detection	Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically. Selecting this option may delay the call response time on this trunk.
	Forward fax to eFax account	Some incoming faxes' numbers do not match those of your eFax accounts. Selecting this option and a fax receiving account will send the faxes to the fax account. This option is only selectable if *Automatic fax detection* is selected.
Phone Number		Click *New* to add the phone number provided by your PSTN service provider. Your PSTN service provider will direct calls from external callers directly to this number. You can add multiple numbers.

4. Click *Create*.

Modifying analog extensions (GS16 only)

The analog FXS (Foreign eXchange Subscriber) ports connect your FortiVoice Gateway to your PSTN service providers and through them to the outside world.

The FortiVoice Gateway has 16 analog ports and 16 default analog extensions. You can edit the extensions' default configuration.

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

To edit the default analog extension

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

GUI field	*Description*
Number	Enter the extension number following the extension number pattern.
User ID	This is the system-generated ID for the extension and is read-only.
Analog port	Enter the analog port number. By default, it is *fxs1*.
Enabled	Select to activate the extension.
Display name	Enter the name displaying on the extension. This is usually the name of the extension user.
Description	Add any notes for the extension.

User Settings	
Management	Configure the extension's role in other settings.
User privilege	Select the services for the extension. Click *Edit* to modify the current user privilege or click *New* to configure a new one.
Department	Select the department that the extension belongs to. Click *Edit* to modify the current department or click *New* to configure a new one.
Survival branch	Select the local survival branch FortiVoice unit for the extension if the extension is in a local survivability network. Click *Edit* to modify the current branch unit.
Voicemail	Configure the extension's voice mailbox. In some cases, you may want other users or groups to share this voice mailbox. For example, a supervisor wants his/her co-workers to access his/her voice mailbox while he/she is away. *Main voice mailbox:* Select the extension's own voice mailbox (*Default*) or that of another extension as the voice mailbox of this extension. Typically, you use the default mailbox. If you select the voice mailbox of another extension, you can click *Edit* to modify that extension. *Users/Groups*: The FortiVoice Gateway turns on the message waiting light on the phones of a user or user group to notify the user or group of a new voice message stored in the voice mailbox associated with this extension. To select users or user groups, under *User(s)* and *Group(s)*, select the users/groups from the *Available* field and click -> to move them to the *Selected* field. To listen to the message after being notified, the user can dial *97 or the code you set and enter the user's own user PIN.
Advanced	Click to configure desktop phone: • *MWI* (Message Waiting Indication): Enable or disable MWI on the phone. • *Auto answer*: Enable or disable automatic answering on the phone. • *Direct call*: Enable or disable direct calling on the phone.
Web Access	Configure web user portal and soft client access from mobile or desktop devices.
Authentication type	Select the extension's authentication type: *Local* or *LDAP*.

User password	Enter the password for user web portal access which can be much longer and stronger to mitigate the risk of password guess attack and preserve the User PIN for phone access only. Control of using personal password or voicemail PIN to access user web portal is set when configuring phone system capacity. You can check the password strength. Click *Generate* to generate a strong password automatically. Select *View password* to display the password. This option is only available when you select *Local* for *Authentication Type*.
LDAP profile	If you select *LDAP* for *Authentication type*, select an LDAP profile to apply to this extension. You can click *New* to create a new profile or *Edit* to modify the selected one.
Authentication ID	If you select *Try common name with base DN as bind DN* as the user authentication option in the authentication profile you select, enter the authentication ID based on the user objects' common name attribute you entered in the *Common name ID* field of the profile, such as `jdoe`. If you select *Search user and try bind DN* as the user authentication option in the authentication profile you select, leave this field blank. This option is only available if you select *LDAP* for *Authentication type*.
Phone Access	Configure voicemail access by phone or access to restricted phone calls.
Voicemail PIN	Enter the password for the extension user to access voicemail and the user web portal. Selection of using personal password or voicemail PIN to access user web portal is set when configuring phone system capacity. You can check the PIN strength. Click *Generate* to generate a strong password automatically. Select the view PIN icon to display the password. If you have configured the default user PIN, the password appears here. However, you can change it.
Personal code	Enter the extension specific account code that can be used to restrict calls. This code is needed to make some restricted calls. You can click *Generate* to get a code.

4. Click *OK*.

Modifying PRI trunks (GT01 & 02 only)

FortiVoice Gateway Primary Rate Interface (PRI) carries multiple DS0 voice and data transmissions to your PRI service providers and through them to the outside world.

