FortiVoice - Cookbook

Version 6.0.9

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 18, 2021
FortiVoice 6.0.9 Cookbook
26-609-590401-20210618

TABLE OF CONTENTS

Change log **6**
Introduction **7**
Auto dialer **8**
Setting up and starting an auto dialer campaign 8
Enabling the auto dialer service 8
Adding contacts 8
Configuring an audio message 9
Configuring the auto dialer campaign 9
Starting an auto dialer campaign 9
Call center **10**
Call center setup 10
Creating a call queue 10
Configuring departments 12
Skill-based routing 13
Creating skill sets 13
Configuring skill levels 13
Assigning a skill level to an extension 14
Configuring the call queue 15
Configuring call handling 16
Call features **18**
Auto attendant 18
Configuring the auto attendant 18
Configuring key actions 19
Configuring advanced settings (optional) 20
Call parking 20
Configuring call parking settings 20
Configuring call parking on programmable phone keys 21
Using call parking 23
Call recording 24
Recording a phone call 24
Conference calls 25
Configuring user conferencing 26
Scheduling a user conference 26
Viewing upcoming user conferences 29
Configuring administrator conferencing 30
Faxes 32
Configuring FortiVoice to receive faxes 33
Configuring fax archive settings 33
Configuring FortiVoice to send faxes 34
Configuring general fax settings 34
Speed dial numbers 35
Extensions **36**
Auxiliary phone and secondary account 36
Adding an auxiliary phone 36

Adding a secondary account ... 36
Auto provisioning for FortiFone devices on different subnets ... 37
Downloading and editing the CSV file ... 37
Importing the CSV file ... 38
Configuring HTTP or HTTPS protocol support ... 39
Configuring your DHCP server ... 40
Caller ID modification ... 40
Caller ID modification hierarchy for normal calls ... 41
Caller ID modification hierarchy for emergency calls ... 44
FortiVoice Click-to-dial configuration on Google Chrome ... 48
Installing FortiVoice Click-to-dial ... 49
Configuring FortiVoice Click-to-dial ... 50
Using FortiVoice Click-to-dial ... 51
Hot desking ... 52
Configuring hot desking ... 52
Using hot desking on FortiFone ... 54
Viewing activity details of hot-desking extensions ... 54
Local IP extensions ... 55
Configuring extension settings ... 55
Configuring notification options ... 58
Remote extension configuration ... 59
Adding a remote extension ... 59
Testing a remote extension ... 59
High availability ... 60
Planning high availability ... 60
Configuring high availability on FortiVoice units ... 61
Configuring service-based failover ... 63
Synchronizing configuration and data in a FortiVoice HA group ... 64
Installing licenses on a FortiVoice HA group ... 64
Enabling high availability activity logging ... 65
Displaying the high availability status ... 65
Hotel management ... 67
Configuring PMS settings ... 67
Configuring hotel management options ... 68
Defining minibar codes ... 69
Configuring room status ... 69
Licensing ... 71
Purchasing a FortiVoice product license ... 71
Registering a FortiVoice product and downloading the license file ... 71
Uploading the license file to FortiVoice ... 72
Managed system ... 73
Gateway management ... 73
FortiVoice units as survivable branches ... 73
FortiFone firmware upgrades ... 74
Reviewing the current FortiFone firmware ... 74
Uploading the FortiFone firmware to FortiVoice ... 74

Scheduling the firmware upgrade 75
Confirming the firmware upgrade 75
Phone system **76**
Emergency numbers 76
Configuring the emergency number 76
Configuring an outbound dialplan for emergency calls 77
LDAP authentication configuration for extension users 77
Creating an LDAP profile 78
Applying the LDAP profile to an extension 79
Schedules – best practices 79
Creating schedules 80
Configuring call handling with schedules 87
Security **90**
Changing the default external access ports 90
Changing the default passwords 91
Disabling recommended features 96
Configuring additional settings 97
Monitoring and reporting 102
Softclient **105**
Deployment of FortiFone softclient for mobile 105
Protocols 105
Call flows 106
Topology 107
Workflow for deployment using SIP over TLS 107
Workflow for deployment using SIP over TCP or UDP 107
Configuring FortiFone softclient for mobile on FortiVoice 108
Configuring FortiGate for SIP over TLS 113
Configuring FortiGate for SIP over TCP or UDP 121
Installing and configuring the FortiFone softclient for mobile 128
Deployment of FortiFone softclient for desktop 129
Protocols 129
Call flows 129
Workflow 129
Configuring FortiFone softclient for desktop settings on FortiVoice 130
Configuring the ICE support 133
Creating virtual IP addresses on FortiGate 134
Configuring a FortiGate firewall policy for port forwarding 137
Installing and configuring the FortiFone softclient for desktop 139

Change log

Date	Change description
2021-06-03	Initial release of the FortiVoice 6.0.9 Cookbook.
2021-06-17	Added the Deployment of FortiFone softclient for desktop on page 129.
2021-06-18	Updated Configuring the ICE support on page 133.

Introduction

The FortiVoice Cookbook is a collection of recipes about configuring and using FortiVoice features.

A recipe focuses on a task that you can perform using the FortiVoice web-based manager. A few tasks described in this document use the CLI or user portal, as required.

Auto dialer

The FortiVoice auto dialing system can assist your organization in reaching multiple contacts quickly and efficiently.

This section includes the following recipe:

- Setting up and starting an auto dialer campaign on page 8

Setting up and starting an auto dialer campaign

An auto dialer campaign allows you to broadcast a recorded message to the dialed phone numbers.

For this recipe, perform the following tasks:

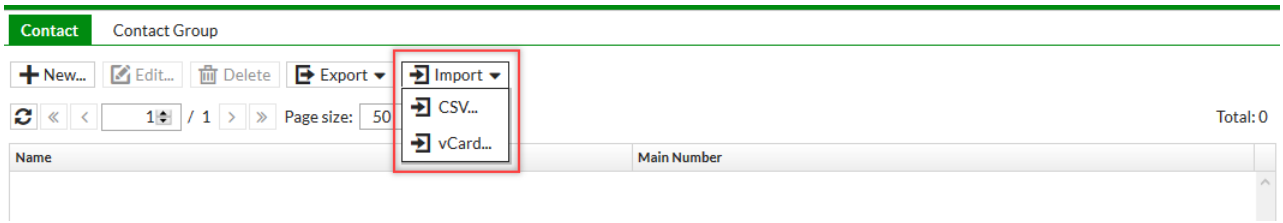
1. Enabling the auto dialer service on page 8
2. Adding contacts on page 8
3. Configuring an audio message on page 9
4. Configuring the auto dialer campaign on page 9
5. Starting an auto dialer campaign on page 9

Enabling the auto dialer service

1. Go to **Auto Dialer > Setting > Setting**.
2. Click **Enable service**.
3. Set **Maximum channel** to the maximum number of contacts that can be dialed at the same time.
4. Click **Apply**.

Adding contacts

1. Go to **Auto Dialer > Contact > Contact** and click **New**.
2. Enter the contact's **Name** and their **Main number**, and any other family, business, and emergency settings as required.
3. Click **Create**.
4. To **Import** (and **Export**) multiple contacts at once, select **CSV** or **vCard**.



Configuring an audio message

An audio message can either be uploaded or recorded.

To upload an audio message

Make sure to upload an audio file that meets the following requirements:

- WAVE (.wav) format
- Mono, 16-bit PCM (8000 MHz)

1. Go to **Auto Dialer > Campaign > Audio** and click **New**.
2. Enter a **File name** for the audio message.
3. Click **Upload**.
4. Locate the file to upload and click **Open**.
5. Click **Create**.

To record a new phone message

1. Click **Record** to record a new message by phone.
2. Set **Send record call** to your extension. Answer the call and record your message, then click **OK**. Follow the audio prompts to complete the recording.
3. Click **Download** once the file is recorded (if you would like to retain a copy in WAVE compression format), and click **Create**.

Configuring the auto dialer campaign

1. Go to **Auto Dialer > Campaign > Campaign** and click **New**.
2. Enter a **Name** and a **Caller ID** for the campaign to be displayed on called phones.
3. Set **Sound file** to the audio message from Configuring an audio message on page 9.
4. Set **Retry** to the number of times you want the auto dialer to retry calling the client if the call is missed.
5. Under **External Numbers**, select the external phone numbers and click the right-arrow to add them to the campaign.
6. Under **Internal Numbers**, add any internal extensions from your local network to be added to the campaign.
7. Click **Create**.

Starting an auto dialer campaign

1. Go to **Auto Dialer > Campaign > Campaign** and click **New**.
2. In the campaign list, select a campaign that has a status other than *Completed*.
3. Click **Start**.
4. Select a start and end time.
5. Click **OK**.

Call center

This section includes the following recipes:

- Call center setup on page 10
- Skill-based routing on page 13

Call center setup

Callers may outnumber available agents, often forcing a caller to call back repeatedly to reach an available agent. Thankfully, FortiVoice queues multiple incoming calls and can prioritize them.

This recipe guides you through the process of creating a call queue to handle large volumes of incoming calls and then set up the appropriate department to handle the calls.

This recipe includes the following tasks:

- Creating a call queue on page 10
- Configuring departments on page 12

Creating a call queue

Call queues establish the order in which incoming calls are placed when an agent is unavailable.

1. Go to **Call Center > Call Queue > Call Queue** and click **New**.
2. Enter a **Queue ID** for the queue.
3. Enter an available extension **Number** for callers to dial and enter into a call queue following the extension number pattern.
4. Enable **Status**.
5. Enter a **Display name** and brief **Description**.
6. Leave **Department** set to **None**, as you will configure one and add it to the queue later. See Configuring departments on page 12.

Queue setting

1. Under **Queue Setting**, set **Maximum queue capacity** to the maximum number of callers the queue can handle.
2. Set a **Maximum queuing time** in minutes and **Ring duration** in seconds. Once these time durations have elapsed, the caller will be dealt with according to the **Timeout Call Handling** action selected.

3. Select the **Music on hold** audio file you want for the call queue.

Call distribution

1. Under **Call distribution**, determine whether calls in the call queue will be subjected to **Skill Based Routing**, whereby calls are routed depending on the operator's skill. For more information, see Skill-based routing on page 13.
   Note that skill based routing can be configured along with a distribution policy, in which case the distribution policy will only take effect when you have more than one agent with the same skill level in a queue.
2. Set **Distribution policy** to one of the following:
   - **Ring all**: Dials all available agents.
   - **Round Robin**: Dials all agents in order from top to bottom and then bottom to top.
   - **Sequential**: Dials each agent in a sequential manner.
   - **Random**: Dials an agent at random.
   - **Least Recent**: Dials the agent that least recently received a call.
   - **Fewest Calls**: Dials the agent that has completed the fewest calls in this queue.
   - **Weight Random**: Dials a random agent, but uses the agent's penalties as a weight.
   - **Priority Based**: Dials agents based on the agents' rated ability to handle calls in that call center.

Additional setting

Under **Additional Setting**, you can configure a variety of options, including the following:

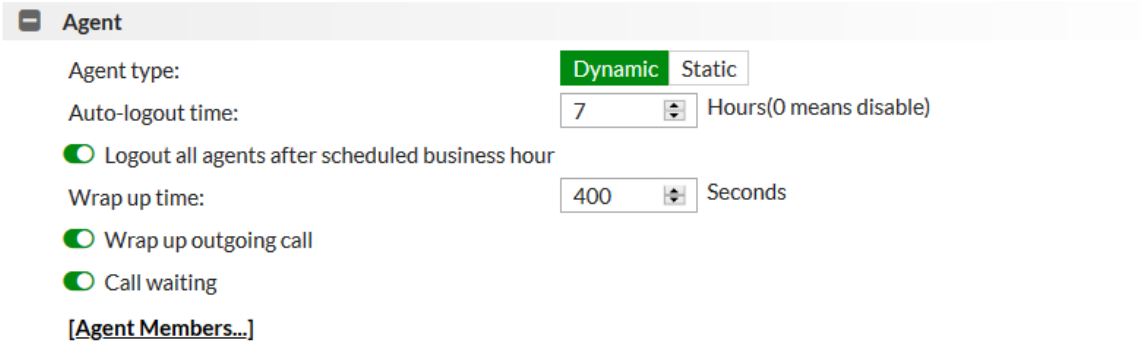
- **Distinctive Setting for Agent**: In some cases, one agent may need to handle calls from multiple queues, and needs to be able to distinguish between queues when they receive the calls. Use this setting to define an audio message that announces the queue name, and control how the caller's ID is displayed.
- **Business Schedule**: Determine when agents are available to answer calls.
- **Announcement to Caller**: Determine whether callers will be told where they are in a queue, and control how often those announcements are made.
- **Service Level**: Determine how often the FortiVoice unit checks to see whether the queue service level threshold is reached.
- **Alert**: Determine what events will trigger an alert, such as queue overflow and agent unavailability, and control how alert notifications will be sent to the appropriate contact.
- **Callback Setting**: Allow callers waiting in a queue to request a callback. The system can callback automatically

when an agent becomes available.

- **Survey Settings**: Define how the system collects customer feedback.

Agent

1. Under **Agent**, set **Agent type** to either **Dynamic** or **Static**. Dynamic agents are required to log in to the queue, while static agents are always connected to the queue.
2. If you have selected the **Dynamic** agent type, set **Auto-logout time** to the duration of time agents have before they are logged out of the queue. Additionally, enable or disable **Logout all agents after scheduled business hour** for dynamic agents.
3. Set **Wrap up time** to the duration of time in seconds needed by agents to complete a queue call. Similarly, enable **Wrap up outgoing call** to apply the same time constraint for agents to make and finish any outgoing customer calls.
4. Enable **Call waiting** to display caller information on the agent's phone when a queue call comes in while the agent is already on the phone. The agent can choose to answer the call or not. If the agent does not answer the call, after the ring duration is due, the call is transferred to the next agent.



Call handling

1. Under **Call handling**, set **When no logged-in agent** to either **Queue Caller** or **Do Not Queue**. For example, if there are no agents available, you may set this option to **Do Not Queue**, in which case any incoming calls will be handled by your general call handling configuration, such as the auto attendant.
2. Optionally configure additional scheduled and non-scheduled business hour call handling options.
3. Click **Create**.

Configuring departments

Once the call queue is created, the department that the client will contact can be configured and assigned to the appropriate managers, members, and the call queue itself. The department can be helpful for management and reporting purposes.

1. Go to **Extension > Group > Department** and click **New**.
2. Enter a **Name** for the department.
3. Under **Call Center**, move the **Member** extensions you want to be members of the department to the **Selected** column.
4. Similarly, move **Manager** extensions you want to be managers of the department to the **Selected** column.

5. Move the newly created call **Queue** to the **Selected** column.
6. Click **Create**.

Skill-based routing

When a customer dials an organization's support line they are commonly greeted with an automated attendant that transfers the customer's call to a specific department based on the number the customer selects.

This recipe guides you through the process of configuring FortiVoice to transfer customer calls to the most qualified agent.

Skill-based routing requires configuring the call center, extension, and virtual number features.

Creating skill sets

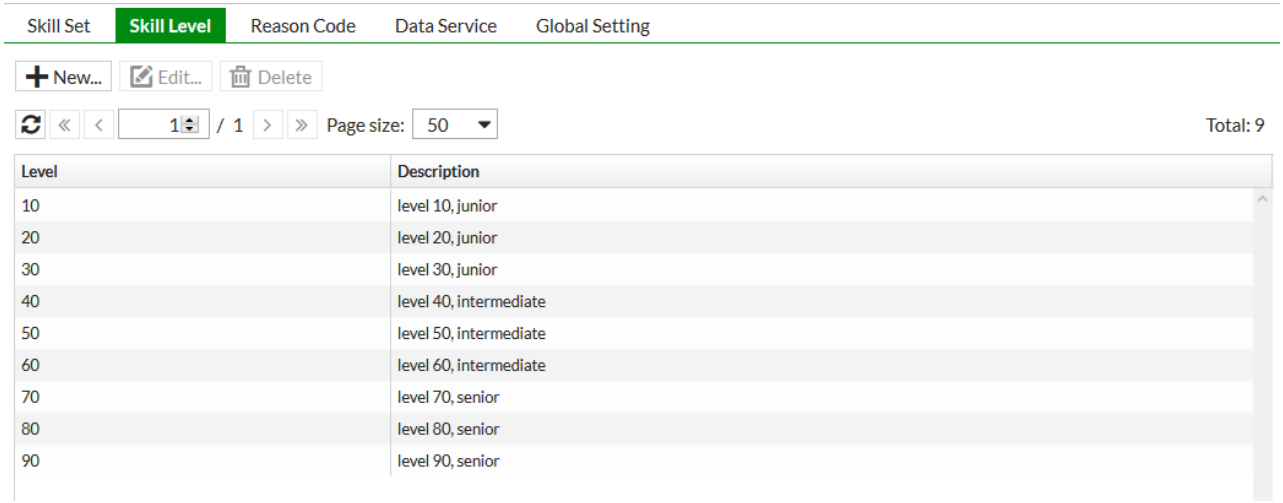
Varying skill sets must first be established for each department. For example, a skill set is created for the Sales department.

1. On FortiVoice, go to **Call Center > Configuration > Skill Set** and click **New**.
2. Enter a **Name** and **Description** for the Sales department, and click **Create**.

Configuring skill levels

Once skill sets have been created, individual skill levels must be defined.

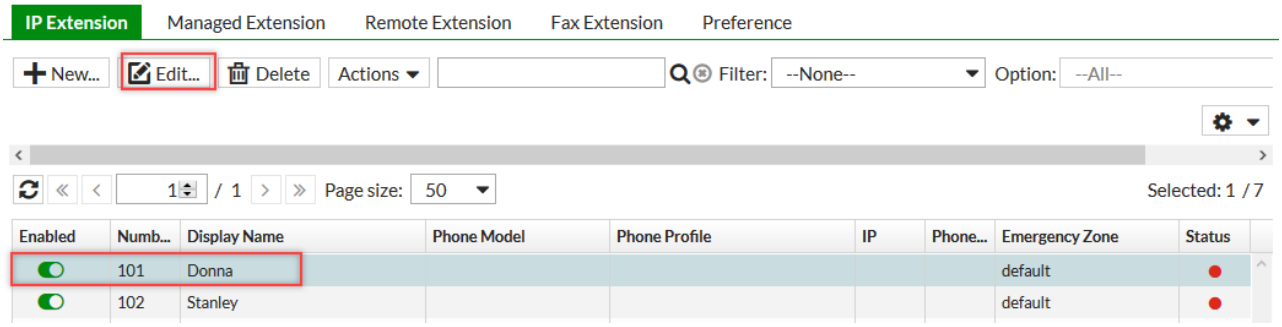
1. Go to **Call Center > Configuration > Skill Level**. The FortiVoice already has a pre-defined list of skill levels, showing varying degrees of skill-progression from junior through intermediate to senior.
2. Either create your own levels by clicking **New**, edit, or use the default levels.
   For the purpose of this recipe, default levels will be used.



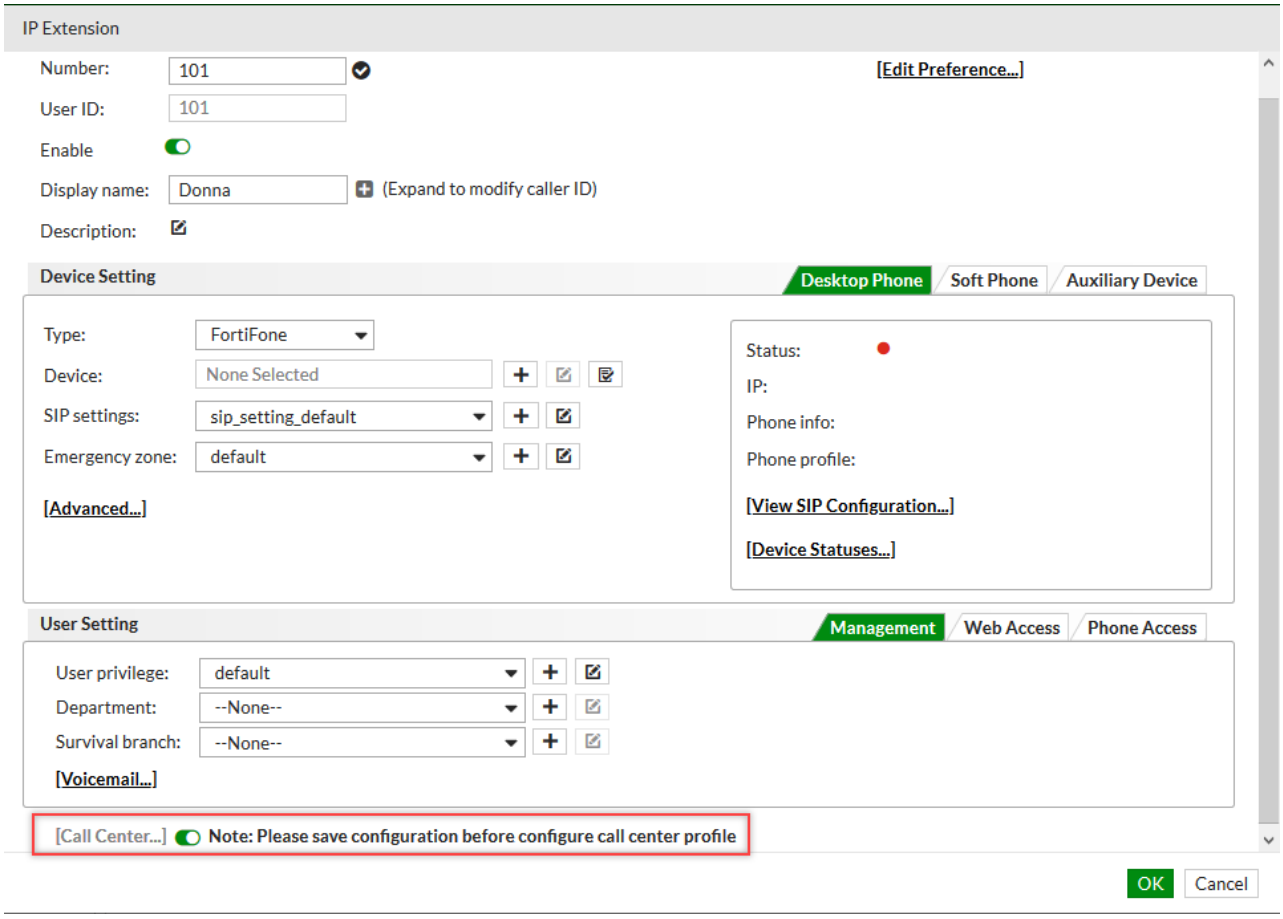
Assigning a skill level to an extension

Assign a skill level to each agent.

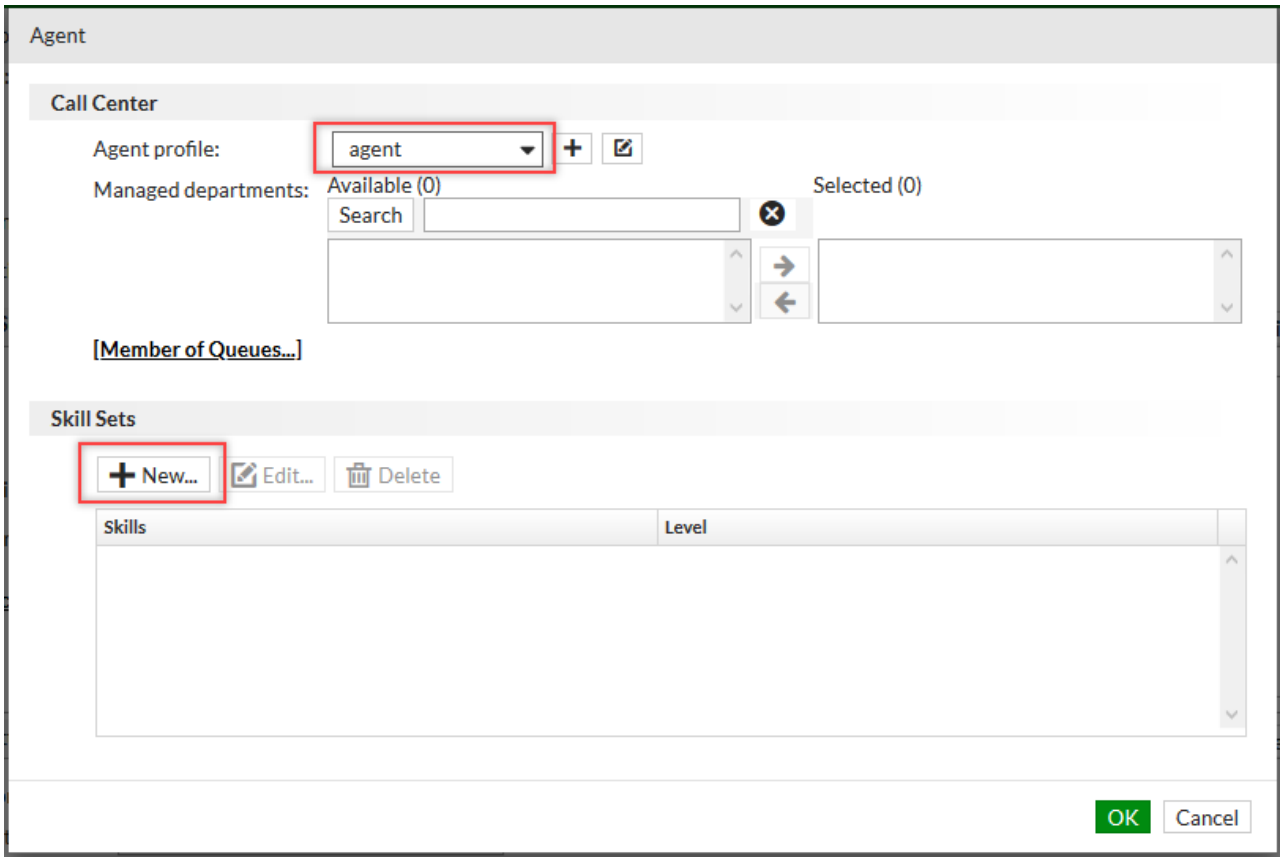
1. Go to **Extension > Extension > IP Extension**.
2. Select an agent's extension and click **Edit** (in the example, **Donna**).



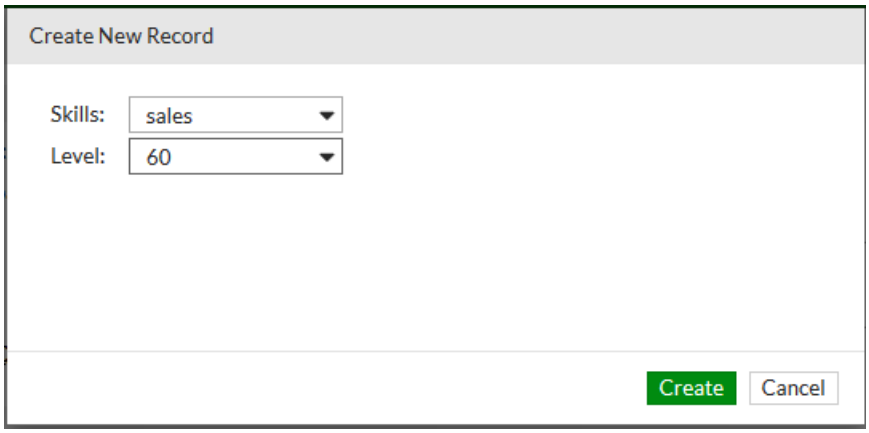
3. Enable **Call Center**. A prompt appears stating that you must save the configuration before configuring the call center profile of the extension.



4. Click **OK**, edit the profile again, and click **Call Center**.
5. Set **Agent profile** to **agent**.
6. Under **Skill Sets**, click **New**.



7. Set **Skills** to **Sales**, and set the **Level** accordingly. In this example, Donna is being assigned to the **Sales** skill set, and assigned a skill level of **60**; a strong intermediate level.
8. Click **Create**.

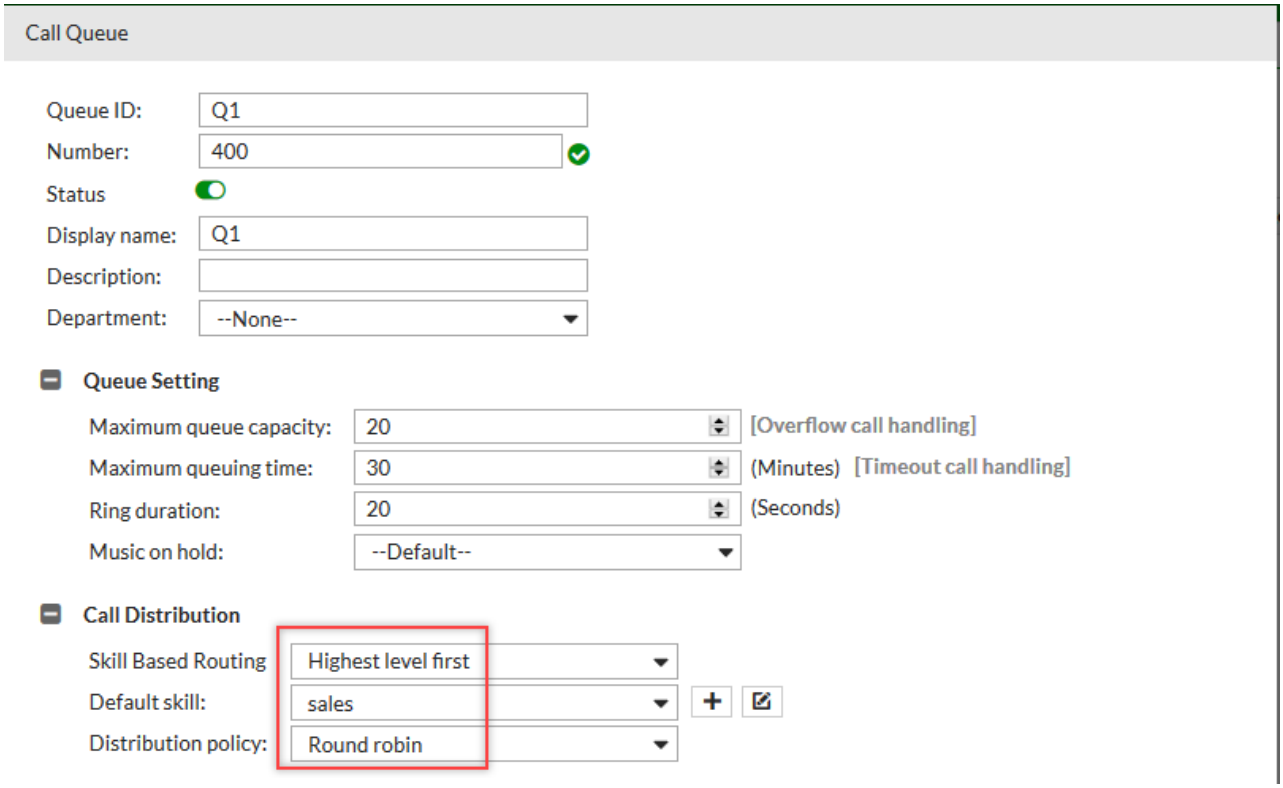


9. To complete the call center settings, click **OK**.
10. To finish configuring the agent IP extension, click **OK**.
11. Repeat the same steps for your other agents, assigning the appropriate skill level where applicable.

Configuring the call queue

Calls are routed to different call queues depending on the set skills.

1. Go to **Call Center > Call Queue > Call Queue** and click **New**.
2. Under **Call Distribution**, set **Skill Based Routing** to one of the following:
   - **Lowest Level First**: The call transfers to the agent with the lowest skill level score first and then moves up the ranks to the first available agent.
   - **Highest Level First**: The call transfers to the agent with the highest skill level score first and then moves down in rank to the first available agent.
3. Set **Default skill** to the defined skill set (Sales), meaning only agents from the Sales department will pick up calls from the queue.
4. Select a **Distribution policy** from the drop-down menu. In this example, **Round Robin** is selected, whereby all agents in the queue will be equally called from the top to the bottom of the list and so on.



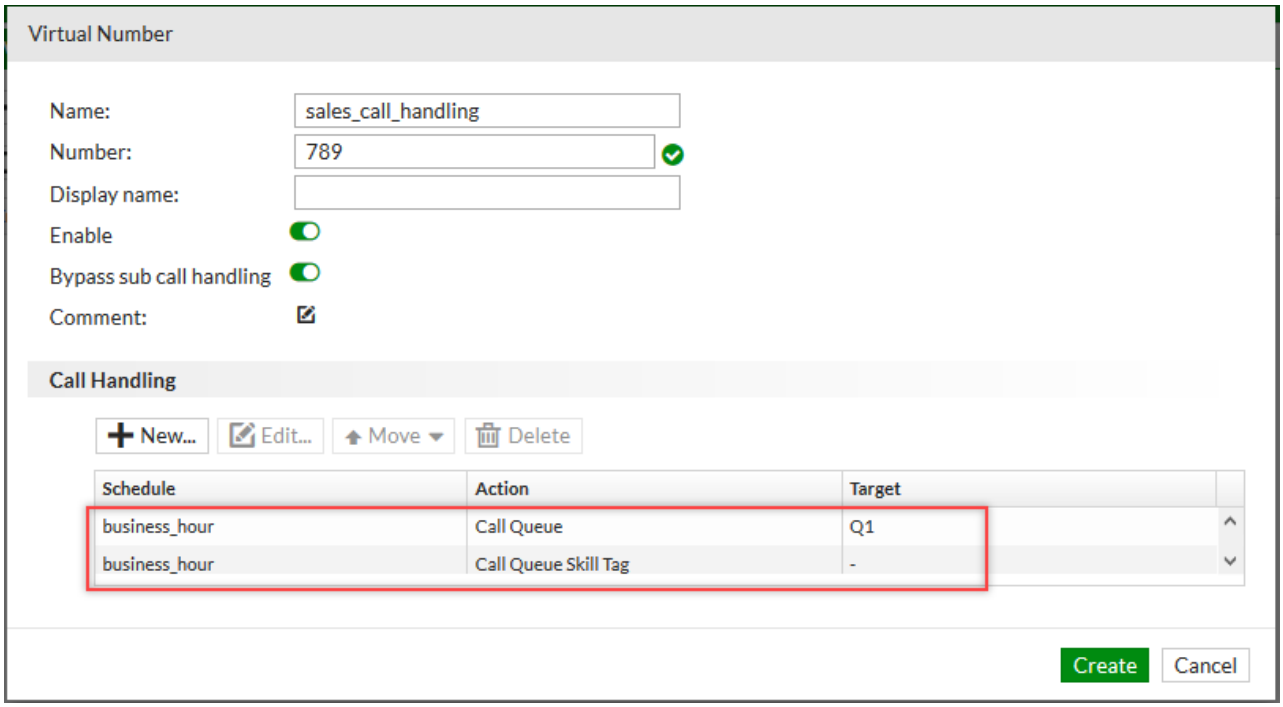
5. Under **Agent**, click **Agent Members**.
6. Select all agents that you want to be assigned to the call queue and click **OK**.
7. Click **Create**.

Configuring call handling

After establishing skill-based routing, configure call handling for virtual numbers. Skill-based call handling helps to associate (tag) an incoming call with a specific skill set to distributed a call among agents with that specific skill set. Two actions need to be defined: one to tag the call with a skill to process the call as a skill-based call, and a second to route the call to the queue where the agents with configured skill levels are assigned the appropriate calls.

1. Go to **Extension > Virtual Number > Virtual Number** and click **New**.
2. Enter a **Name** and an unassigned **Number**.
3. Under **Call Handling**, click **New**.
4. Set an appropriate **Schedule**, and set **Action** to **Call Queue Skill Tag**.

5. Click **OK**.
6. Click **New** again.
7. Set the **Schedule**, and set **Action** to **Call Queue**.
8. Assign the newly created **Call queue** from the drop-down menu.
9. Click **OK**. Your virtual number call handling should look similar to the example below.
10. Click **Create**.



Call features

This section includes information about the following call features:

- Auto attendant on page 18
- Call parking on page 20
- Call recording on page 24
- Conference calls on page 25
- Faxes on page 32
- Speed dial numbers on page 35

Auto attendant

What if you need FortiVoice to answer calls and direct users to various departments within your office? An auto attendant can answer calls with a prerecorded message and then guide the user to the department they desire with a simple press of a button.

This recipe guides you through the process of configuring auto attendants, exploring the user options, and establishing how a caller navigates through the auto attendant.

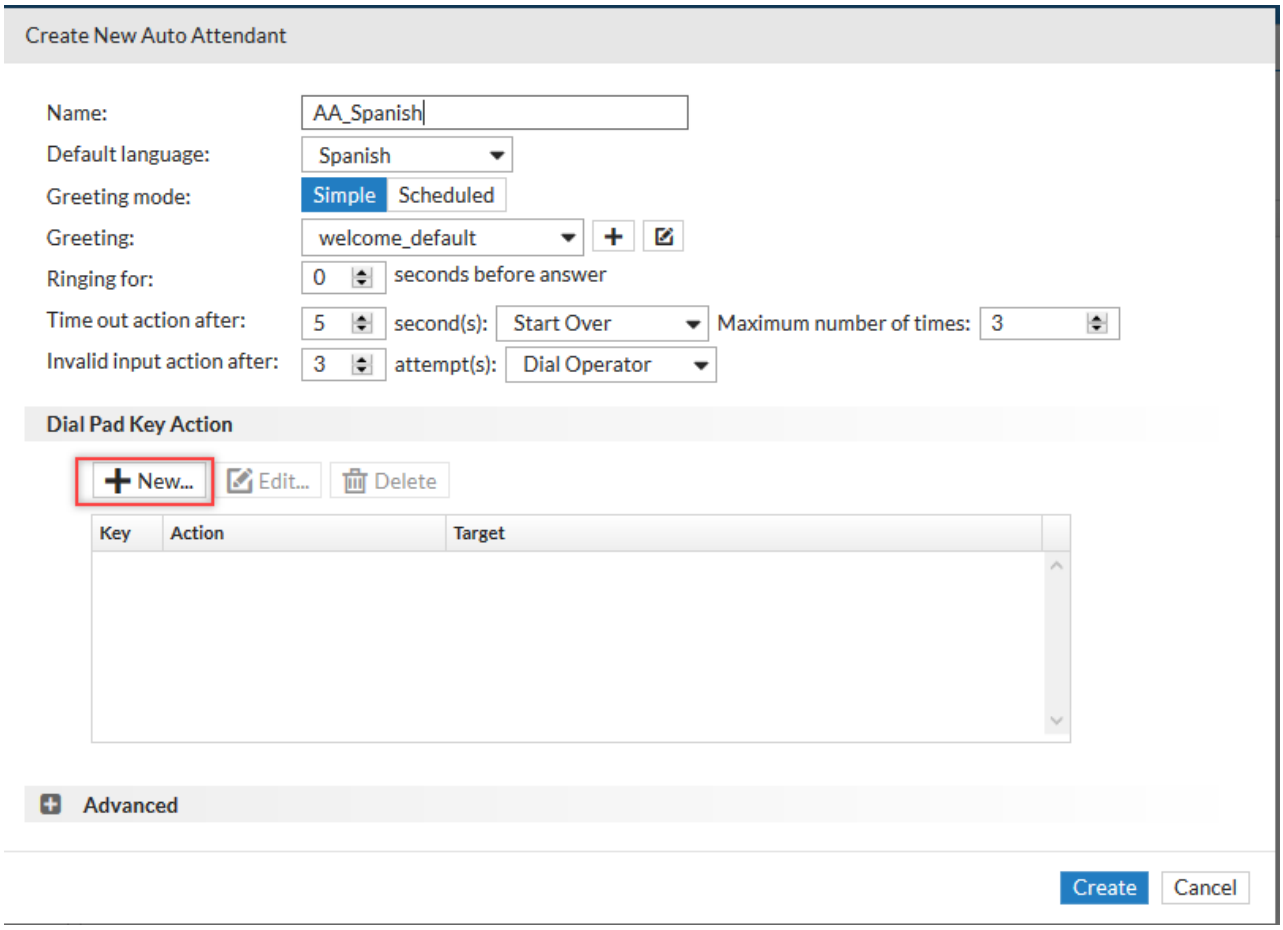
This recipe includes the following tasks:

- Configuring the auto attendant on page 18
- Configuring key actions on page 19
- Configuring advanced settings (optional) on page 20

Configuring the auto attendant

1. Go to **Call Feature > Auto Attendant > Auto Attendant** and click **New**.
2. Enter a **Name** and set the **Default language**.
3. Select a **Greeting mode**, and select the desired sound file for the **Greeting**.
4. Enter the amount of time that the phone will ring before being answered, and the time out and invalid input settings.

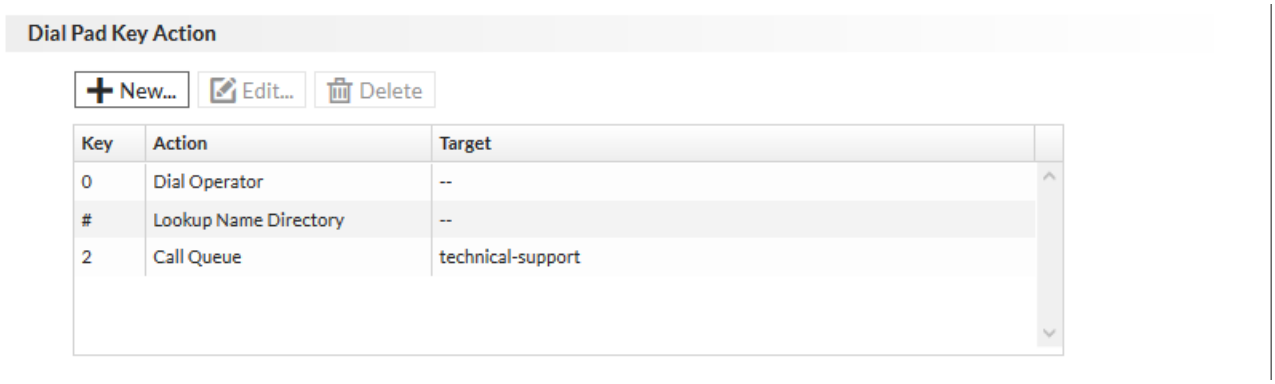
5. Before you click **Create**, configure the dial pad key action settings in Configuring key actions on page 19.



Configuring key actions

Configure the auto attendant keys for caller to use when navigating through the auto attendant hierarchy.

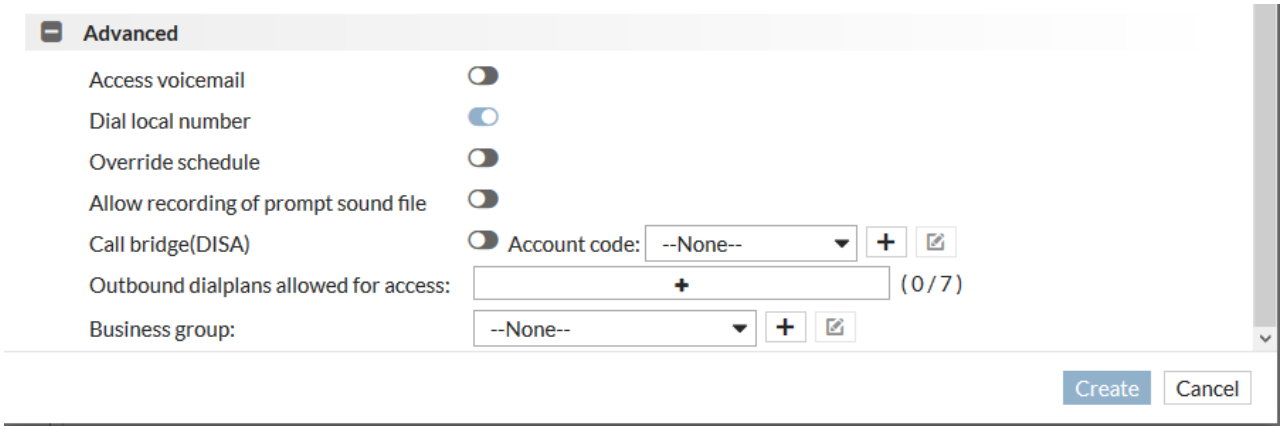
1. Under **Dial Pad Key Action**, click **New**.
2. Map keys with the appropriate **Language** and **Action**, and any additional settings according to the action selected. In this example, the **Dial Pad Key Action** section shows number 2 assigned to the technical support call queue.



Additional advanced settings can be optionally configured in Configuring advanced settings (optional) on page 20.

Configuring advanced settings (optional)

1. Expand the **Advanced** tab.
2. Enable **Access voicemail**, if required, to allow external callers to reach their voicemail boxes by dialing their voicemail prompt code. Dial local number should already be enabled by default, allowing external callers to dial local extensions.
3. Disable **Dial local number** if you do not want callers to be able to dial extensions directly. This forces users to use the Dial Pad Key Actions only – used in many call centers.
4. Enable **Override schedule**, if required, to allow an administrator with the privilege to dial a code followed by the administrator PIN to replace the original schedule with a system schedule.
5. Enable **Call bridge (DISA)**, if required, and select an account. This allows external users to dial into the FortiVoice device and use the FortiVoice service like a local extension.
6. If **Call bridge (DISA)** is enabled, select the outbound dial plan for users to make outbound calls using FortiVoice.
7. Click **Create**.



Call parking

Sometimes active calls at extensions are put on hold within the FortiVoice for other extensions to pick up. This process is called “parking”. FortiVoice features the ability to easily park calls, unpark calls, and monitor parking slots on FortiFone devices with programmable keys. Monitored parking slots can easily unpark calls by simply pressing the programmable key. Calls can also be parked by using the call park feature code, which is useful for FortiFone devices without programmable keys.