To view the PRI trunks, go to *Gateway* > *PRI.*

GUI field	*Description*
Enabled	Select to activate the trunk.
Name	The name of the trunk.
Status	The trunk statuses, including: • *In service:* The trunk is currently in use. • *Not activated:* The trunk is not enabled. • *Idle*: The trunk is not in use. • *Unavailable*: The trunk is not reachable. • *Conflict*: The trunk conflicts with another one. • *Alarm detected*: There is a problem with the trunk. • *Admin down*: The trunk is disabled.
Type	The trunk type: analog.

To add a PRI trunk

1. Go to *Gateway* > *PRI.*
2. Click *New*.
3. Configure the following:

GUI field		*Description*
Trunk Setting		
	Name	The name of this trunk. This is view only.
	Enable	Select to activate the trunk.
	Display name	Enter your caller ID that will appear on the called phone, such as Example Company.
	Number	Enter the phone number that will appear on the called phone.
	Relay FAX	Select if you want the extension to relay fax.
Hardware Property		Use this option to configure the T1/E1 span. Spans represent trunks (spans) of T1/E1 PSTN lines. The FortiVoice unit supports T1/E1 lines according to the installed voice card. You can add a span name using the CLI.
	Edit span	Select the span you want to modify and click the *Edit* icon. For more information, see “Configuring the T1/E1 span” on page 56.

	Span	Use this option to configure the PRI trunk. Select a span in the *Available* field and click -> to move it into the *Selected* field.
	Max channel	Indicates the total number of B channels of the spans.
	Max outgoing channel	Enter the number of outgoing channels out of the maximum number of B channels.
Fax		Configure fax and phone signal automatic detection and fax handling.
	Automatic fax detection	Select for the FortiVoice unit to detect incoming fax signal on this trunk automatically.
	eFax account	Select the fax receiving account for the detected faxes.
Phone Number		Click *New* to add the phone number provided by your PSTN service provider. Your PSTN service provider will direct calls from external callers directly to this number. You can add multiple numbers.

4. Click *OK*.

Configuring the T1/E1 span

You can configure the settings of the T1/E1 span, including full or fractional PRI (T1/E1), to match the same settings of your PSTN service provider.

For GT02, if a PRI trunk includes two spans, the configuration of the second span is much simpler as the spans share many configurations.

For more information, see "Hardware Property" on page 55.

To configure the T1/E1 span

1. Go to *Gateway* > *PRI.*
2. Select a span name and click *Edit*.
3. For *Edit span* under *Hardware Property*, select a span and click the *Edit* icon.
4. Configure the following:

GUI field	***Description***
Standard Options	
Name	The name of this span. This is view-only.
Type	Select the span type: *PRI T1* or *PRI E1*. A T1 span usually supports 23+1 channels, while an E1 span supports 30 channels in CAS (Channel Associate Signaling) mode and 30 B channels and one D channel in ISDN mode.

	Signalling	Select the signaling type of the ISDN PRI: • *PRI signalling, CPE* (Customer Premises Equipment) *side* • *PRI signalling, Network Side* • *PRI R2 signalling*
Advanced Options		
	Framing and coding option	Specify the type of framing and coding to provision the PRI with your PSTN service provider.
	Clocking options	Select the FortiVoice unit's clock synchronization: • Clock sourcing from PSTN network • Internal clocking source This option does not need to match that of your PSTN service provider.
	Receive sensitivity	Select the level of receiver sensitivity which is the ability of the phone receiver to pick up the required level of phone signals to make it operate more effectively within its application. This option does not need to match that of your PSTN service provider.
	D-channel signalling format	Select a signalling method for the D channel which is a signalling channel and carries the information needed to connect or disconnect calls and to negotiate special calling parameters (for example, automatic number ID, call waiting, data protocol). The D channel can also carry packet-switched data using the X.25 protocol.
	Line build out	Select the line build out (LBO). LBO settings are an inherent part of T1 and T3 network element transmission circuitry. Since cable lengths between network elements and digital signal cross-connect (DSX) vary in the central office, LBO settings are used to adjust the output power of the transmission signal to achieve equal level point (ELP) at the DSX.
	D-channel	By default, depending on your selection of "Type" on page 56, the typical channel numbers are: • Full T1: 24 • Full E1: 16 You can also set the channel numbers to others such as 1. The settings you configure must match the same settings of your PSTN service provider.