The following recipes cover specific tips to program and use call parking on FortiVoice and FortiFone devices:

- Configuring call parking settings on page 20
- Configuring call parking on programmable phone keys on page 21
- Using call parking on page 23

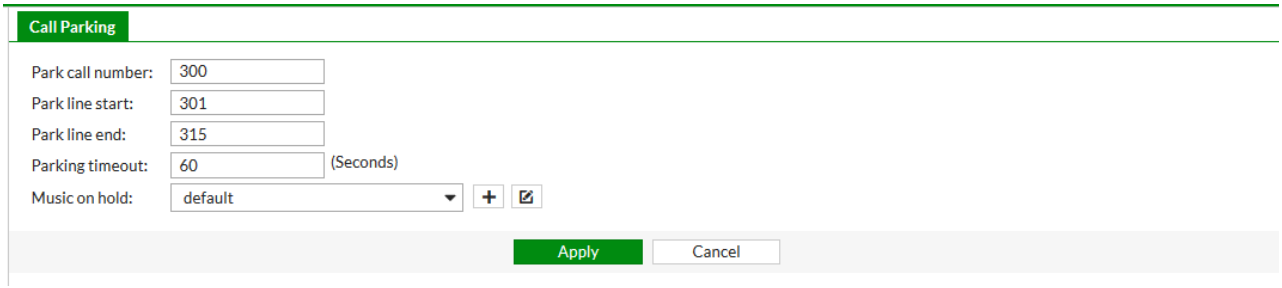
Configuring call parking settings

First, call parking must be configured on FortiVoice. It is recommended to keep the numbering scheme separate from the extension number scheme, keeping it unique to call parking. By default, the FortiVoice reserves 300 to 320 for call parking. This can be broken down as follows:

- **300**: Number reserved to park a call in the first available slot.
- **301-320**: Numbers reserved as call park slots.

For more information on how to use these number schemes, see Using call parking on page 23.

1. Go to **Call Feature > Call Parking > Call Parking**.
2. Set **Park call number** to the number used to park calls automatically to the first available call park slot.
3. Set **Park line start** and **Park line end** to define the total range of call park slots.
4. Set **Parking timeout** to the amount of time in seconds that the call will remain parked. Once this timeout is reached, the parked call is returned to the extension that had parked it.
5. Select the desired hold music from the **Music on hold** drop-down menu, and click **Apply**.



Configuring call parking on programmable phone keys

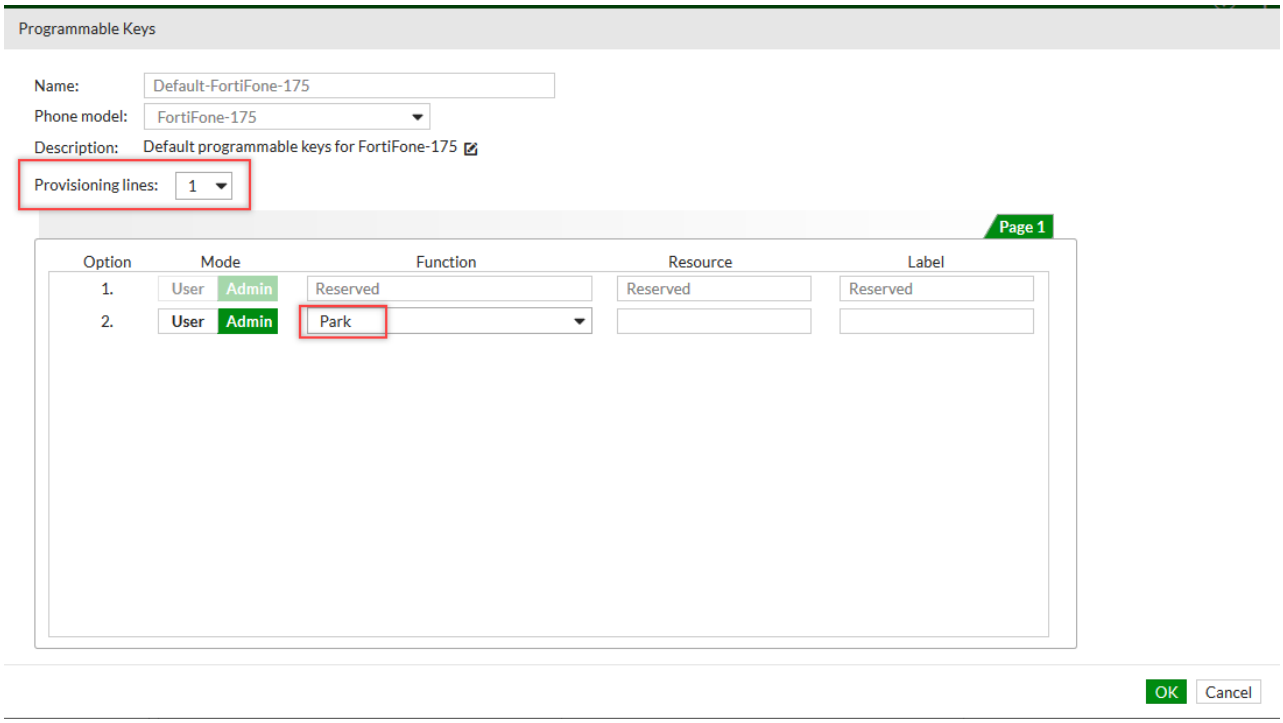
FortiFone devices that support programmable phone keys can be configured with one touch call parking. There are two types of call park programmable phone keys:

- **Park**: Places the call into the first available call park slot.
- **Park appearance**: Monitors the selected call park slots, informing the user if there is a call parked. It may also be used to park a call in the specified call park slot if it is not already in use.

Configuring automatic parking

1. Go to **Phone System > Profile > Programmable Keys**.
2. Select a FortiFone profile and click **Edit**.
3. In **Provisioning lines**, select **1**.
4. Under **Page 1**, set the **Function** for line 2 to **Park**.

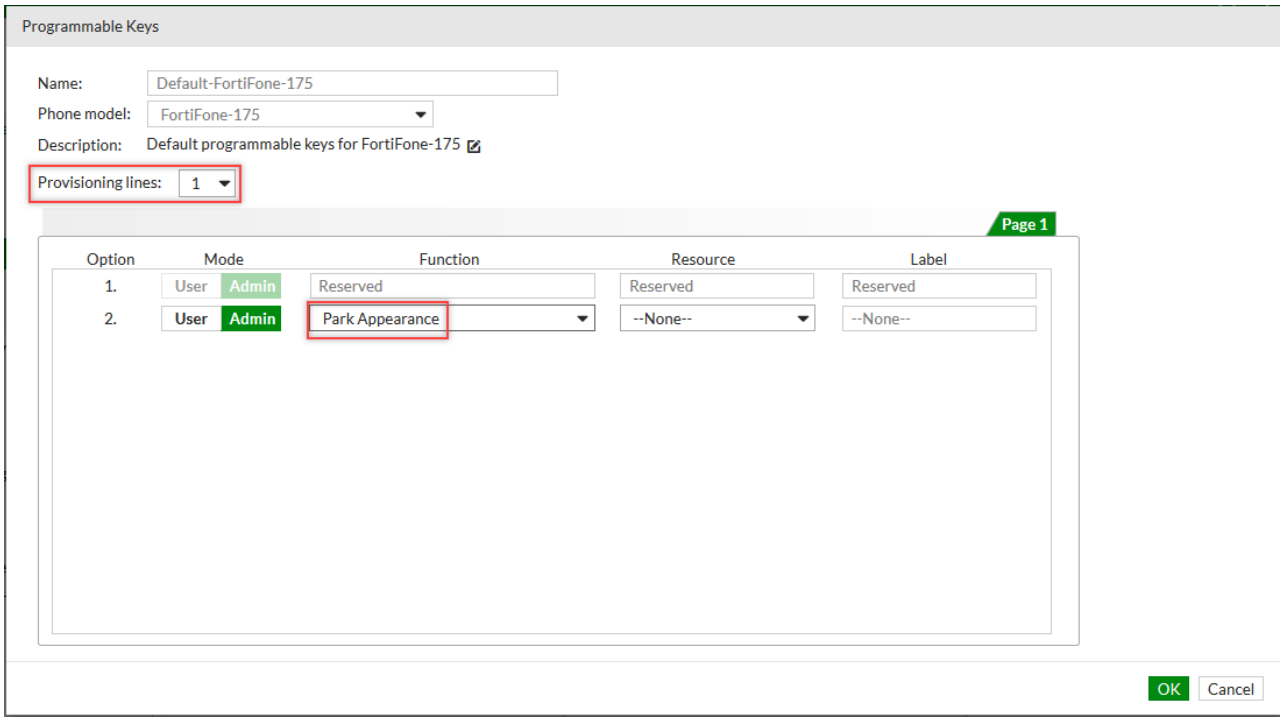
5. Click **OK**. For changes to take effect, the FortiFone device must reboot.



Configuring park appearance

1. Go to **Phone System > Profile > Programmable Keys**.
2. Select a FortiFone profile and click **Edit**.
3. In **Provisioning lines**, select **1**.
4. Under **Page 1**, set the **Function** for line 2 to **Park appearance**.
5. Set **Resource** to the call park slot you would like to monitor. The **Label** will automatically propagate.
6. Click **OK**. For changes to take effect, the FortiFone device must reboot. Repeat this for as many call park slots that

you would like to monitor.



Using call parking

You can park a call in the following ways:

- Call park feature code
- Programmable phone key with park
- Programmable phone key with park appearance

All FortiFone models support the feature code method.

Feature code

1. While on a call, dial ***40**.
   The call is now parked. The extension will be notified of the call park slot number.
2. To retrieve the parked call from any extension, dial the call park slot number.

Programmable key with park

1. While on a call, press the **Park** programmable phone key on the FortiFone device.
   FortiVoice will indicate the call park slot the call has been placed in (for example, 301).
2. To retrieve the parked call from any extension, dial the call park slot number.

Programmable key with park appearance

1. While on a call, press the **Park appearance** programmable phone key on the FortiFone device.
   The call is now parked.
2. To retrieve the parked call, press the **Park appearance** programmable phone key again or dial the call park slot number.

When using call park, keep in mind the following:

- The feature code and programmable phone key park methods will place the call in the first available call park slot.
- Programmable phone keys with park appearance will indicate if a call is parked. Press the key to retrieve the call.
- Programmable phone keys with park appearance may be used to park calls, only if the key is not already in use.

Call recording

FortiVoice allows you to monitor and supervise incoming and outgoing calls, but you can also record calls, allowing you to have a permanent record of particularly important phone calls.

For details about configuring call recordings and archiving recorded calls, see the FortiVoice Phone System Administration Guide.

This section includes the following recipe:

- Recording a phone call on page 24

Recording a phone call

With FortiVoice, the following two types of phone call recordings are available:

- **Personal recording**: You can access your phone call recordings from the FortiVoice user portal.
- **System recording**: With the administrator privilege, you can access phone call recordings from the FortiVoice web-based manager.

Before you begin

- **To allow an extension to perform a call recording**: Make sure to apply a user privilege with the personal recording or system recording option enabled, as applicable, to that extension. To enable recording options, the FortiVoice system administrator can go to **Phone System > Profile > User Privilege** and then **Monitor/Recording**.
- **To allow an extension to access a personal call recording from the FortiVoice user portal:** Make sure to apply a user privilege with the call recording option enabled to that extension. To enable the call recording option on the FortiVoice user portal, the FortiVoice system administrator can go to **Phone System > Profile > User Privilege** and then **User Portal**.
- **To view codes**: Personal and system recording procedures in this section use the default feature codes for recording phone calls. To view or edit those codes, the FortiVoice system administrator can go to **Call Feature > Feature Code > Mid-Call/DTMF Code**.

Before recording a phone call, have the agreement of the person you are talking with or check your local laws regarding phone recording.

To start and manage a personal recording

1. During a phone call, start the personal recording by pressing *30.
2. To pause a personal recording, press *31. To resume the recording, press *30 again.
   The recording will continue until you hang up.
3. To access the recording from the FortiVoice user portal, open a web browser and go to `https://<IP_address_or_FQDN>/voice`.
   Where <IP_address_or_FQDN> is the IP address or the FQDN of the FortiVoice phone system.
   If the FortiVoice system administrator has changed the access port, then you must also include the port, for example:
   `https://<IP_address_or_FQDN>:446/voice`
4. Go to **Call Recording**.
5. Perform one of the following actions:
   - To listen to the recorded phone call, click ▶.
   - To remove the recorded phone call, click **Delete**. To confirm the deletion, click **Yes**.
   - To send the recorded phone call to another extension, click **Forward**. Select the extension and click **OK**.

     When you download multiple recorded phone calls at the same time, they are saved in the TGZ file format. To decompress and extract the recorded phone calls from this file, use a third-party tool that supports the TGZ file format.

   - To save the recorded phone call (WAV file format), click **Download**. Select to save the file and click **OK**.

To start and manage a system recording

1. During a phone call, start the system recording by pressing *35.
   - To pause the system recording, press *36.
   - To resume the system recording, press *37.
   - To cancel the system recording, press *38.

   If you did not pause or cancel the system recording, the recording will end when you hang up.
2. To listen to the recording:
   - Log in to the FortiVoice web-based manager.
   - Select **Monitor > Storage > Recorded Call**.
   - Double-click a call record folder to open the archived call files.
   - Select a recording and click **Play**.

Conference calls

FortiVoice features conference calling, allowing multiple clients to join a live group discussion.

This recipe details how to create three kinds of call conferencing instances:

- **User Conferencing**: Administrators provide the ability for users to create and schedule conferences through the FortiVoice user portal. Users can add attendees to the conference in order to get an email invite with the information regarding the conference.

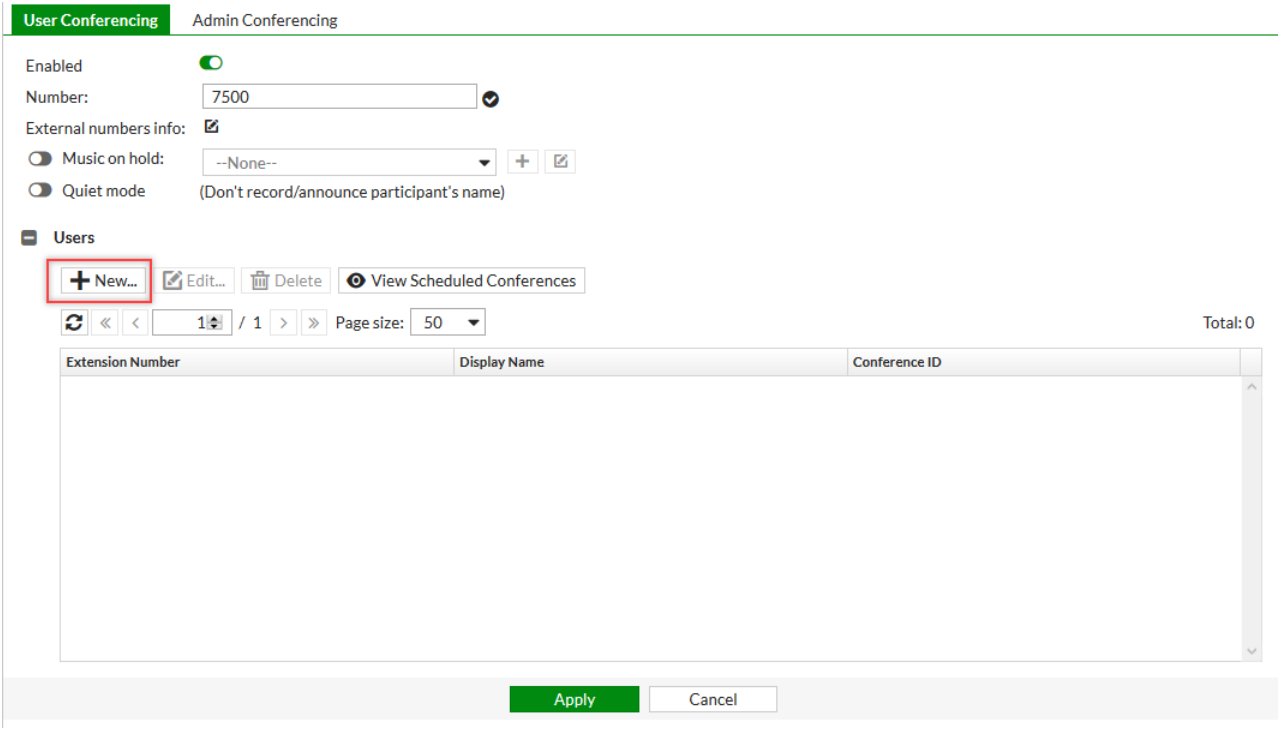
- **Static Conference**: Administrators create rooms for conference that can be used based upon schedule profile (office hours, anytime, and so on) or only available for a specific date and time. These conferences are the most restrictive. To avoid conflicts administrators would need to create multiple rooms.
- **Dynamic Conference**: Administrators create a room, and then can create unique conference events based upon time and dates required. These events will have unique conference IDs limiting conflicts in participants. Similar to user conferencing attendees can receive email invites with the call details for the conferences.

This section includes the following recipes:

- Configuring user conferencing on page 26
- Scheduling a user conference on page 26
- Viewing upcoming user conferences on page 29
- Configuring administrator conferencing on page 30

Configuring user conferencing

1. Go to **Call Feature > Conferencing > User Conferencing** and click **Enabled**.
2. Set **Number** to the extension number that is mapped to the external number that callers can use to dial to join the conference call.
3. Under **Extensions**, click **New** to add extensions users who have the privilege to organize conference calls.

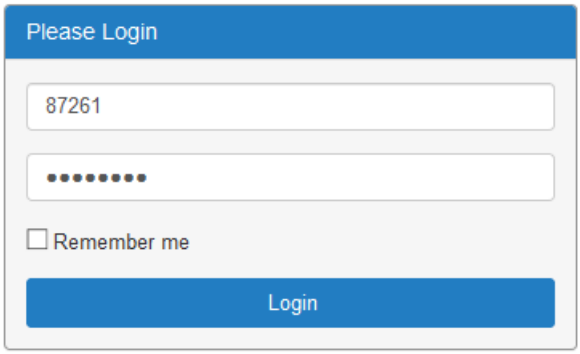


4. Select the **Extension** from the drop-down list.
5. For **Conference ID**, enter a code or generate one by clicking **Generate**.
6. Select **OK**, and select **Apply** to finish the **User Conferencing** configuration.

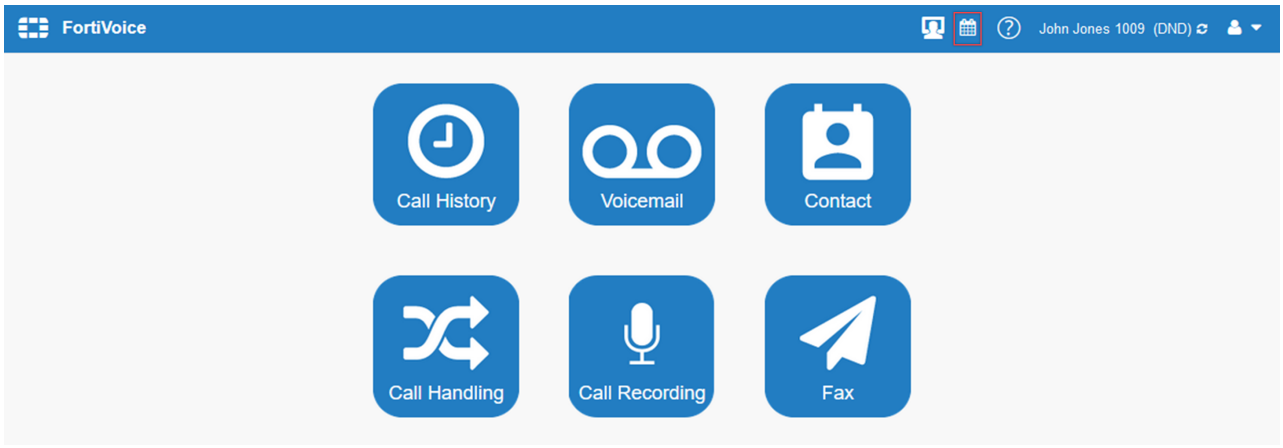
Scheduling a user conference

Access the FortiVoice user portal to schedule a user conference and invite attendees.

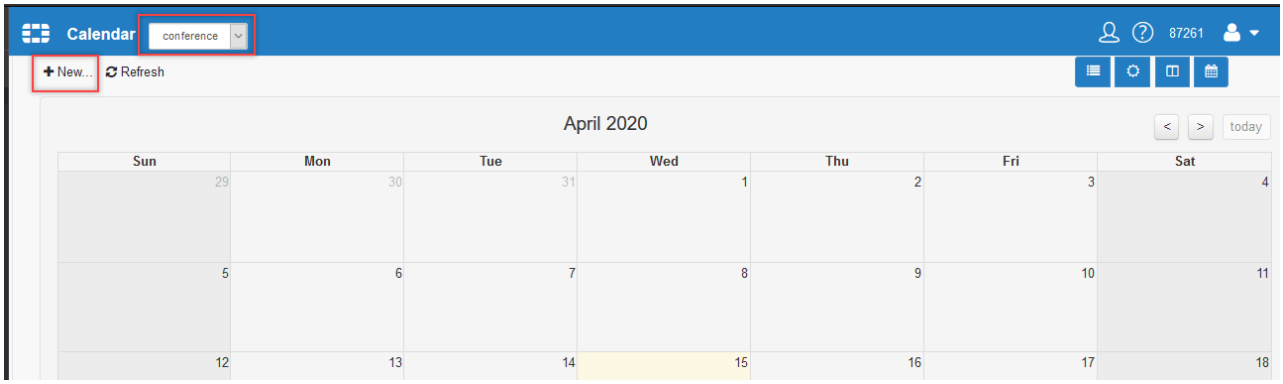
1. Open a web browser and go to `https://<IP_address_or_FQDN>/voice`.
   Where <IP_address_or_FQDN> is the IP address or the FQDN of the FortiVoice phone system.
   If the FortiVoice system administrator has changed the access port, then you must also include the port, for example:
   `https://<IP_address_or_FQDN>:446/voice`
2. Log in as the user that has been added to the list of extensions.



3. After you are logged in, click on the calendar.
   The **Conference** option is available to extensions that have been added to the extension list that allows conference scheduling.

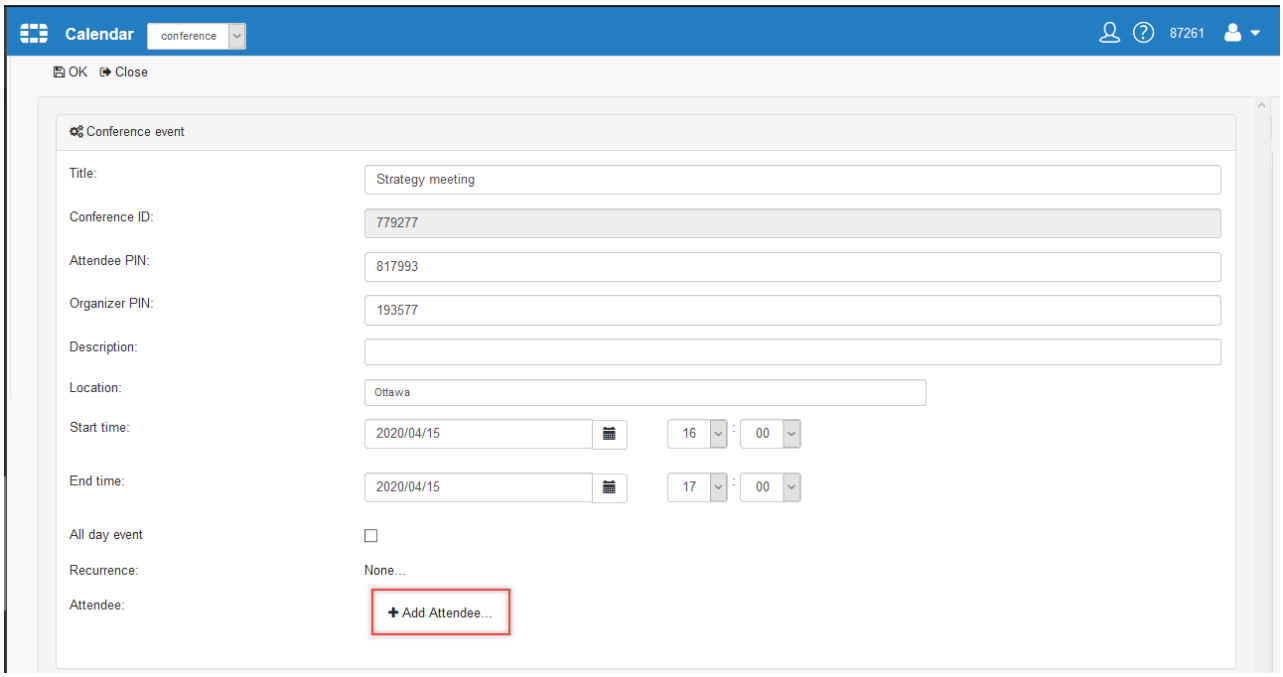


   A new window opens to a calendar view, where the user can schedule upcoming conference calls.
4. Select **Conference** and then click **New** or the date you wish to schedule the conference for.

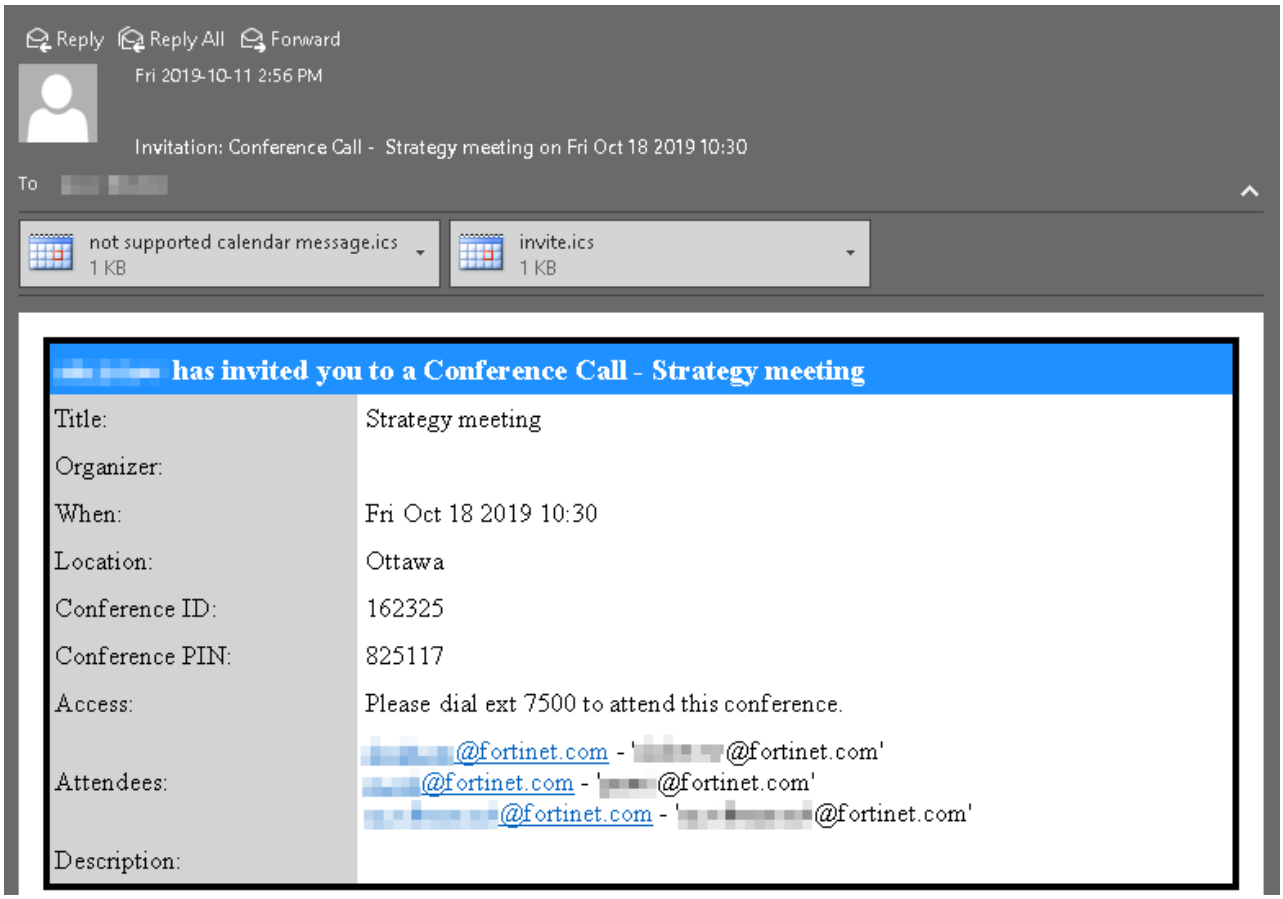


5. Fill in details for this meeting.
6. Make note of the **Attendee PIN**. Attendees invited to the conference call will need this PIN.

7. Make note of the **Organizer PIN**. You will need this PIN to start the meeting.
8. In **Attendee**, click **Add Attendee**.



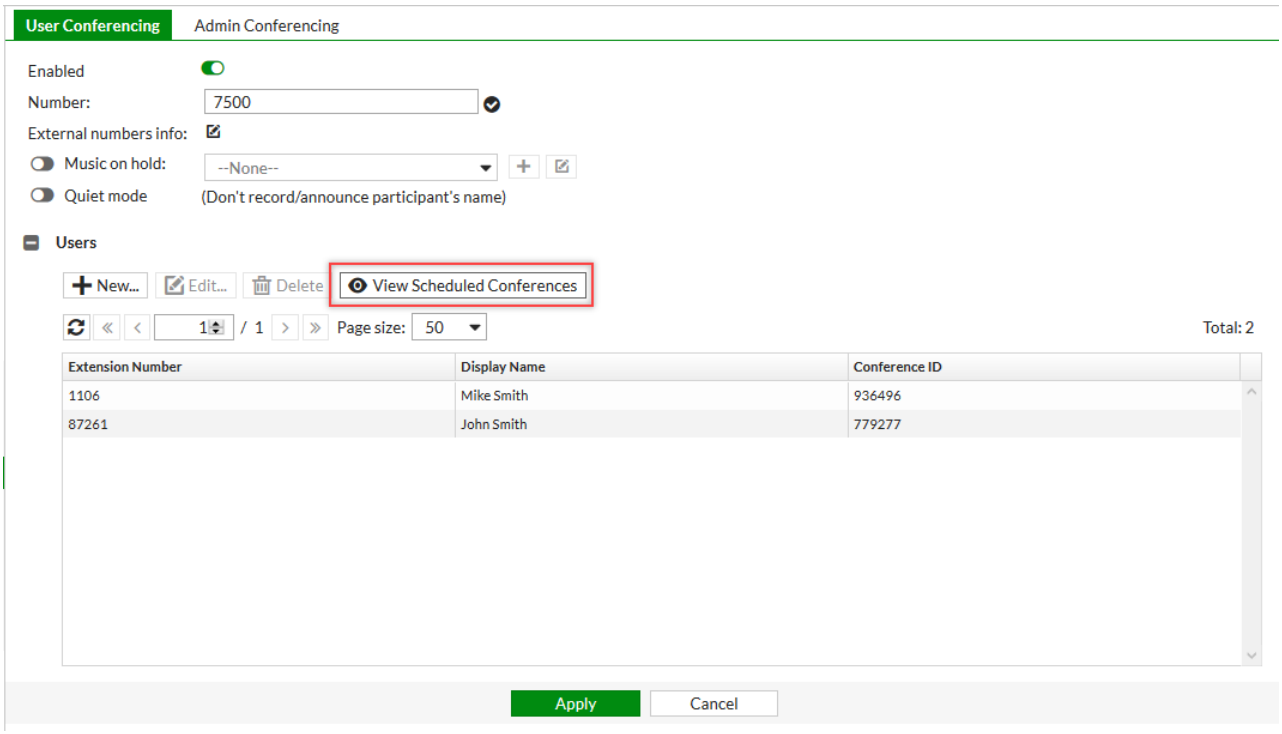
9. Enter the **Email** address of the attendee you wish to invite to the conference call, with an optional **Display name**. Click **Create**.
10. Add any additional attendees you wish to invite.
11. To finish the scheduling of the conference call, click **OK**.
    Upon clicking **OK**, all invited attendees will receive an email invitation to the conference call, with all the relevant information they need to attend the conference call.



Viewing upcoming user conferences

As an administrator, you can view upcoming conferences in the FortiVoice web-based manager.

1. Go to **Call Feature > Conferencing > User Conferencing**.
2. Click **View Scheduled Conferences**.

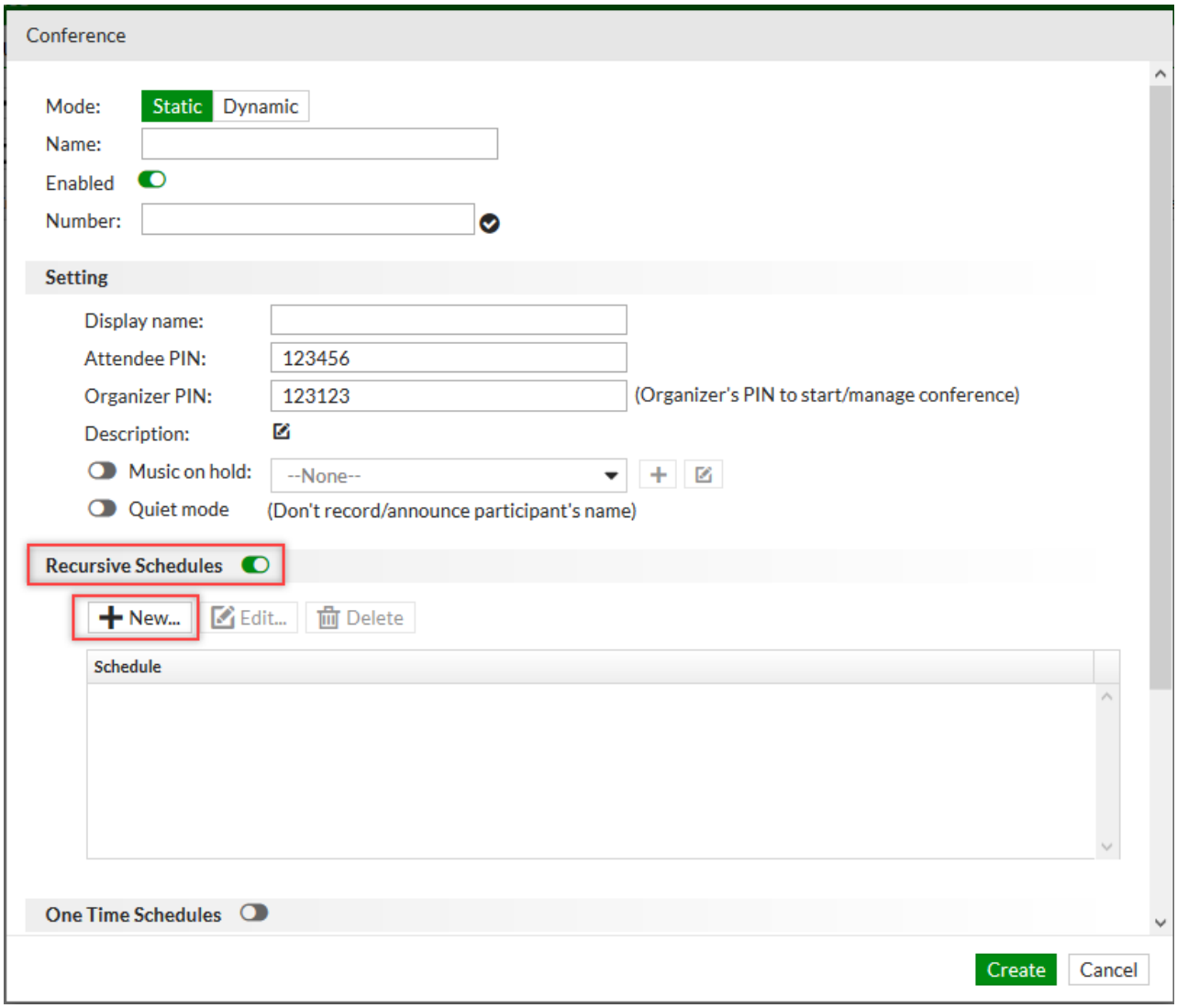


Configuring administrator conferencing

Both **Static** and **Dynamic** administrator conferences can be configured.

Configuring a static conference call

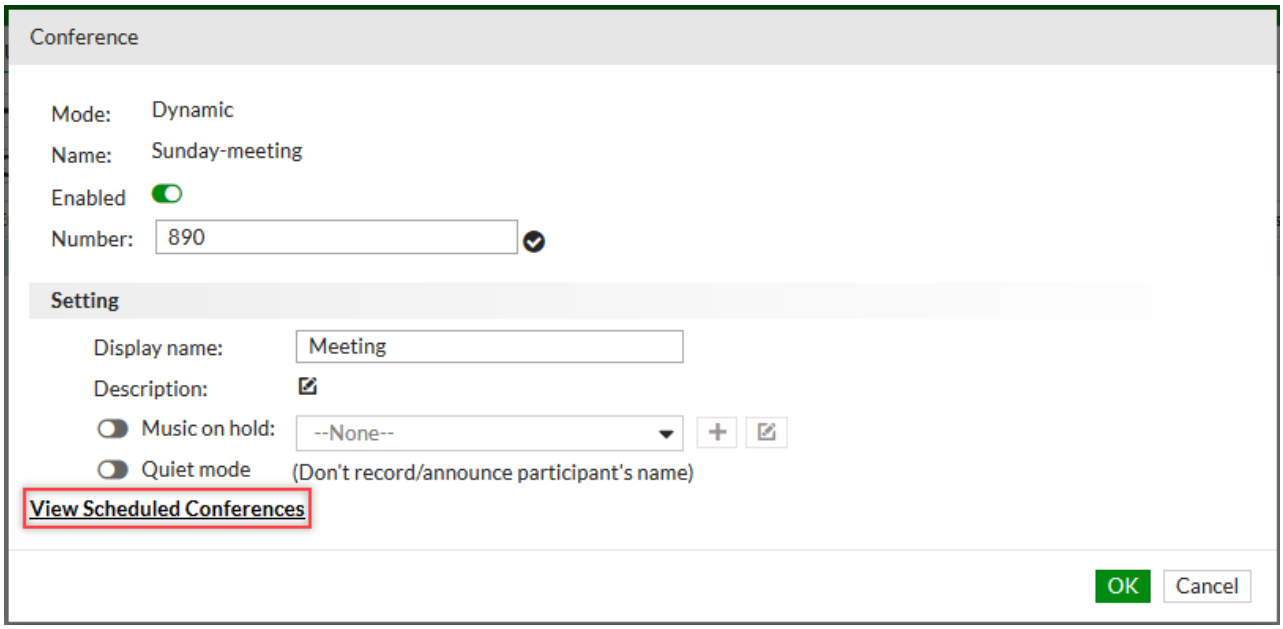
1. Go to **Call Feature > Conferencing > Admin Conferencing** and click **New**.
2. Set **Mode** to **Static**, enter a **Name**, and set to **Enabled** (if not already activated).
3. Enter an extension **Number** that callers can dial to join the conference call.
4. Under **Setting**, enter a **Display name** for the conference call, and an optional **Description**.
5. Enter a **User PIN**, which is the password users must enter to join the conference call.
   Callers need to dial the conference number and then enter their PIN.
6. Enter an **Admin PIN**, which is the password an administrator must use to begin the conference call.
7. To configure a recurring frequency for this static conference call, enable **Recursive Schedules** and click **New**.



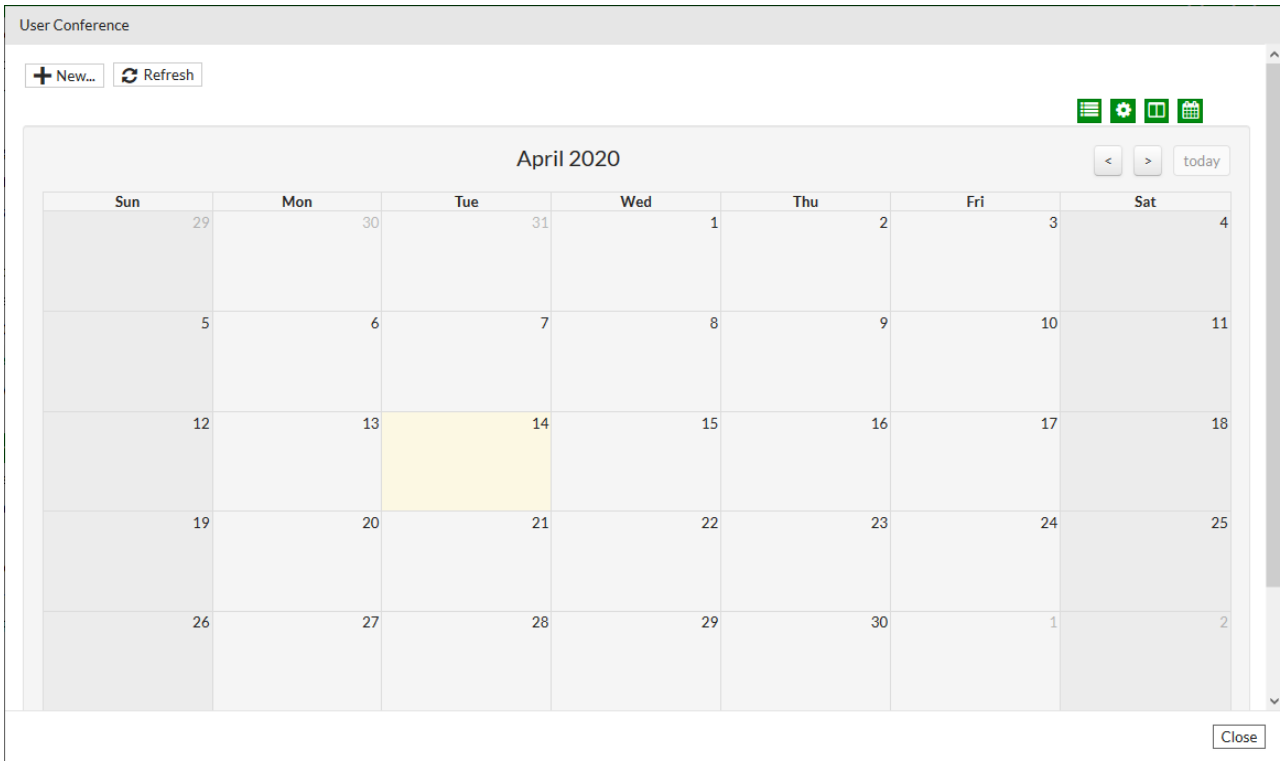
8. Assign an appropriate **Schedule** from the drop-down list, and enter a **Password**. Then click **Create**. This recursive schedule will make sure that users can only join the conference call during the scheduled time period by entering the configured password.
9. Alternatively, enable **One Time Schedules** and click **New** to schedule a single conference call.
10. Click **Create**.

Configuring a dynamic conference call

1. Go to **Call Feature > Conferencing > Admin Conferencing** and click **New**.
2. Set **Mode** to **Dynamic**, enter a **Name**, and set to **Enabled** (if not already activated).
3. Enter an extension **Number** that callers can dial to join the conference call.
4. Under **Setting**, enter a **Display name** for the conference call, and an optional **Description**.
5. Click **Create**.
6. Select your newly created conference call and click **Edit**.
7. Click **View Scheduled Conferences** to show the calendar view.



8. To schedule conference calls, click the desired date.



Faxes

FortiVoice can send and receive faxes to the FortiVoice user portal, email, and physical fax machines. This section guides you through the process of configuring the FortiVoice unit to send and receive faxes.

This section includes the following recipes:

- Configuring FortiVoice to receive faxes on page 33
- Configuring fax archive settings on page 33
- Configuring FortiVoice to send faxes on page 34
- Configuring general fax settings on page 34

Configuring FortiVoice to receive faxes

1. Go to **Call Feature > Fax > eFax Account** and click **New**.
2. Under **Incoming Fax Setting**, enter a **Name** and extension **Number**.
3. Enter a **Display name** of the extension, and click **Enable**.
4. Under **External Numbers**, click **New**.
5. Map the direct inward dialing (DID) numbers to the extension of the fax. Select the **Incoming trunk** used for dialing the DID numbers, and enter the **DID Numbers** that you want to map to an extension.
   All DID numbers assigned here will reach this extension for incoming faxes.
6. Under **Select Fax Monitors**, assign the extensions that can monitor the faxes received on this fax extension in their FortiVoice user portal. From their FortiVoice user portal, users can choose to view, delete, resend, forward, or download the faxes. These users, who have email addresses linked to their extensions, will receive an email notification when a fax is received.
7. Set **Fax to Email** to the email addresses you want to receive the faxes sent to this fax extension. These email addresses will receive the faxes in a PDF file.
8. If required, under **Relay to Fax Machine**, assign the fax machines connected to the FortiVoice unit using T.38 adapters. Faxes will be relayed to the selected machines.
9. Under **Archive**, enable **Fax archive** to activate fax archiving and enter the **File name format** to archive, according to the formats available from the drop-down menu. To configure additional fax archive settings, see Configuring fax archive settings on page 33.
10. Click **Create**.

Configuring fax archive settings

If you have enabled **Fax archive** in an **eFax Account** (Configuring FortiVoice to receive faxes on page 33), specify rotation and destination settings.

Procedure steps

1. Go to **Call Feature > Fax > Archive**.
2. Under **Rotation Setting**, configure settings that trigger the rotation of archived faxes:
   a. Set the **Fax rotation size** in MB and **Fax rotation time** in seconds. The FortiVoice unit starts generating a new archive file when either one of these parameters (size or time) is reached first.
   b. Set **Archiving options when disk quota is full** to determine what the FortiVoice unit should do if it runs out of disk space. Click **Overwrite** to remove the oldest archived folder to make space for new archives, or click **Do Not Overwrite** to stop archiving.
   c. Set a **Schedule** for archiving to take place. Archiving will not take place outside of the selected schedule.
3. Under **Destination Setting**, decide where you want to save the archived faxes.
   a. To use the hard drive of the FortiVoice unit or a NAS server, set **Destination** to **Local**.
   b. To use a remote FTP or SFTP storage server, set **Destination** as **Remote** and configure the remote server options, as necessary.

4. Click **Apply**.

Configuring FortiVoice to send faxes

1. Go to **Call Feature > Fax > Sending Rule** and click **New**.
2. Enter a **Name** and click **Enable**.
3. Under **Dialed Number Match**, click **New**.
4. Enter a **Match Pattern** number. This is the extension number pattern in your dial plan that can match many different numbers for sending faxes.
   The following pattern matching syntax is supported, in order to match a wide range of potential numbers:

Syntax	Description
X	Matches any single digit from 0 to 9.
Z	Matches any single digit from 1 to 9.
N	Matches any single digit from 2 to 9.
[15-7]	Matches a single character from the range of digits specified. In this case, the pattern matches a single 1, as well as any number in the range 5, 6, 7.
.	Wildcard match; matches one or more characters, no matter what they are.
!	Wildcard match; matches zero or more characters, no matter what they are.