	B-channel	By default, depending on your selection of "Type" on page 56, the typical channel settings are: • Full T1: 1-23 • Full E1: 1-15, 17-31 You can also configure the fractional channel numbers. For example, for T1/E1, the channels can be: • 1-12 • 2, 3, 4, 9-15 • 2-4, 9-15 The settings you configure must match the same settings of your PSTN service provider.
PRI R2 Settings		Since there is no single signaling standard for R2, the FortiVoice Gateway addresses this challenge by supporting many localized implementations of R2 signaling. This option is active only if you select PRI R2 signalling for "Signalling" on page 57.
	Country	Select the country for PRI R2 settings.
	Max ANI digits	ANI (Automatic Number Identification) is a system used by telephone companies to identify the DN (Directory Number) of a calling subscriber. It allows subscribers to capture or display caller's telephone number. Enter the number of digits of a caller's phone number to be captured.
	Max DNIS digits	Dialed Number Identification Service (DNIS) is a service provided by telephone companies that lets the subscribers determine which telephone number was dialed by a caller. Enter the number of digits of a dialed call to be sent by the telephone company.
	Caller category	Select the caller type.
	Incoming digits mode	Select the incoming digits mode by consulting your telephone company.
	DTMF dialing	Select to enable dual-tone multi-frequency signaling (DTMF) dialing.
	DTMF answering	Select to enable dual-tone multi-frequency signaling (DTMF) answering.
	Allow collect calls	Select to allow collect calls.

5. Click *OK*.

Mapping a SIP peer with the FortiVoice Gateway

Mapping Rule allows for calls to be made from a SIP peer to the FortiVoice Gateway and then out on an analog trunk. Likewise, calls can come in on an analog trunk and be answered through the SIP peer. When creating a mapping rule, you are linking the analog trunks to the SIP peer or link analog extensions to SIP peers, depending on the platform.

To add a mapping rule

1. Go to *Gateway* > *Mapping Rule.*
2. Click *New*.
3. Configure the following:

GUI field	*Description*
Enabled	Select to activate the rule.
PSTN trunk (GO08 only)	Select the analog trunk profile that you want to map to the SIP peer.
SIP peer	Select the SIP trunk profile that you want to map to the PSTN trunk.
PRI trunk (GT01 & 02 only)	Select the PRI trunk profile that you want to map to the SIP peer.
Extension (GS16 only)	Select the analog extension that you want to map to the SIP peer.
Comments	Enter any comments you have for this mapping rule.

4. Click *Create*.

Configuring Logs

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

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

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

This topic includes:

About FortiVoice Gateway logging

FortiVoice Gateway can log multiple events. See “FortiVoice Gateway log types” on page 60.

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 60.

A FortiVoice Gateway can save log messages to its hard disk.

This topic includes:

FortiVoice Gateway log types

FortiVoice Gateway can record the following types of log messages. You can view and download these logs from the *Logs* submenu of the *Status* tab.

Table 2: Log types

Log type	Description
System	Includes system and administration events, such as downloading a backup copy of the configuration.
Mail	Includes SMTP server events.
Voice	Includes phone calls events.
DTMF	Includes DTMF (Dual Tone Multi-Frequency) 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 3: Log severity levels

Levels	Description
0 - Emergency	Indicates the system has become unusable.
1 - Alert	Indicates immediate action is required.
2 - Critical	Indicates functionality is affected.
3 - Error	Indicates an error condition exists and functionality could be affected.
4 - Warning	Indicates functionality could be affected.
5 - Notification	Provides information about normal events.
6 - Information	Provides general information about system operations.
6 - Debug	Provides information useful to debug a problem.

For each location where the FortiVoice Gateway can store log files, you can define the severity threshold of the log messages to be stored there.

Avoid recording log messages using low severity thresholds such as Information or Notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

The FortiVoice Gateway stores all log messages equal to or exceeding the severity level you select. For example, if you select *Error*, the FortiVoice Gateway stores log messages whose severity level is *Error*, *Critical*, *Alert*, or *Emergency*.

Configuring logging

The *Log Settings* submenu lets you:

- set the severity level
- configure which types of log messages to record

This section includes the following topics:

Configuring logging to the hard disk

You can store log messages locally on the hard disk of the FortiVoice Gateway.

To ensure that the local hard disk has sufficient disk space to store new log messages and that it does not overwrite existing logs, you should regularly download backup copies of the oldest log files to your management computer or other storage, and then delete them from the FortiVoice Gateway.

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 Gateway's system time is accurate. For details, see "Configuring the time and date" on page 33.

To configure logging to the local hard disk

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

2. Select *Enabled* 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 Gateway 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 Gateway will do when the local disk is full and a new log message is caused, either:
   - *Do not log*: Discard all new log messages.
   - *Overwrite*: Delete the oldest log file in order to free disk space, and store the new log message.
8. In *Logging Policy Configuration*, click the arrow to review the options and enable the types of logs that you want to record to this storage location. For details, see "Log types" on page 60.
9. Click *Apply*.

Configuring alert email

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

To set up alerts, you must configure both the alert email recipients (see "Configuring alert recipients" on page 63) and which event categories will trigger an alert email message (see "Configuring alert categories" on page 63).

Alert email messages also require that you supply the FortiVoice Gateway with the IP address of at least one DNS server. The FortiVoice Gateway uses the domain name of the SMTP server to send alert email messages. To resolve this domain name into an IP address, the FortiVoice Gateway must be able to query a DNS server. For information on DNS, see "Configuring DNS" on page 29.

This section contains the following topics:

Configuring alert recipients

Before the FortiVoice Gateway can send alert email messages, you must create a recipient list.

To configure recipients of alert email messages

1. Go to *Log & Report* > *Alert* > *Configuration*.

GUI field	*Description*
Test (button)	Clicking on the button will send a test alert email to all configured recipients in the list.
Alert Email Account	Displays the names of email accounts receiving email alerts.

2. Click *New* to add the email address of a recipient.
3. In *Email to*, enter a recipient email address.
4. Click *Create*.
5. Repeat the previous steps to add more users.

Configuring alert categories

Before the FortiVoice Gateway can send alert email messages, you must specify which events cause the FortiVoice Gateway to send an alert email message to your list of alert email recipients (see “Configuring alert recipients” on page 63).

To select events that will trigger an alert email message

1. Go to *Log & Report* > *Alert* > *Category*.
2. Select one or more of the following event categories check boxes:

Table 4: Alert email category choices

GUI field	*Description*
Critical events	Send an alert email message when the FortiVoice Gateway unit detects a system error that may affect its operation.
Disk is full	Send an alert email message when the hard disk of the FortiVoice Gateway unit is full.
FXO alarm	Send an alert email when the PSTN analog line has a problem. This option is not available for every FortiVoice model.
Trunk lines are saturated	Send an alert email when the SIP/PSTN/PRI trunk lines are fully occupied. SIP trunk alert only works if you select *Overflow check* when configuring SIP trunk.
SIP trunk/office peer connectivity alert	Select the trunks of which an alert email is sent when a trunk has an issue. Also set the time interval for sending alert email in seconds.

3. Click *Apply*.

Installing firmware

Fortinet periodically releases FortiVoiceGateway firmware updates to include enhancements and address issues. After you have registered your FortiVoiceGateway, FortiVoiceGateway 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 FortiVocie Gateway, you must first register your FortiVocie Gateway 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

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 FortiVocie Gateway.

To test a new firmware image

1. Connect your management computer to the FortiVocie Gateway console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
2. Initiate a connection from your management computer to the CLI of the FortiVocie Gateway.
3. Connect port1 of the FortiVocie Gateway 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 FortiVocie Gateway can reach the TFTP server.

   To use the FortiVocie Gateway 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 FortiVocie Gateway:

   ```
   execute reboot
   ```

6. As the FortiVocie Gateway 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 FortiVocie Gateway reboots and you must log in and repeat the `execute reboot` command.

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

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

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

7. Type `G` to get the firmware image from the TFTP server.

   The following message appears:

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

8. Type the IP address of the TFTP server and press Enter.

   The following message appears:

   ```
   Enter Local Address [192.168.2.99]:
   ```

9. Type a temporary IP address that can be used by the FortiVocie Gateway 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 FortiVocie Gateway 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 FortiVocie Gateway 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 66.
    - If the new firmware image does ***not*** operate successfully, reboot the FortiVocie Gateway 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 FortiVocie Gateway.

Administrators whose access profile contains *Read-Write* access in the *Others* category, such as the `admin` administrator, can change the FortiVocie Gateway 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 `FortiVocie Gateway 2.00,build0082,120827`, changing to `FortiVocie Gateway 2.00,build0081,120801`, an earlier build number and date, indicates that you are reverting.

Reverting to an earlier version may cause the FortiVocie Gateway 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 70.

Therefore, no matter if you are upgrading or downgrading, it is always a good practice to back up the configuration and call data. For details, see “Backing up configuration” on page 42.

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 manger as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
4. Install firmware in one of two ways:
   - Go to *Status* > *Dashboard* > *Dashboard*, and in the *System Information* widget, 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 FortiVocie Gateway. The FortiVocie Gateway 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 FortiVocie Gateway reverts the configuration to default values for that version of the firmware. You must either reconfigure the FortiVocie Gateway 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 *Status* > *Dashboard* > *Dashboard*. 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 FortiVocie Gateway console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
4. Initiate a connection from your management computer to the CLI of the FortiVocie Gateway, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
5. Connect port1 of the FortiVocie Gateway 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 FortiVocie Gateway can reach the TFTP server.