5. Enter any required **Modification** settings, such as stripping or appending prefixes or postfixes to the number pattern, and click **Create**.
6. Under **Call Handling**, click **New**.
7. Set the appropriate **Schedule**, **Action**, and **Outgoing trunk** and/or **Caller ID modification** for your dial plan requirements, to determine the call handling action for the numbers matching the configured number pattern.
8. Click **Create**, and **Create** again to finish configuring the **Sending Rule**.

Configuring general fax settings

1. Go to **Call Feature > Fax > Setting**.
2. Enter a **System station ID** and **System fax header** that shows on each fax sent from the FortiVoice unit.
3. You can adjust the **Maximum Transmission Rate** and **Minimum Transmission Rate**.
4. The **Enable T.30 ECM (error correction mode)** is enabled by default. This mode can detect and correct errors in the fax page data to make the fax transmission successful.
5. Under **T.38 Fax**, determine whether the FortiVoice unit will resend a T.38 invite if the remote end is unresponsive, and whether the FortiVoice will fallback to G.711 mode if T.38 communication fails.
   A T.38 fax requires significantly less bandwidth, and helps mitigate packet loss.
6. T.38 uses UDP Transport Layer (UDPTL) as its transport protocol. Enter the start and end ports.
7. Under **Send Queue**, set **Max retry times** to the maximum number of times the FortiVoice unit will attempt to resend a fax if the fax is unable to be sent due to busy lines.
8. Set a **Retry interval** to the duration of time in seconds that the FortiVoice unit will wait between retries.
9. Set a **Wait time for an answer** to the wait time for a "go-ahead" signal from the fax receiving terminal.
10. Click **Apply**.

Speed dial numbers

You can import and export speed dial number lists for fast configuration and backup purposes.

To export a speed dial number list

1. Go to **Call Features > Speed Dial > Number**.
2. Click **Export**.
3. Select **Export** to save the speed dial list as a CSV file.
4. Select **Download sample** to learn how to prepare speed dial numbers to import into the FortiVoice unit.

To import a speed dial number list

1. Go to **Call Features > Speed Dial > Number**.
2. Click **Import**.
3. Browse for the number list file.

Extensions

This section includes the following topics:

- Auxiliary phone and secondary account on page 36
- Auto provisioning for FortiFone devices on different subnets on page 37
- Caller ID modification on page 40
- FortiVoice Click-to-dial configuration on Google Chrome on page 48
- Hot desking on page 52
- Local IP extensions on page 55
- Remote extension configuration on page 59

Auxiliary phone and secondary account

You can update an IP extension to enable and configure the following settings:

- **Auxiliary phone**: When you add an auxiliary phone to your extension, you have two phones with the same extension number. The phones will ring at the same time but you can only use one phone to answer the call. This function is useful when you want to access the same extension from two different locations.
- **Secondary account**: When you add a secondary account to your extension, you can set the secondary extension to ring at the same time as your existing extension. However, the secondary extension operates separately. For example, extension 100 sets extension 200 to be a secondary account. When a call comes in to extension 100, both extensions (100 and 200) will ring and you can answer one of them. In that same example, if a call comes into extension 200, only extension 200 will ring.

Adding an auxiliary phone

1. Go to **Extension > Extension > IP Extension**.
2. Double-click the extension that you want to add the auxiliary phone to.
3. In **Device Setting**, click the **Auxiliary Phone** tab.
4. Click **New**.
5. In **Device**, add a new phone or select an existing phone .
6. If you select an existing phone, make sure that it is not assigned.
7. Complete the configuration.
8. To complete the addition of the auxiliary phone, click **Create**.
9. To save the changes to IP extension, click **OK**.

Adding a secondary account

The secondary account setting is available when your extension is using a FortiFone phone, not a generic phone.

1. Enable the secondary account setting:
   a. Go to **System > Advanced > Auto Provisioning**.
   b. In **Other Setting**, enable **Secondary account**.
   c. Click **Apply**.
2. Add a secondary account to an extension:
   a. Go to **Extension > Extension > IP Extension**.
   b. Double-click the extension that you want to add the secondary account to.
   c. In **Device Setting**, click **Advanced**.
   d. Expand **Secondary account**.
   e. In **Account**, select the extension that you want to add as the secondary account.
   f. To save changes to the advanced settings, click **OK**.
   g. To save changes to the IP extension, click **OK**.

Auto provisioning for FortiFone devices on different subnets

When configuring FortiFone IP extensions on your FortiVoice system on a single LAN deployment, they will auto discover utilizing SIP PnP, in which a multicast is sent out on the network.

For FortiFone devices on networks that use a different subnet than FortiVoice, the multicast will not make it across the various subnets. In deployments using different subnets, it is best to use HTTP or HTTPS with Option 66 configured on your DHCP server.

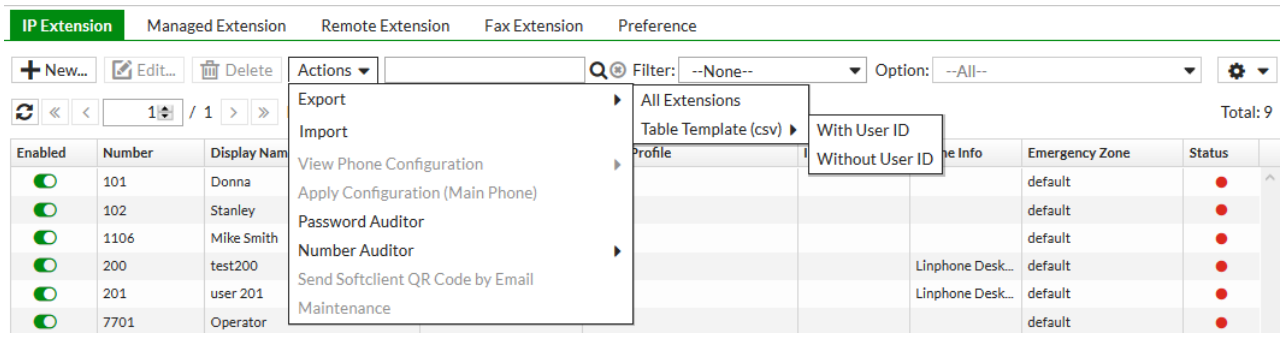
The HTTP and HTTPS protocols increase the reliability of FortiFone devices being able to auto provision across the network. Option 66 set on the DHCP server creates an easy way to have all phones directed towards the FortiVoice system to complete the auto provisioning.

This recipe covers the following best practices for a large deployment of FortiFone devices with the FortiVoice system:

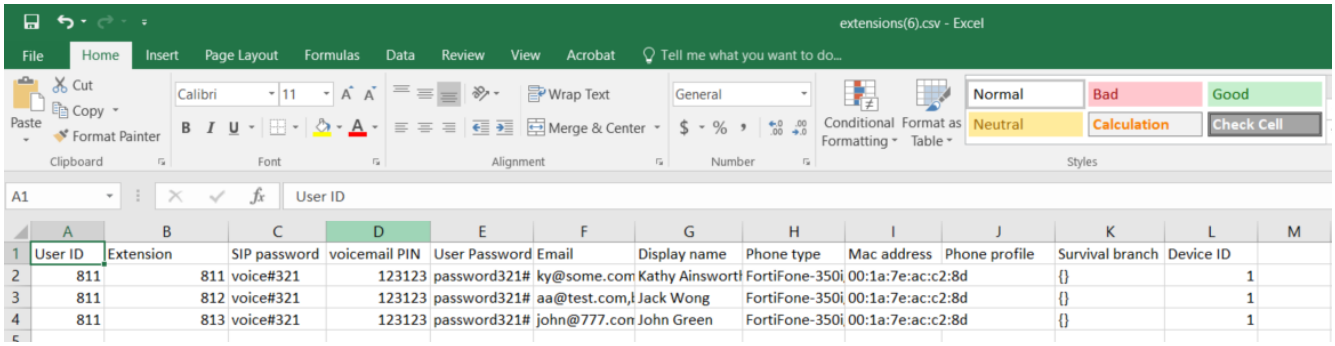
- Downloading and editing the CSV file on page 37
- Importing the CSV file on page 38
- Configuring HTTP or HTTPS protocol support on page 39
- Configuring your DHCP server on page 40

Downloading and editing the CSV file

1. On FortiVoice, go to **Extension > Extension > IP Extension**.
2. Under the **Actions** drop-down, select **Export > Table Template (csv) > With User ID**.
   A sample file will be downloaded entitled **extensions.csv**.



3. Open the newly downloaded sample CSV file.
4. Replace the sample's content with the information for your extensions. Make sure to configure the following sections: **User ID**, **Extension**, **Display Name**, **Phone Type**, and **MAC Address**.



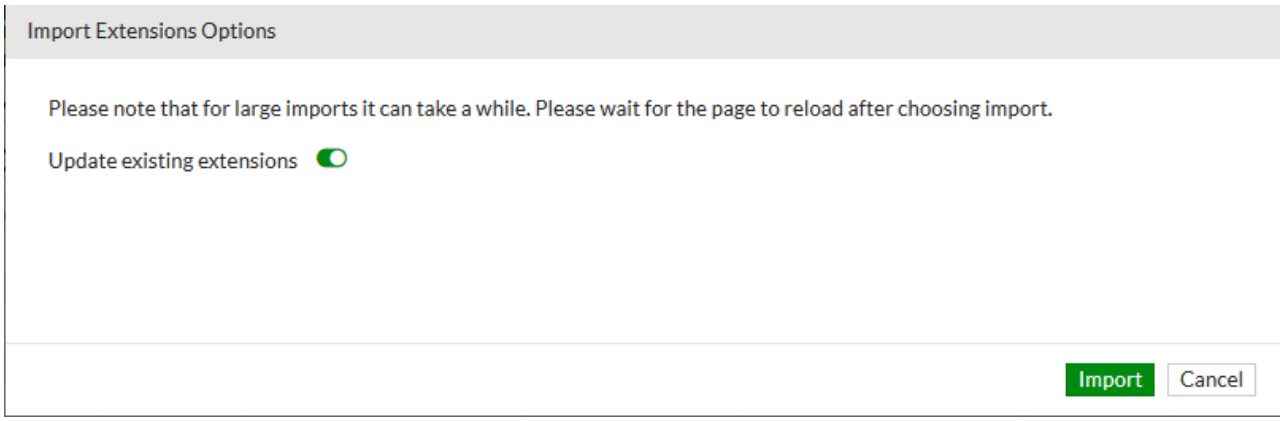
The **Phone Type** must be entered as “FortiFone-XXX”, where “XXX” is your model type (for example, **FortiFone-570**). To see a current list of FortiFone models, go to **Phone System > Profile > Phone**.

The **MAC Address** sections must be populated as “xx:xx:xx:xx:xx:xx”. FortiVoice will automatically format the MAC address once the CSV file is imported.

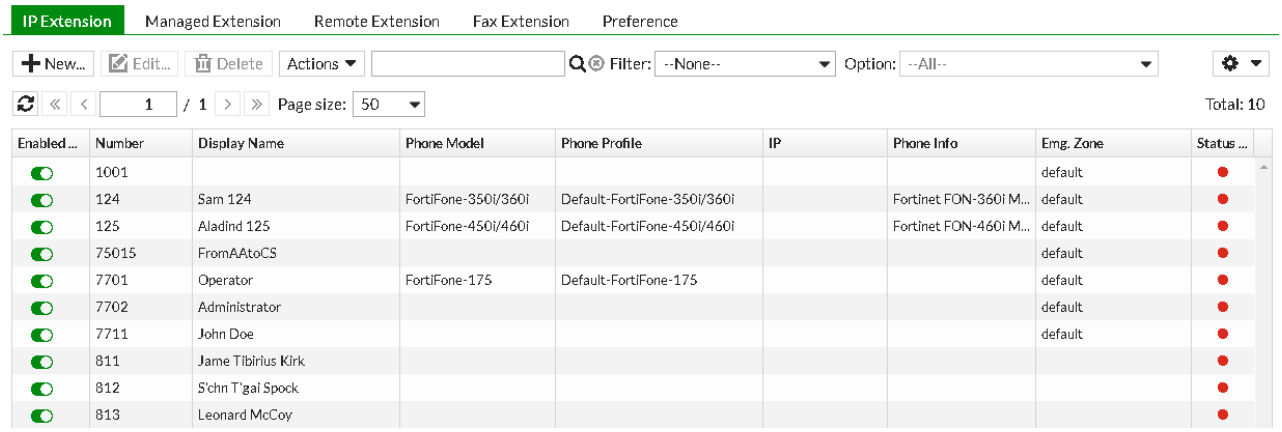
If a custom phone profile using the default settings is in use, the **Phone profile** section will also need to be configured.

Importing the CSV file

1. Go to **Extension > Extension > IP Extension**.
2. Under the **Actions** drop-down, select **Import**.
3. Navigate to and select the configured CSV file and select **OK**.
   A window will appear stating that large imports can take a while, with **Update existing extensions** enabled.
4. Select **Import**.



5. Review your list of pre-existing and newly imported extensions.

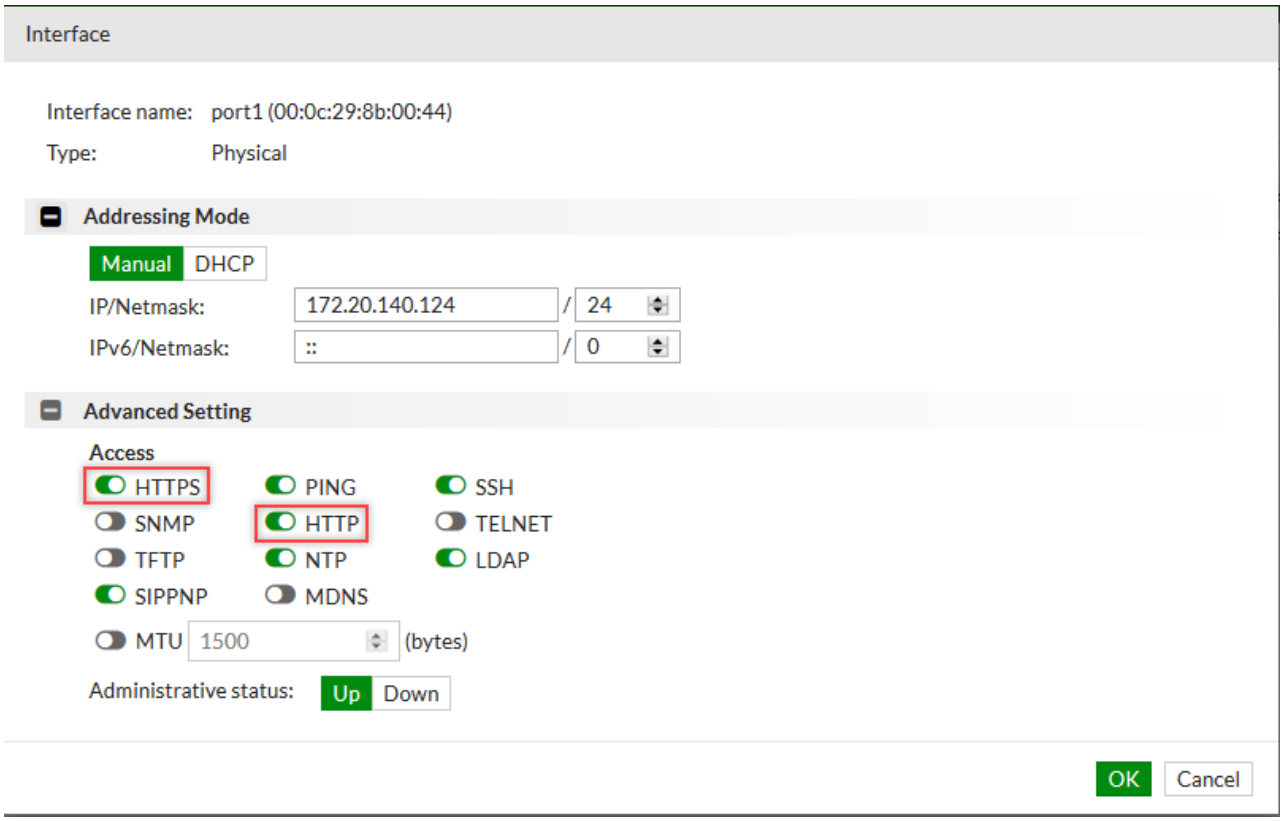


Enabled ...	Number	Display Name	Phone Model	Phone Profile	IP	Phone Info	Emg. Zone	Status ...
	1001						default	
	124	Sam 124	FortiFone-350i/360i	Default-FortiFone-350i/360i		Fortinet FON-360i M...	default	
	125	Aladind 125	FortiFone-450i/460i	Default-FortiFone-450i/460i		Fortinet FON-460i M...	default	
	75015	FromAAtoCS					default	
	7701	Operator	FortiFone-175	Default-FortiFone-175			default	
	7702	Administrator					default	
	7711	John Doe					default	
	811	Jame Tibirius Kirk						
	812	S'chn T'gai Spock						
	813	Leonard McCoy						

Configuring HTTP or HTTPS protocol support

For successful auto provisioning to occur across multiple subnets, the HTTP or HTTPS protocols must be enabled on the FortiVoice network interface.

1. Go to **System > Network > Network**.
2. Select the network interface in use (in this example, **port1**) and select **Edit**.
3. Expand **Advanced Setting**.
4. Under **Access**, make sure **HTTP** and/or **HTTPS** is enabled, then select **OK**.



5. Go to **System > Advanced > Auto Provisioning**.
6. Under **Auto Provisioning**, select **Enabled** (and optionally enable **Unassigned phone**).
7. Set **Provisioning protocol** to either **HTTPS** or **HTTP**, and select **Apply**.

Configuring your DHCP server

1. On your DHCP server, configure the following settings:
   a. Option 66 to the protocol in use
   b. IP address of FortiVoice
   c. Protocol port number
   d. Provisioning folder (for example, *http://192.168.1.99:80/provisioning/*, or *https://192.168.1.99:443/provisioning/*)
2. The protocol ports can be changed from their default values on FortiVoice by going to **System > Configuration > Option**. Make note of any changes made on FortiVoice.
3. After configuring the DHCP settings, connect FortiFone devices to the network. If they are already connected, reboot them.

Caller ID modification

For outbound calls from the FortiVoice unit, you can customize the caller ID to be any name, number, or both. As there are multiple areas where you can modify the caller ID within the FortiVoice UI, there is a hierarchy to which the caller ID

modification takes precedence. This recipe details the caller ID modification hierarchy to help you decide how to configure your FortiVoice caller IDs.

The hierarchy of caller ID modification options is different for a normal call or an emergency call.

This section includes the following topics:

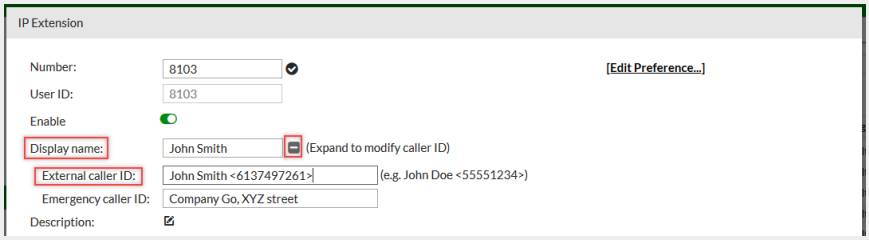
- Caller ID modification hierarchy for normal calls on page 41
- Caller ID modification hierarchy for emergency calls on page 44

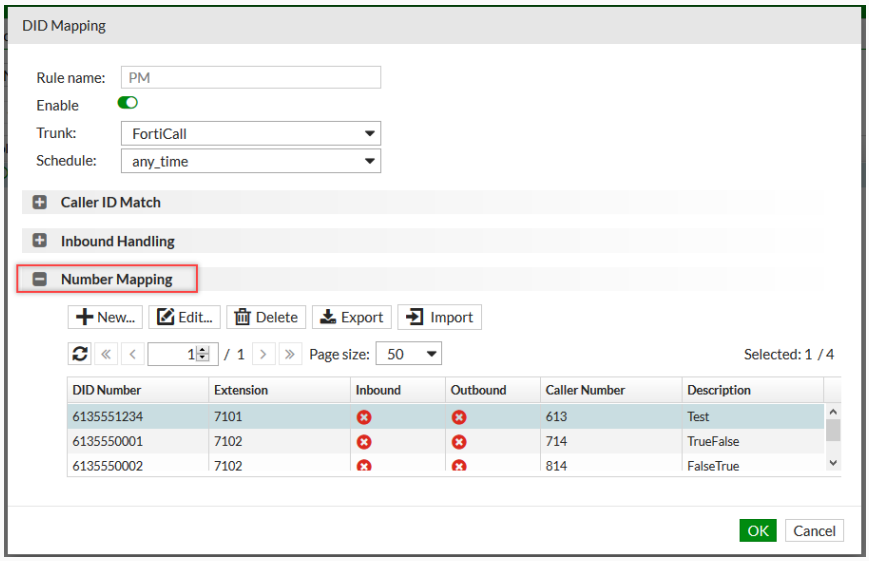
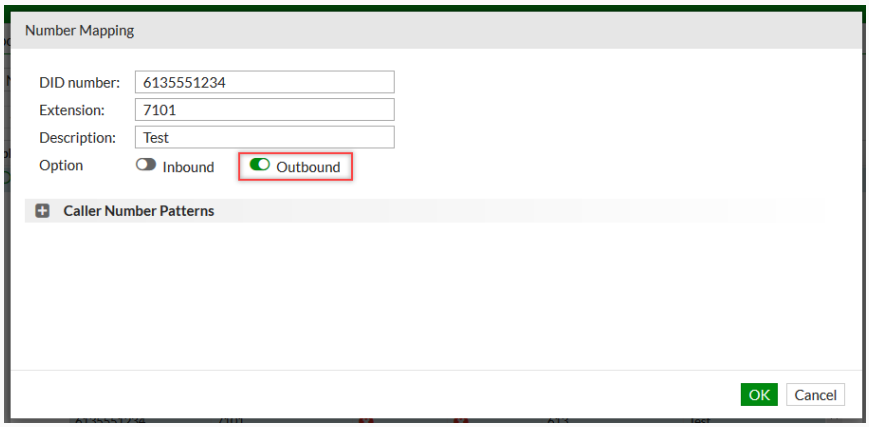
Caller ID modification hierarchy for normal calls

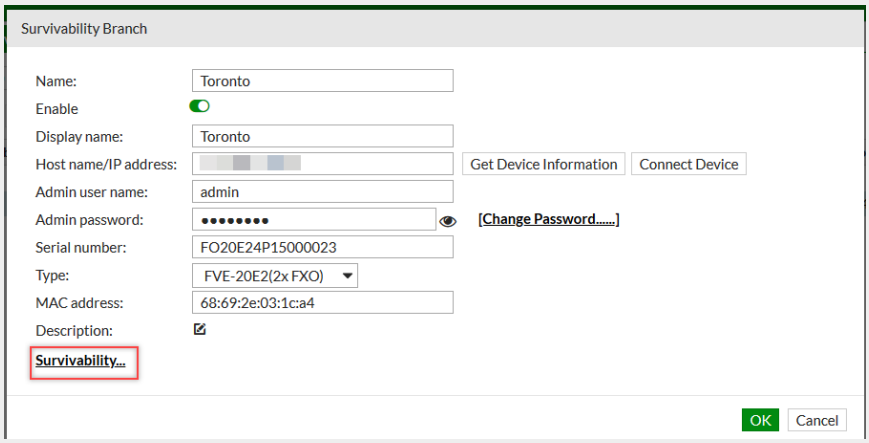
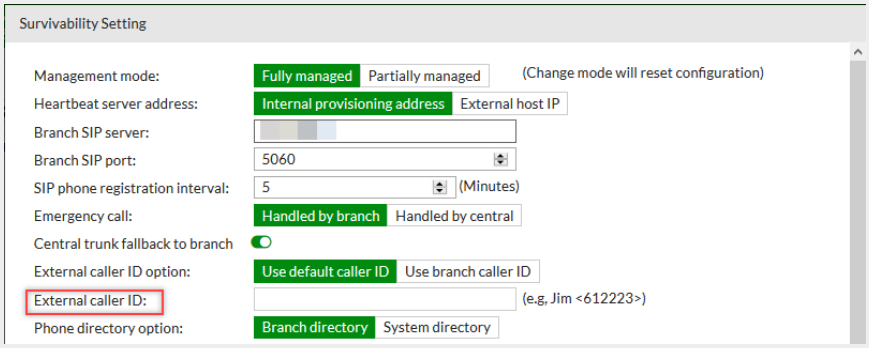
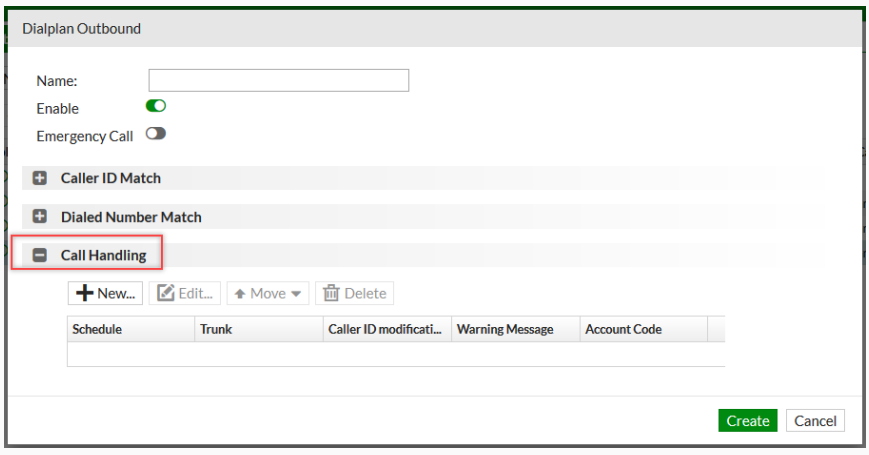
A normal call is any outbound call that is not an emergency call, as defined by the regional emergency number settings.

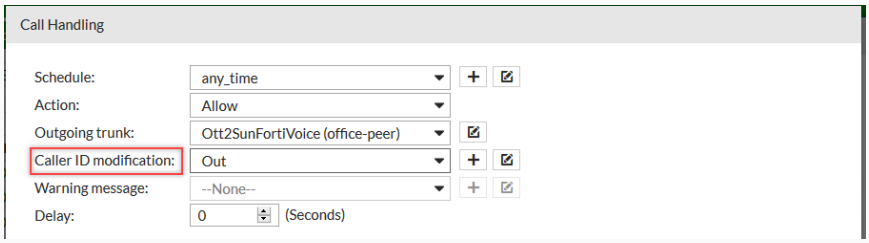
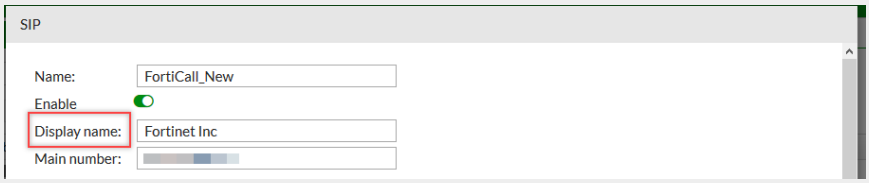
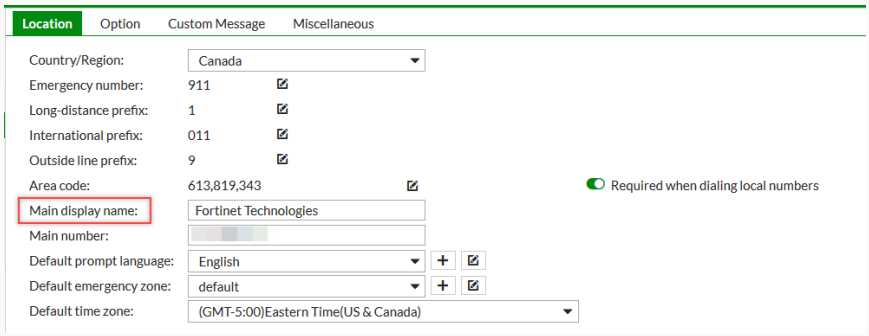
The following table displays the caller ID modification options available on normal calls from the highest priority (1) to the lowest priority (6).

For example, if you configure the caller ID settings using the direct inward dialing (DID) number mapping (priority 2) and the Caller ID modification (priority 4), the FortiVoice unit displays the caller ID configured using the DID number mapping because this setting has a higher priority.

Priority	Setting	Steps
1	External caller ID	1. Go to **Extension > Extension > IP Extension**. 2. Edit an extension or create a new one. 3. Go to **Display name** and click to expand. 4. In **External caller ID**, enter the caller ID such as a name and number (example, John Doe <55551234>). 5. Click **OK** or **Create**, as applicable. 
2	DID number mapping	1. Go to **Call Routing > Inbound > DID Mapping**. 2. Edit a rule or create a new one. 3. Under **Number Mapping**, create a new DID number mapping or edit an existing one.

Priority	Setting	Steps
		 4. In **Option**, select **Outbound**. 5. Click **OK** or **Create**, as applicable. 
3	External caller ID, survivability setting for local survivable gateway (LSG)	1. Go to **Managed System > Survivability > Survivability Branch**. 2. Edit an existing branch or create a new one. 3. Click **Survivability**.

Priority	Setting	Steps
		 4. In **External caller ID**, enter a caller ID such as a name and number (example, Jim <612223>). 5. Click **OK** or **Create**, as applicable. 
4	Caller ID modification	1. Go to **Call Routing > Outbound > Outbound**. 2. Edit an existing rule or create a new one. 3. In **Call Handling**, edit an existing rule or create a new one.  4. In **Caller ID modification**, select an existing profile or create a new one.

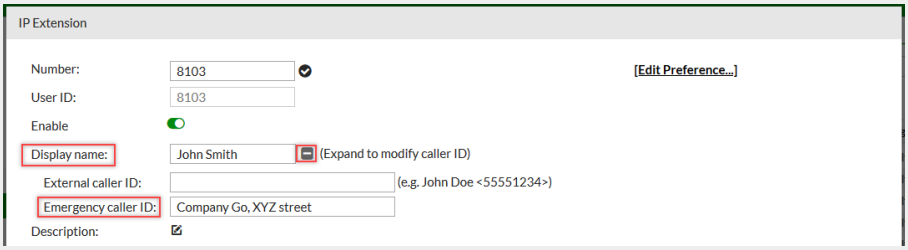
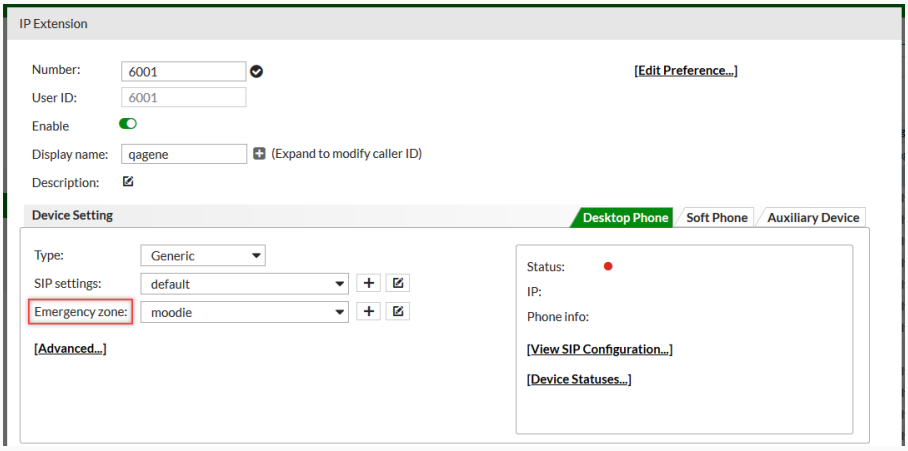
Priority	Setting	Steps
		5. Click **OK** or **Create**, as applicable. 
5	Trunk display name	1. Go to **Trunk > VoIP > SIP**. 2. Edit an existing trunk or create a new one. 3. In **Display name**, enter a name. 4. Click **OK** or **Create**, as applicable. 
6	Location main display name	1. Go to **Phone System > Setting > Location**. 2. In **Main display name**, enter the name displaying on the FortiVoice phone system unit. Your PSTN provider assigns this name. 3. Click **OK** or **Create**, as applicable. 

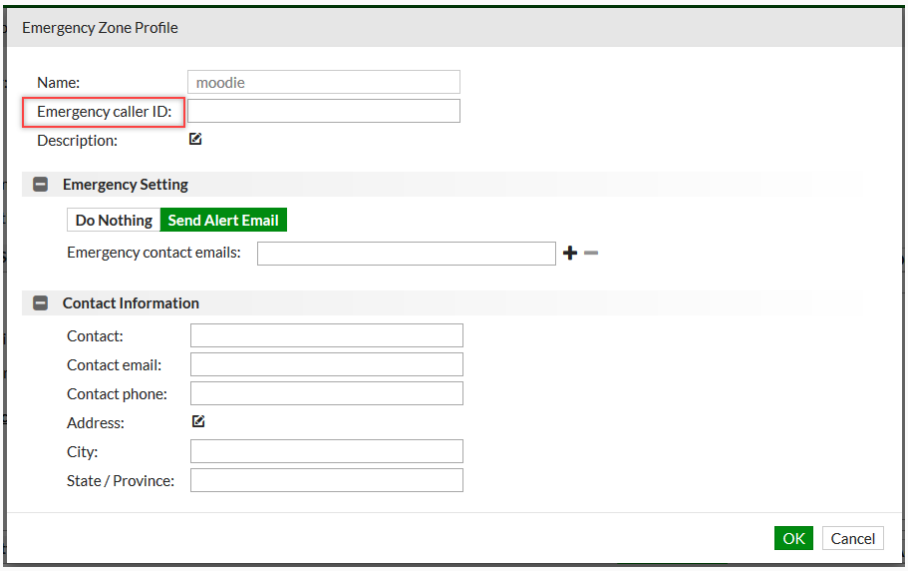
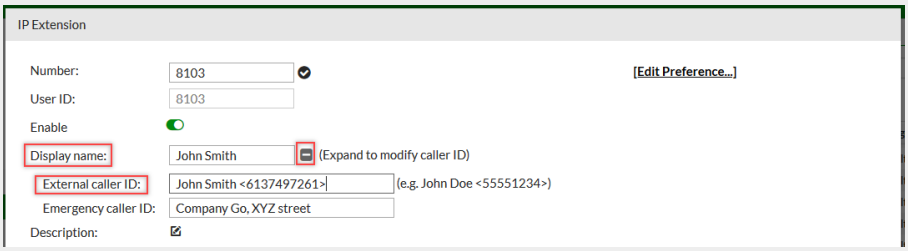
Caller ID modification hierarchy for emergency calls

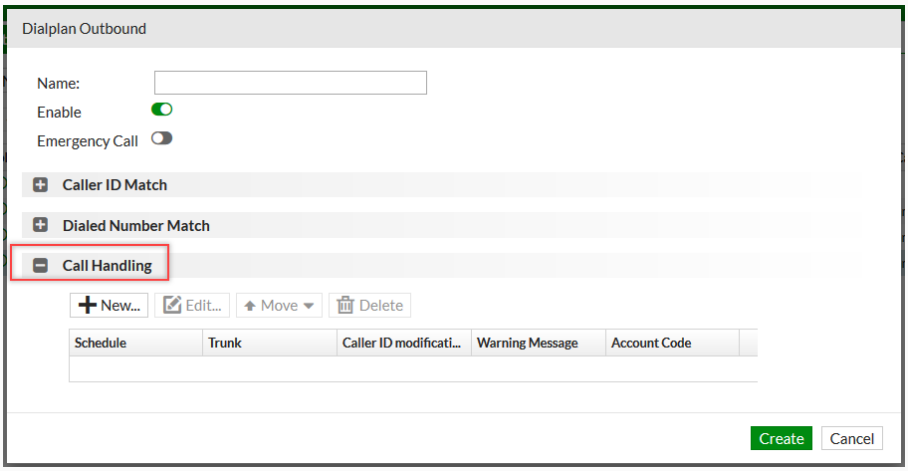
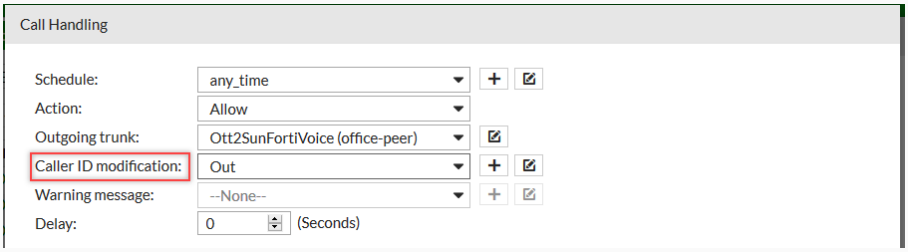
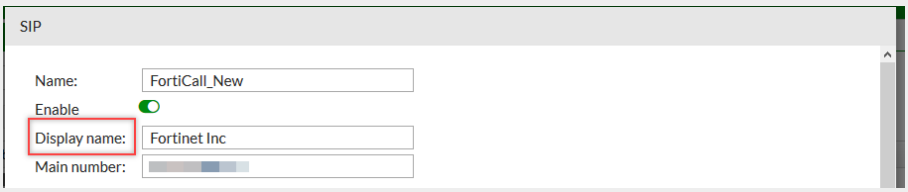
When you place an emergency call, the hierarchy for caller ID modification changes to alert emergency services about the correct location of the caller.

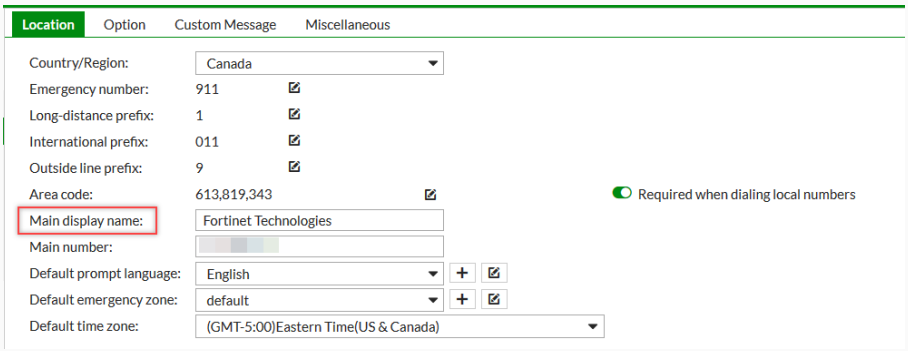
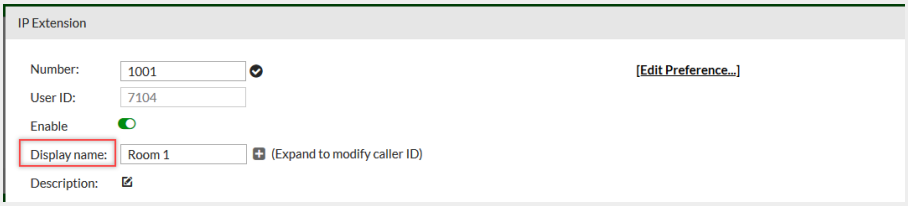
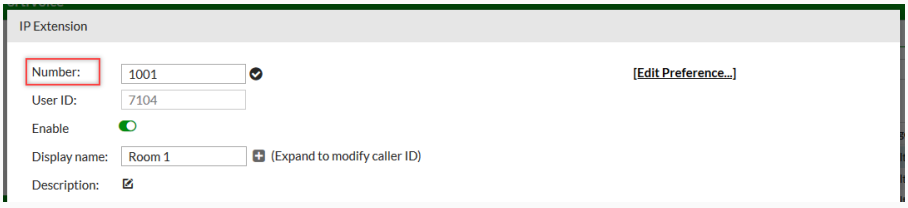
The following table displays the caller ID modification options available on emergency calls from the highest priority (1) to the lowest (8).

For example, if you configure the caller ID settings using the Extension emergency caller ID (priority 1) and the Extension external caller ID (priority 3), the FortiVoice unit displays the caller ID configured using the Extension emergency caller ID because this setting has a higher priority.

Priority	Setting	Steps
1	Extension emergency caller ID	1. Go to **Extension > Extension > IP Extension**. 2. Edit an extension or create a new one. 3. Go to **Display name** and click to expand. 4. In **Emergency caller ID**, enter the caller ID to display on the destination phone when you dial the emergency number. 5. Click **OK** or **Create**, as applicable. 
2	Emergency zone caller ID (Extension setting)	1. Go to **Extension > Extension > IP Extension**. 2. Edit an extension or create a new one. 3. In **Emergency zone**, select a profile or create a new one.  4. In **Emergency caller ID** of the profile, enter the caller ID to display on the destination phone when you dial the emergency number. 5. Click **OK** or **Create**, as applicable.

Priority	Setting	Steps
		
3	Extension external caller ID	1. **Extension > Extension > IP Extension**. 2. Edit an extension or create a new one. 3. Go to **Display name** and click to expand. 4. In **External caller ID**, enter the caller ID such as a name and number (example, John Doe <5551234>). 5. Click **OK** or **Create**, as applicable. 
4	Caller ID modification	1. **Call Routing > Outbound > Outbound**. 2. Edit an existing rule or create a new one. 3. In **Call Handling**, edit an existing rule or create a new one.

Priority	Setting	Steps
		 4. In **Caller ID modification**, select an existing profile or create a new one. 5. Click **OK** or **Create**, as applicable. 
5	Trunk display name	1. Go to **Trunk > VoIP > SIP**. 2. Edit an existing trunk or create a new one. 3. In **Display name**, enter a name. 4. Click **OK** or **Create**, as applicable. 
6	Location main display name	1. Go to **Phone System > Setting > Location**. 2. In **Main display name**, enter a name. 3. Click **OK**.

Priority	Setting	Steps
		
7	Extension display name	1. Go to **Extension > Extension > IP Extension**. 2. Edit an extension or create a new one. 3. In **Display name**, enter the name to display on the destination phone calling this extension. 4. Click **OK** or **Create**, as applicable. 
8	Extension number	1. Go to **Extension > Extension > IP Extension**. 2. Edit an existing extension to change its extension number or create a new extension and enter an extension number. 3. Click **OK** or **Create**, as applicable. 

FortiVoice Click-to-dial configuration on Google Chrome

FortiVoice Click-to-dial is a Google Chrome extension that allows you to click on a phone number on a website and call them from your desk phone. This recipe details the steps required to install and set up the extension from the Chrome Web Store.

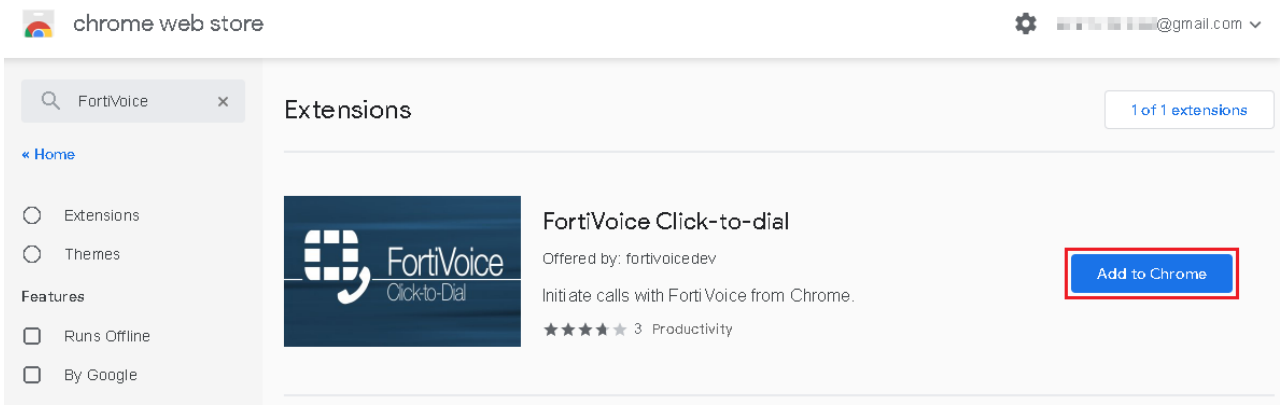
This section includes the following recipes:

- Installing FortiVoice Click-to-dial on page 49
- Configuring FortiVoice Click-to-dial on page 50

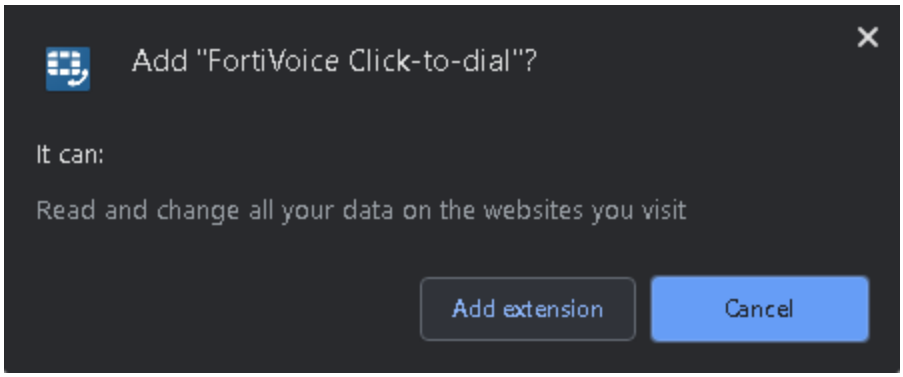
- Using FortiVoice Click-to-dial on page 51

Installing FortiVoice Click-to-dial

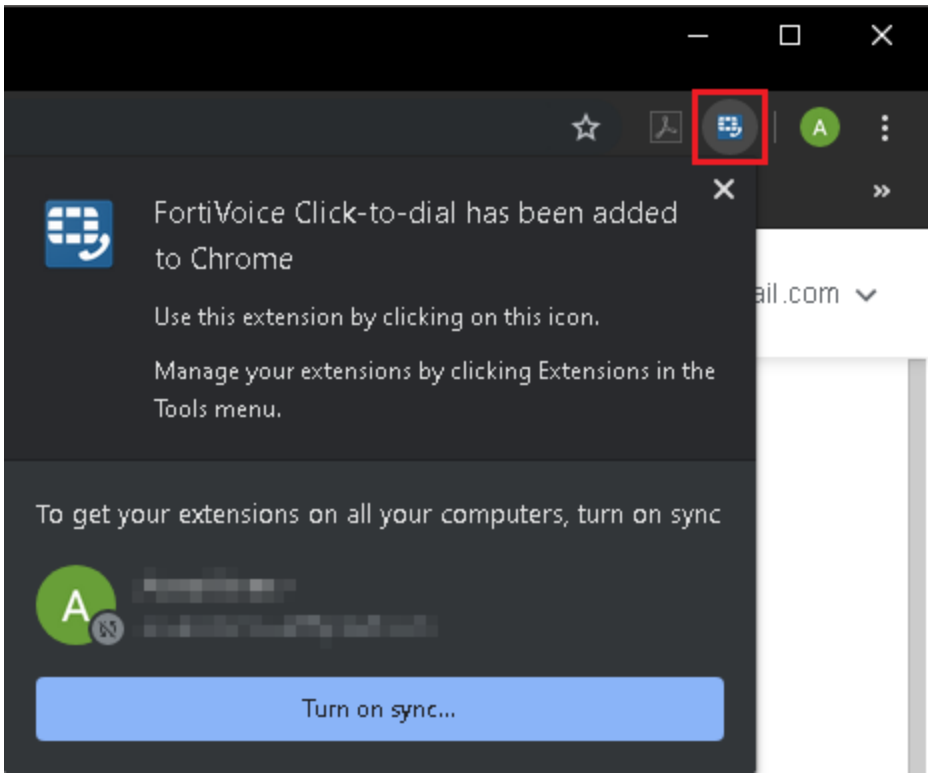
1. Start the Google Chrome web browser and go to the Chrome Web Store.
2. Search for **FortiVoice**.
   Google Chrome displays **FortiVoice Click-to-dial**.
3. Select **Add to Chrome**.