   To use the FortiVocie Gateway 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 FortiVocie Gateway:

   ```
   execute restore image tftp <name_str> <tftp_ipv4>
   ```

   where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.2.99, enter:

   ```
   execute restore image tftp image.out 192.168.2.99
   ```

   One of the following messages appears:

   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```

   or:

   ```
   Get image from tftp server OK.
   Check image OK.
   This operation will downgrade the current firmware version!
   Do you want to continue? (y/n)
   ```
9. Type `y`.

   The FortiVocie Gateway downloads the firmware image file from the TFTP server. The FortiVocie Gateway 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 FortiVocie Gateway reverts the configuration to default values for that version of the firmware. You must either reconfigure the FortiVocie Gateway 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 FortiVocie Gateway using its default IP address for port1, 192.168.1.99, and restore the configuration file. For details, see "Reconnecting to the FortiVocie Gateway" on page 68 and "Restoring the configuration" on page 69.

    If you have upgraded the firmware version, to verify the conversion of the configuration file, see "Verifying the configuration" on page 70. If the upgrade is unsuccessful, you can downgrade the firmware to a previous version.

Reconnecting to the FortiVocie Gateway

After downgrading to a previous firmware version, the FortiVocie Gateway reverts to default settings for the installed firmware version, including the IP addresses of network interfaces through which you connect to the FortiVocie Gateway web-based manager and/or CLI.

If your FortiVocie Gateway 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 FortiVocie Gateway to its default configuration in order to reconnect using the default network interface IP address. For more information, see “Clean installing firmware” on page 71.

To reconnect using the CLI

1. Connect your management computer to the FortiVocie Gateway console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
2. Start HyperTerminal, enter a name for the connection and click *OK*.
3. Configure HyperTerminal to connect directly to the communications (COM) port on your computer and click *OK*.
4. Select the following port settings and click *OK*:

   Table 5: Port settings

Bits per second	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

5. Press Enter to connect to the FortiVocie Gateway 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 69.

Restoring the configuration

You can restore a backup copy of the configuration file from your local PC using either the web-based manager or CLI. For information about configuration backup, see "Backing up configuration" on page 42.

If you have just downgraded or restored the firmware of the FortiVocie Gateway, restoring the configuration file can be used to reconfigure the FortiVocie Gateway 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 FortiVoiceGateway 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 70.

To restore the configuration file using the CLI

1. Initiate a connection from your management computer to the CLI of the FortiVocie Gateway, 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 FortiVocie Gateway 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 FortiVocie Gateway can reach the TFTP server.

   To use the FortiVocie Gateway 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 FortiVoiceGateway 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 70.

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 FortiVocie Gateway, 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 FortiVocie Gateway using the web-based manager or the CLI
- you want to install firmware ***without*** preserving any existing configuration
- a firmware version that you want to install requires that you format the boot device (see the Release Notes accompanying the firmware)

Unlike upgrading or downgrading firmware, clean installing firmware re-images the boot device. Also, a clean install can only be done during a boot interrupt, before network connectivity is available, and therefore requires a local console connection to the CLI. ***A clean install cannot be done through a network connection.***

Back up your configuration before beginning this procedure, if possible. A clean install resets the configuration, including the IP addresses of network interfaces. For information on backups, see "Backing up configuration" on page 42. For information on reconnecting to a FortiVocie Gateway whose network interface configuration has been reset, see "Reconnecting to the FortiVocie Gateway" on page 68.

If you are reverting to a previous FortiVocie Gateway 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 FortiVocie Gateway console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
3. Initiate a ***local console connection*** from your management computer to the CLI of the FortiVocie Gateway, and log in as the `admin` administrator, or an administrator account that has system configuration read and write privileges.
4. Connect port1 of the FortiVocie Gateway 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 FortiVocie Gateway can reach the TFTP server.

   To use the FortiVocie Gateway 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 FortiVocie Gateway:

   ```
   execute reboot
   ```

   or power off and then power on the FortiVocie Gateway.
8. As the FortiVocie Gateway 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 FortiVocie Gateway 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 FortiVocie Gateway 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 FortiVocie Gateway 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 FortiVocie Gateway downloads the firmware image file from the TFTP server. The FortiVocie Gateway installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.

    The FortiVocie Gateway 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 FortiVocie Gateway or restore the configuration file from a backup. For details, see “Restoring the configuration” on page 69.

Index

K

L

M

N

P

R

S

T

U

V

W