4. In the confirmation window select **Add extension**.

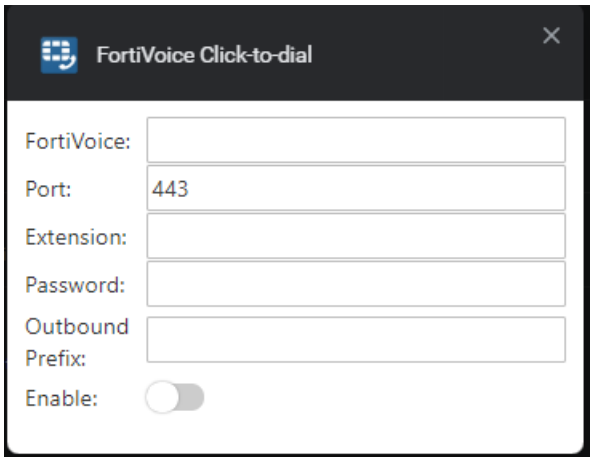


5. After the installation is complete, the FortiVoice Click-to-dial icon appears in the search bar.



Configuring FortiVoice Click-to-dial

1. Right-click on the Click-to-dial icon and select **Options**.
2. Complete the following fields:
   - **FortiVoice**: The IP address or FQDN of the FortiVoice device. If on the same network as the FortiVoice, enter the private IP address.
   - **Port**: The HTTPS port used by FortiVoice (443 by default).
   - **Extension**: The extension number of the user.
   - **Password**: The PIN code or password for that extension (the same as the voicemail PIN).
   - **Outbound Prefix**: (Optional) If required to dial an outbound code before the number, such as 9.
   - **Enable**: Turn on the extension.



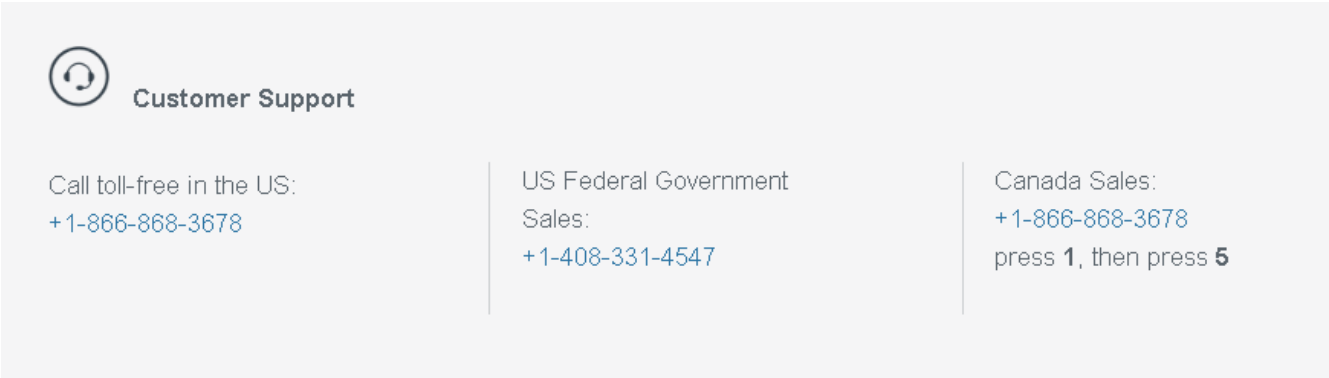
Note that the following errors can appear when you attempt to enable the extension:

- **Connection error**: Indicates that the **IP/FQDN** or **Port** is incorrect, or if the firewall is not routing the traffic correctly if attempting to use externally.
- **Invalid credentials**: Indicates that the wrong **Password** has been entered.

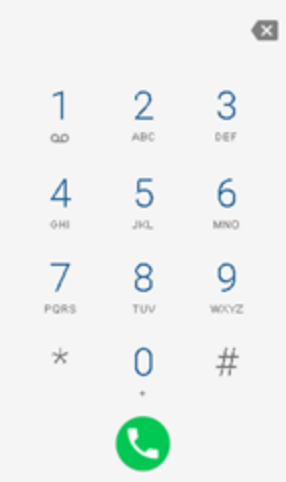
If the **Enable** toggle remains on, the configuration is correct.

Using FortiVoice Click-to-dial

After the configuration is complete, any web page that contains a phone number will be highlighted; click on the number to initiate the call from your extension.



Alternatively, you can select the Click-to-dial icon to open the phone dialer and manually enter the phone number.



Hot desking

Hot desking enables a user to log in to an unassigned phone and take total control of that phone by applying all of their own phone settings until logging out.

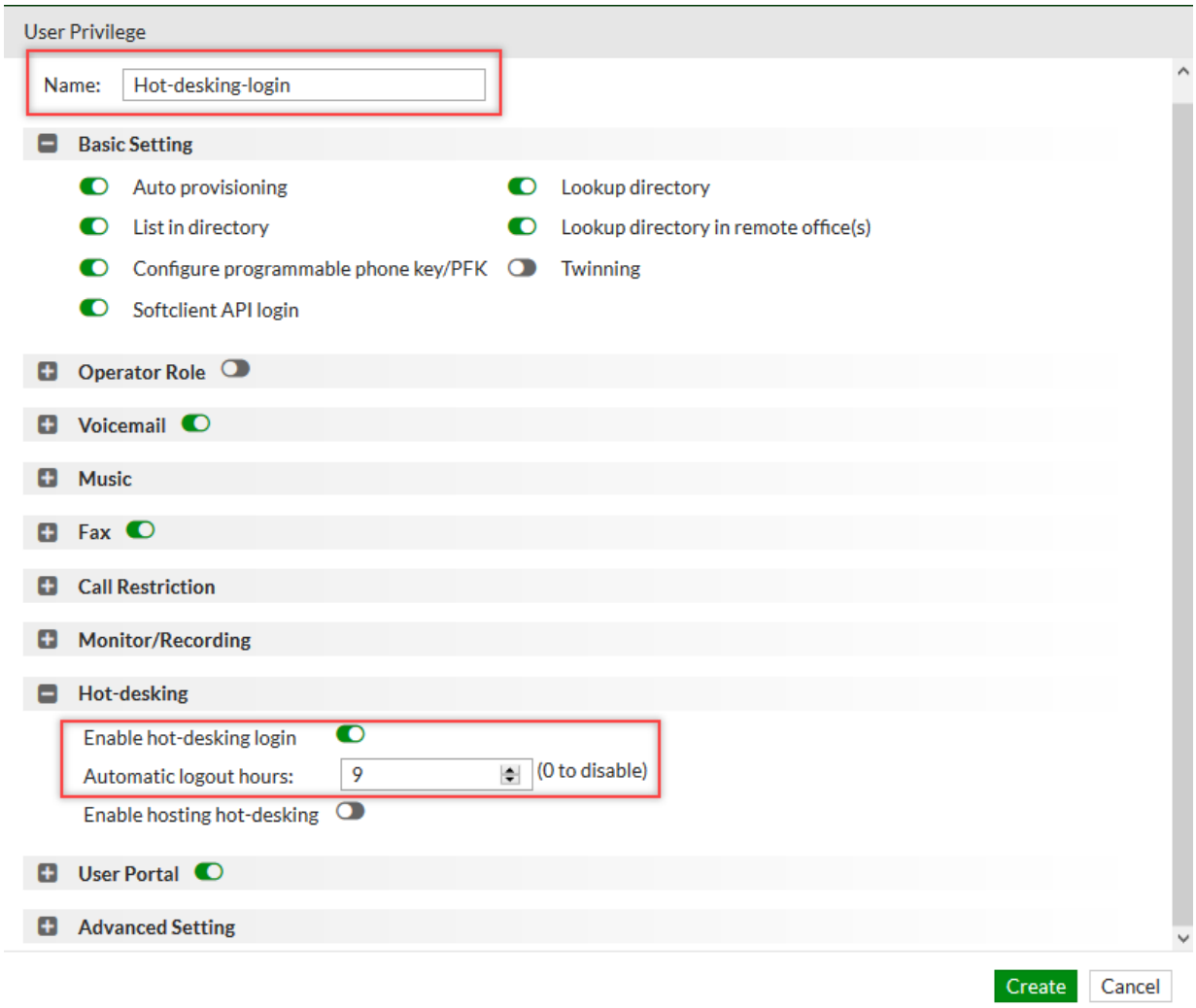
Hot desking is particularly useful in a call center or sales office environment where users need to be able to sit at any desk and use their phone extension.

The hot-desking configuration requires two phones:

- Registered phone: This phone has an extension and is used to log in to a hot-desking host. This extension requires a user privilege with the hot-desking login enabled.
- Unassigned phone: This phone is the hot-desking host which users log in to. The unassigned phone has no extension and does not require a user privilege.

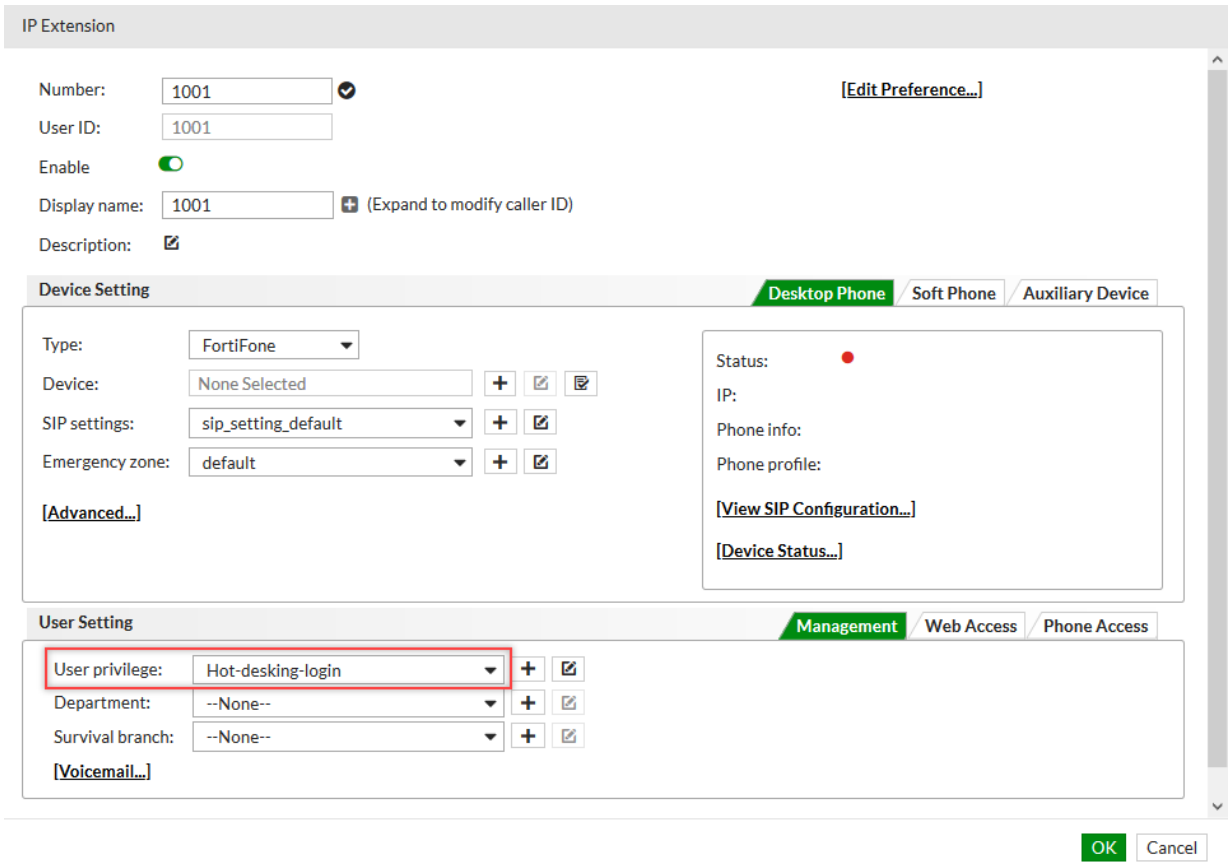
Configuring hot desking

1. Log in to the FortiVoice web-based manager.
2. Create a user privilege to enable hot-desking login:
   a. Go to **Phone System > Profile > User Privilege**.
   b. Click **New**.
   c. In the **Name** field, add a name for this user privilege.
   Note: The **Name** field does not support the following characters: space, quotation mark, and backward slash.
   d. Select **Enable hot-desking login** to allow phones associated with this user privilege to log in to other phones.
   e. In the **Automatic logout hours** field, enter the time in hours after which the phone automatically logs out of hot desking.



f. Click **Create**.

3. Associate the user privilege (example, Hot-desking-login) to the extension used for logging in to another phone:
   a. Go to **Extension > Extension > IP Extension**.
   b. Double-click on the row of the extension number (example, 1001) that wants to log in to other phones.
   c. From the **User privilege** drop-down list, select the user privilege (example, Hot-desking-login) that you created in step 2.



d. Click **OK**.

Using hot desking on FortiFone

1. On the FortiFone unit that you want to log in to, dial *11.
2. Enter your extension number (example, 1001#) and user PIN.
   Depending of the phone model, the FortiFone unit may reboot.
   The new extension and name display on the FortiFone screen.
3. To place a call, dial an extension (example, 3004).
   The screen of the receiving FortiFone unit displays the extension number (example, 1001).
4. To log out of the FortiFone unit, dial *12.
   Depending of the phone model, the FortiFone unit may reboot.

Viewing activity details of hot-desking extensions

1. Go to **Monitor > Extension & Device > Hot Desking**.
   When an extension is used for logging in or logging out of a hot-desking host, FortiVoice populates the table. The table includes one row for each extension, not multiple rows. If the table is empty, then none of the extensions have used hot desking.

2. For the extension that is logged in to a phone or has logged out, you can view the following hot-desking details:
   - **Status**: The status of the hot-desking extension as logged in or logged out.
   - **Number**: The number of the hot-desking extension.
   - **Display Name**: The name displayed on the phone that is hosting hot desking.
   - **Host Device**: The MAC address of the unassigned phone. This is the phone that a hot-desking user logs into. When the status of the hot-desking extension is "Logged out", then the host device is blank.
   - **Last Login**: The last login performed on the hosting phone.
   - **Expiry**: The expiry time (in the yyyy-mm-dd hh:mm:ss format) of the hot-desking login. The value is set in the **Automatic logout hours** field of the user privilege for the hot-desking login. When the status of the hot-desking extension is "Logged out", the expiry time is all zeros.

Local IP extensions

FortiVoice allows you to configure IP phone extensions, edit analog extensions, and determine extension preferences.

This recipe shows how to configure an internal IP extension, a phone connected on the same LAN as the system. An external IP extension is a phone connected outside the LAN.

This section includes the following recipes:

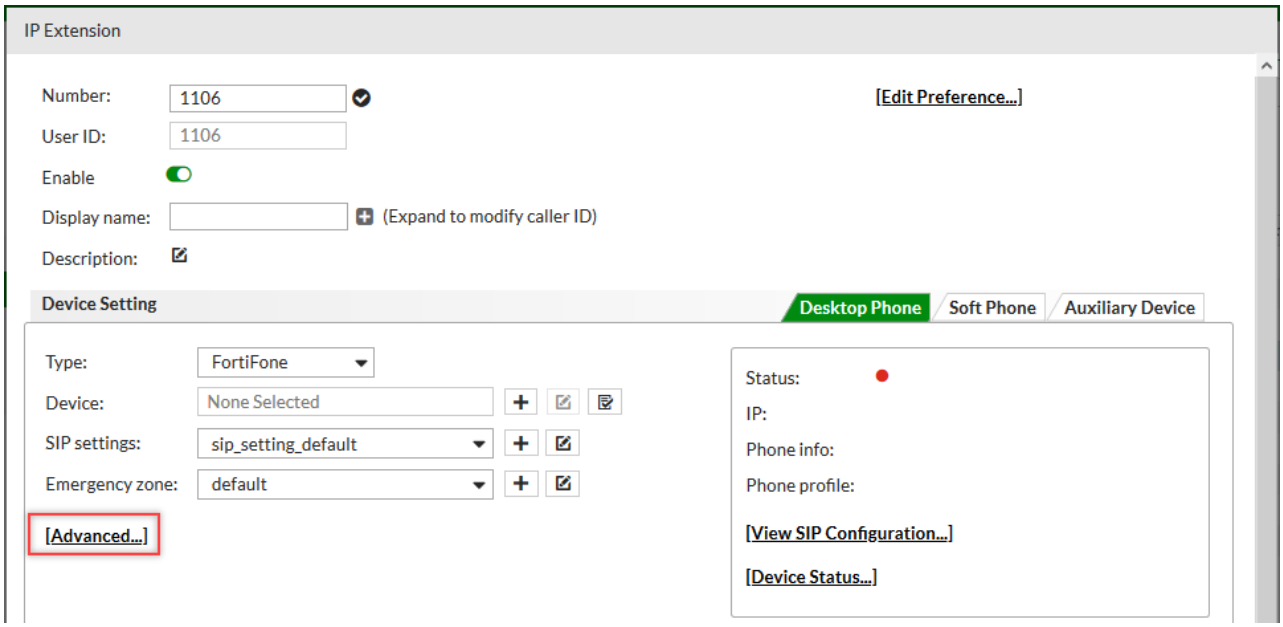
- Configuring extension settings on page 55
- Configuring notification options on page 58

Configuring extension settings

1. Go to **Extension > Extension > IP Extension** and click **New** (or select and **Edit** an existing extension).
2. Enter an extension **Number**. A green check mark will appear to indicate that the number entered is **Available**. FortiVoice auto-populates the **User ID** field.
3. Enter a **Display name** for the user. This is the name that appears on the phone screen when receiving a call from this extension.

Configuring device settings

1. In the **Device Setting** section, you can determine whether the IP extension is assigned as either a **Desktop Phone**, **Soft Phone**, or an **Auxiliary Device**. For this example, stay on the **Desktop Phone** tab, and set the **Type** to **FortiFone** from the drop-down menu.
2. For **Device**, click **New**, where you can enter the extension's device **MAC address**, **Phone model**, and assign a **Phone profile**.
3. Assign an appropriate SIP profile from the **SIP settings** drop-down, and assign an **Emergency zone**.
4. Then click **Advanced** to open the desktop phone advanced settings.



5. Enter or **Generate** a **SIP password**, and set **Location** to **Internal**.
   Note that IP extensions that are designated as **Internal** are those extensions that do not traverse through NAT to connect to the FortiVoice unit. Select **External** if the extension does require NAT.
6. Optionally, enable message waiting indication (**MWI**), **Auto answer**, and **Direct call**. Then click **Create**.

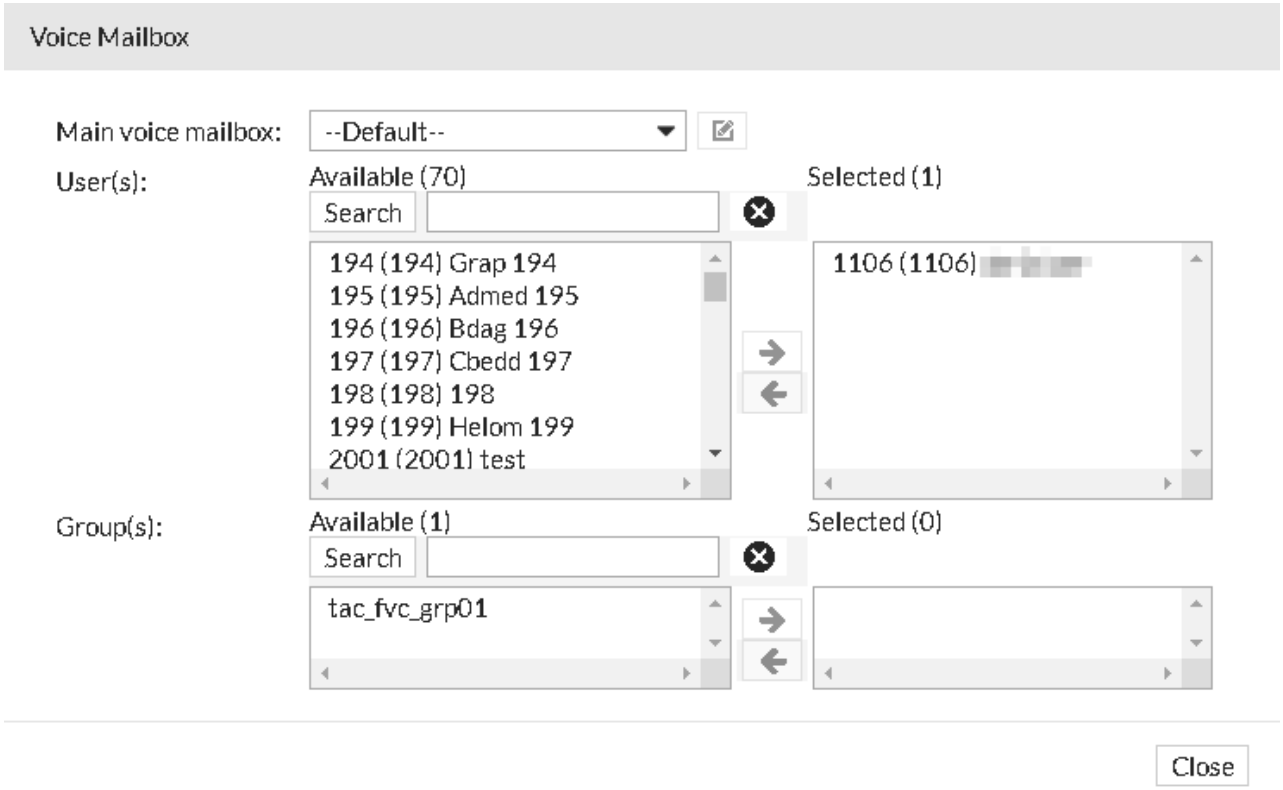
Configuring user settings

1. In the **User Setting** section, under the **Management** tab, assign a **User privilege**, the **Department** the extension belongs to, and a **Survival branch** profile.
   See Configuring voicemail on page 56 for information on configuring the **Voicemail** settings.
2. Under the **Web Access** tab, set **Authentication type** to **Local** and enter or **Generate** a **User password**.
3. A warning may appear indicating that the system password policy is disabled. If this is the case, click **Password policy is disabled** to enable **Password/PIN Policy**, and configure the minimum requirements for passwords as appropriate.
4. Under the **Phone Access** tab, enter or **Generate** a **Voicemail PIN** and **Personal code**. These are used by the extension user to access their voicemail and the FortiVoice user portal, and to make restricted calls, respectively.

Configuring voicemail

1. In the **User Setting** section, under the **Management** tab, click **Voicemail**.
2. Set **Main voice mailbox** to the extension's own voice mailbox or that of another extension as the voice mailbox of this extension. Typically, you will use the default mailbox.

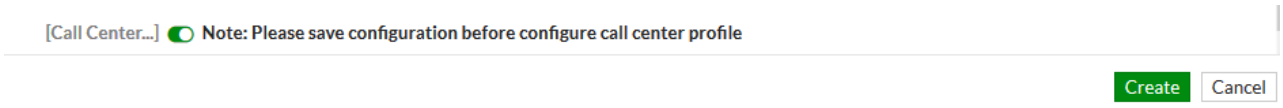
3. From the **Users (s)** and **Groups(s)** tables, assign those users and groups you wish to notify when a new voicemail is received.
4. Click **Close**.



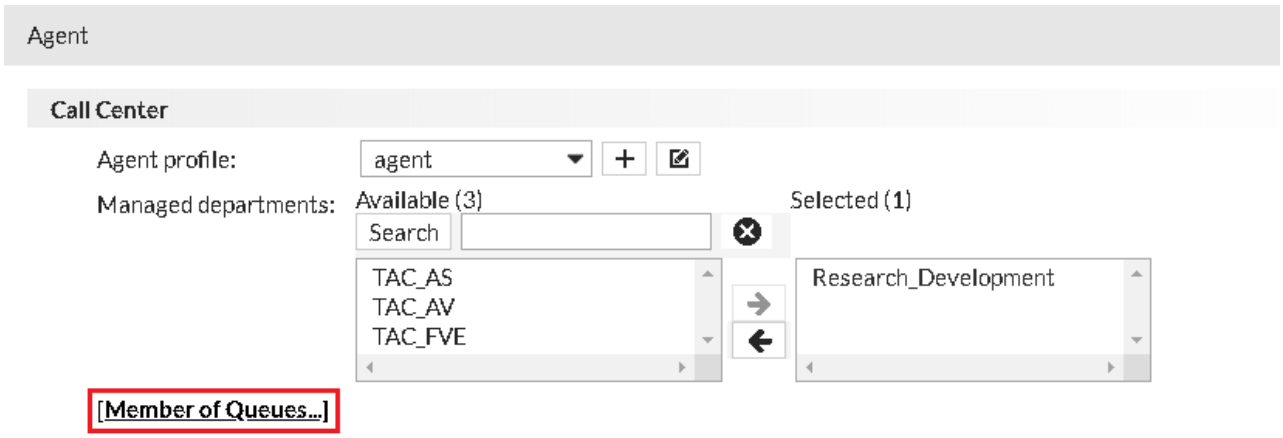
Configuring call center

You can enable the call center option, if you have purchased a call center license and uploaded that license on FortiVoice.

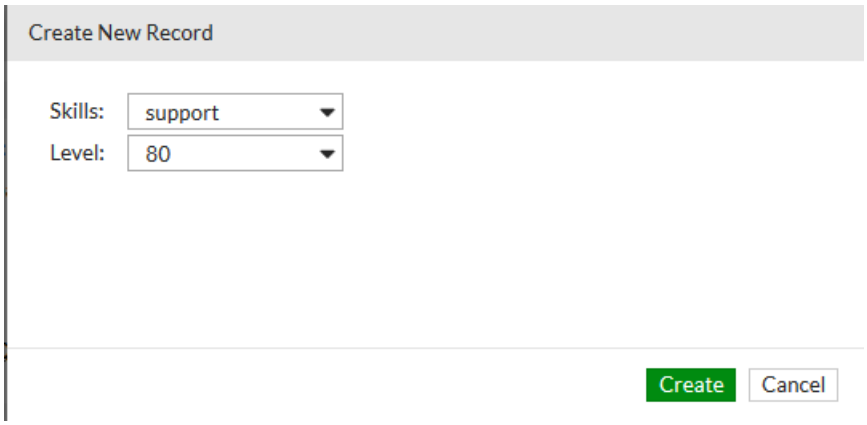
1. When you have completed the configuration of the various IP extension settings, enable **Call Center**. Call center profiles can only be configured once the IP extension configuration has been saved. Click **Create**.



2. Select the newly created IP extension from the list, click **Edit**, and click **Call Center**.
3. Under **Call Center**, assign an **Agent profile** from the drop-down menu. For example, you can designate the extension as either a call center **agent** or **manager**.
4. An agent, or especially a manager, may need to monitor call queues in certain departments. From the **Managed departments** table, assign those departments you wish to be monitored.
5. Click **Member of Queues**.



6. Set **Main/Outgoing queue** to the primary queue for collecting the outgoing calls from all queues by this agent.
7. From the **Queues** table, assign the queues you want the extension to be a member of.
8. Click **OK** when finished.
9. Under **Skill Sets**, click **New**.
10. Assign the appropriate skill and skill level for the agent from the drop-down menu. For more information on agent skill and skill-based routing, see Skill-based routing on page 13.



11. Click **Create**, and **OK** to complete configuring the **Call Center**, and **OK** again to complete configuring the **IP Extension**.

Configuring notification options

You can set up the options to receive an email when you receive a voicemail or fax and miss a phone call.

1. Go to **Extension > Extension > IP Extension**.
2. Double-click on an extension.
3. Click **Edit Preference**.
4. In **Notification Options**, update the **Voicemail** and **Fax** settings, as applicable.
5. If you want to be notified when you miss an incoming phone call, enable **Missed call**.
6. Enter the **email address** to send the notification to.
7. Click **OK**.

Remote extension configuration

Callers can connect to remote extensions through auto attendants or through call cascade transfers. A remote extension reaches an external phone by automatically selecting a line from a trunk and dialing the phone number. For example, a remote extension could reach an employee's cell phone or home phone, or a phone at a branch office.

This recipe guides you through the process of configuring a remote extension. It is assumed that an auto attendant is already established.

Remote extensions are designed to operate with most major telephone service providers. Unfortunately, phone numbers and mobile phones roaming internationally may not support remote extensions.

This section includes the following topics:

- Adding a remote extension on page 59
- Testing a remote extension on page 59

Adding a remote extension

1. Go to **Extension > Extension > Remote Extension** and click **New**.
2. Set **Number** to the local extension number from which calls are transferred to a remote extension.
3. Enter the **Remote number**. Calls to the local extension are transferred to this remote number.
4. Click **Enable**.
5. Enter a **Display name**, and expand to modify the caller ID.
6. Under **User Setting**, in the **Management** tab, apply a **User privilege** rule and a **Department**, if required.
7. Click **Voicemail** to assign a voice mailbox, and optionally allow other users and/or groups to access the same voice mailbox. For example, you may want others to access the mailbox when you are away.
8. In the **Web Access** tab, select the appropriate **Authentication type**.
9. Enter the **User password**, for local authentication extensions.
10. In the **Phone Access** tab, set **Voicemail PIN** to the PIN for the user to access voicemail.
11. Click **Create**.

Testing a remote extension

1. Call the auto attendant associated with the FortiVoice unit, which dials the local extension.
2. When the extension's user is not available to answer the call, the call is transferred to the configured remote extension. For example, the user's cell phone number.
3. The user will receive the call through their remote extension.

High availability

With FortiVoice high availability (HA), you set up redundancy between two FortiVoice units in case of a system failure. FortiVoice HA uses an active-passive mode which means that you have a primary (active) unit and a secondary (passive) unit. These two units make up an HA group. The secondary unit is not used until a failure occurs on the primary unit and triggers the secondary unit to assume the responsibilities of the primary unit.

FortiVoice HA units use a heartbeat link to communicate. This heartbeat link lets the secondary unit know that the primary unit is up and running, and allows the primary unit to copy configuration and data information to the secondary unit whenever the primary configuration changes. If a failure occurs on the primary unit, the loss of the heartbeat triggers the secondary unit to take over as the primary and be a copy of that primary unit.

This section includes the following recipes:

- Planning high availability on page 60
- Configuring high availability on FortiVoice units on page 61
- Configuring service-based failover on page 63
- Synchronizing configuration and data in a FortiVoice HA group on page 64
- Installing licenses on a FortiVoice HA group on page 64
- Enabling high availability activity logging on page 65
- Displaying the high availability status on page 65

Planning high availability

For FortiVoice HA, apply the following planning guidelines:

- Make sure that both FortiVoice units in the HA group are the same model and have the same firmware version. If you are using VM instances, you require two VM licenses.
- For *both* primary and secondary FortiVoice units:
  - Connect port 1 to the network switch.
  - Connect port 2 or a secondary port (3, 4, or 5, depending on the model) to the network switch. This port takes on the role of the primary heartbeat interface.
- Plan which interface ports to use for your voice traffic and heartbeat links:
  - Decide which port you want to use for your voice traffic, for example port 1.
  - Make sure to assign the secondary heartbeat status to port 1.
  - Make sure to assign the primary heartbeat status to port 2 (3, 4, or 5, depending on the model).
- FortiVoice HA uses a secondary IP address on the interface ports. This secondary IP address is called a virtual IP address. You configure the primary and secondary units to use this virtual IP address but only the acting primary unit will use it to communicate. Any network traffic that is to be forwarded to the FortiVoice unit can be forwarded to this virtual IP address. If a failover occurs, the secondary unit assumes the role of primary and starts to use the virtual IP address. Your system is then able to continue operating as normal without having to change your port forwarding. For example, the primary unit has an IP address of 192.168.1.200 and the secondary unit has an IP address of 192.168.1.202. The virtual IP address is 192.168.1.210. Both primary and secondary units share this virtual IP address which is also used to receive all port forwarding to the FortiVoice unit.

- Take note of the IP address of each interface port on both FortiVoice units. You will need this information to set up the heartbeat link.

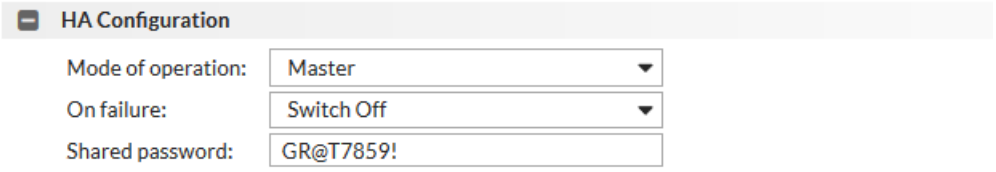
When you are ready to configure HA, go to Configuring high availability on FortiVoice units on page 61.

If a failover occurs and you are using FortiVoice 200F8 or FortiVoice 300E-T, remember to swap the physical FXO and PRI connections to the secondary unit.

Configuring high availability on FortiVoice units

Perform this procedure on both primary and secondary FortiVoice units.

1. Go to **System > High Availability > Configuration**.
2. In **HA configuration**, configure the following settings:
   a. Set **Mode of operation**.
   If the FortiVoice unit is the primary unit, set the **Mode of operation** to **Master**.
   If the FortiVoice unit is the secondary unit, set the **Mode of operation** to **Slave**.
   b. Set the **On failure** behavior to one of the following choices:
      i. **Switch Off**: As part of the HA group, the failed unit will not become a primary unit again until you manually restore the configured operating mode on the **Status** tab.
      ii. **Wait for Recovery then Restore Original Role**: After the unit recovers from failure, it will go back to its programmed **Mode of operation**. For example, if unit 1 (primary) encounters a failure and unit 2 (secondary) effectively becomes the primary, then when unit 1 recovers from failure, unit 1 will be restored as the primary and unit 2 will return to operating as the secondary unit.
      iii. **Wait for Recovery then Restore Slave Role**: After the unit recovers from failure, this unit will operate in secondary mode. For example, if unit 1 (primary) encounters a failure and unit 2 (secondary) effectively becomes the primary, then when unit 1 recovers from failure, it will then assume the secondary mode and unit 2 will continue to operate in primary mode.
   c. Set **Shared password**. Make sure to use the same password for both primary and secondary units.
   Example of HA Configuration settings for primary unit



3. In **Advanced Options**, configure the following port and heartbeat settings:
   a. The **HA base port** is used for the heartbeat signal as well as data and configuration synchronization. The default and recommended port is 20000.
   b. The **Heartbeat lost threshold** setting is the amount of time that must pass with no heartbeat link between the primary and secondary units before the system triggers a failover. The heartbeat signal is sent once per second to ensure that the unit is responding. In order to prevent a premature failover due to the system being under a heavy load, it is recommended to set this setting at 3 seconds or higher.
   c. As an added fail-safe, you can enable **Remote services as heartbeat**. After you enable this setting, you can configure the HTTP and SIP UDP settings in the **Service Monitor** section to act as an additional HA heartbeat

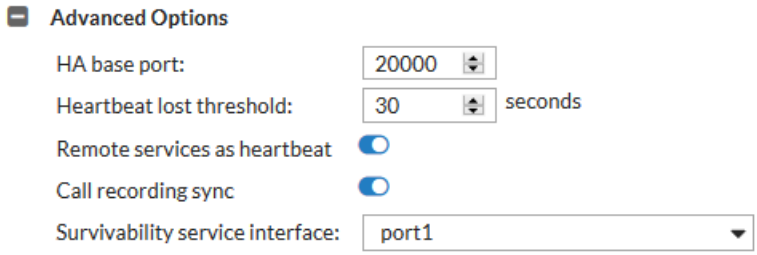
(details are included in Configuring service-based failover on page 63). If both primary and secondary heartbeat links fail but the remote service detects that the primary unit is still available, no failover will occur. Note that this feature is only an additional heartbeat and does not provide any synchronization of files from primary to secondary units. Therefore, Fortinet does not recommend relying on remote services alone. Configure at least one HA heartbeat on an interface port.

d. With **Call recording sync**, you enable or disable the synchronization of recorded calls from the primary to the secondary units. This setting is optional because there can be many recorded calls on the system that can take up quite a bit of memory. Copying these files during synchronization can take a long time and use up network bandwidth.

e. **Survivability service interface** is planned to be functional in a future release.

f. Click **Apply**.

Example of Advanced Options settings



4. In **Interface**, you configure the port behavior. When setting up the ports, make sure that you mirror the primary unit settings on the secondary unit, except for the **Peer IP address** and **Peer IPv6 address** settings.

Make sure to apply the following settings:

- Set port 1 with the secondary heartbeat status.
- Set port 2 (or 3 or 4) with the primary heartbeat status.

Select a port and click **Edit**.

a. **Enable port monitor**: When you enable this setting, the unit performs an internal port check to make sure that this port is responsive. If the port becomes unresponsive, the system triggers a failover. This setting has its timing intervals configured by using the **Service monitor, Interface monitor** section which you can set later in Configuring service-based failover on page 63.

b. **Heartbeat status**: Configure the heartbeat link and system synchronization. The following three choices are available:

   i. **Disable**: There is no heartbeat link or synchronization on this port.

   ii. **Primary**: Make sure to set port 2 (or 3 or 4) as primary. This port provides a heartbeat link and system synchronization from the primary to secondary units.

   iii. **Secondary**: Make sure to set port 1 as secondary. A secondary heartbeat link is used as a backup in case the primary one fails. A failover does not occur unless both primary and secondary heartbeat links are down.

c. **Peer IP address and Peer IPv6 address**: Specify the IP address of the port at the opposite side for the heartbeat link to communicate on. For example, if you are configuring the primary unit, then enter the IP address for port 2 of the secondary unit here. If you are configuring the secondary unit, then enter the IP address of port 2 of the primary unit here.

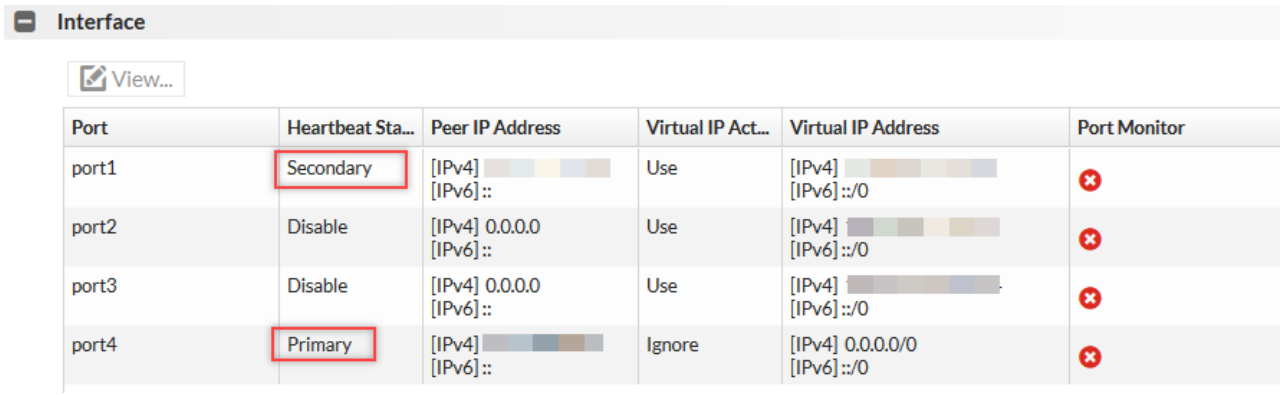
d. **Virtual IP action**: When configuring the virtual IP address, set the **Virtual IP action** to **Use**.

e. **Virtual IP address and IPv6 address**: Make sure that the primary and secondary units share the same virtual IP address on each port. Also, make sure that all port forwarding for voice traffic on your router is forwarded to

the virtual IP address.

f. Click **OK**.

Example of Interface settings



5. **Service Monitor** offers another way of detecting whether or not there is a system failure. For configuration details, see Configuring service-based failover on page 63.
6. When you have completed the configuration on both FortiVoice units in the HA group, go to Synchronizing configuration and data in a FortiVoice HA group on page 64.

Configuring service-based failover

The **Service Monitor** section offers another way of detecting whether or not there is a system failure.

The system uses **Remote HTTP** and **SIP UDP** settings as a heartbeat link to confirm that the secondary unit can connect to the primary unit using HTTP or SIP. If the secondary unit cannot connect to the primary unit, then the system triggers a failover and the secondary unit becomes the primary. In addition to enabling the **Remote HTTP** and **SIP UDP** settings here, make sure that you have enabled **Remote services as heartbeat** in the **Advanced Options** section of Configuring high availability on FortiVoice units on page 61.

The **Interface monitor** and **Local hard drives** settings are locally monitored. If the system detects a failure on one of its interface ports or hard drives, then the system triggers a failover. To enable which ports the unit will monitor for failure, select **Enable port monitor** in the **Interface** section of Configuring high availability on FortiVoice units on page 61.

Perform the following steps on both primary and secondary FortiVoice units.

1. Go to **System > High Availability > Configuration**.
2. In **Service Monitor**, click one of the following services:
   - **Remote HTTP**
   - **SIP UDP**
   - **Interface monitor**
   - **Local hard drives**
3. Click **Edit**.
4. For **Remote HTTP** and **SIP UDP**, click **Enable**, and configure the following settings:
   - **Remote IP**: Enter the peer IP address.
   - **Port**: Enter the port number of the peer service.
   - **Timeout**: Enter the timeout period (in seconds) for one connection test.
   - **Interval**: Enter the frequency (in seconds) of the tests.

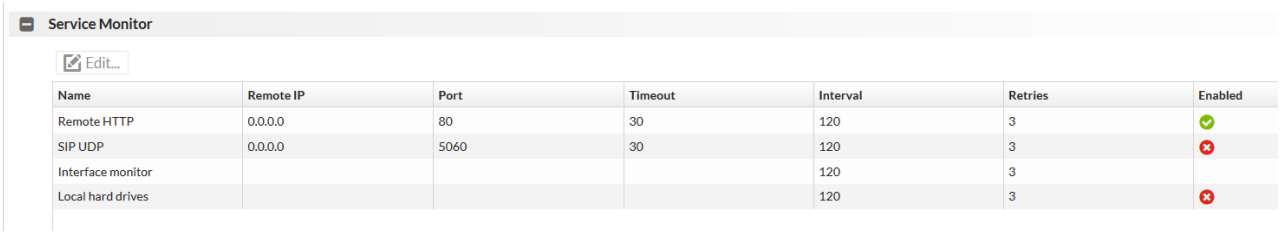
- **Retries**: Enter the number of consecutive tests that are allowed before the primary unit is deemed unresponsive and a failover occurs.

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

- **Enable**: Select to enable local hard drive monitoring.
  For interface monitoring, select **Enable port monitor** in the **Interface** section of Configuring high availability on FortiVoice units on page 61.
- **Interval**: Enter the frequency (in seconds) of the test.
- **Retries**: Enter the number of consecutive tests that are allowed before the local interface or local hard drive is deemed unresponsive and a failover occurs.

5. Click **OK**.

Example of Service Monitor settings



6. Go to Synchronizing configuration and data in a FortiVoice HA group on page 64.

Synchronizing configuration and data in a FortiVoice HA group

Use this procedure to synchronize configuration and data from the primary FortiVoice unit to the secondary FortiVoice unit.

The synchronization does not copy the following data:

- Host name
- Static routes
- Interface configuration
- Main HA configuration
- HA service monitoring settings
- System appearance

Procedure steps

1. Go to **System > High Availability > Status**.
2. Click the link **Click HERE to Start a Configuration/Data Sync**.
3. To confirm, click **OK**.

Installing licenses on a FortiVoice HA group

For the Call Center and Hotel Management features, the primary and secondary FortiVoice units share the license file. However, you must install the license file separately on both primary and secondary FortiVoice units.

Before you begin

Download the license (.lic) file from your Fortinet Support account and know where you save the file on your computer.

Install the license on the primary FortiVoice unit

1. Log in to the primary FortiVoice unit.
2. Go to **Dashboard > Status**.
3. In the **License Information** widget, click **Update License**.
4. Locate the license file that you previously downloaded to your computer and click **Open**.
5. To confirm the upload, click **Yes**.

Install the license on the secondary FortiVoice unit

1. Log in to the secondary FortiVoice unit.
2. Go to **System > High Availability > Status**.
3. Check the **Effective Operation Mode** and wait until it displays **out of sync**.
   You can install the license file on the secondary unit only when the file is out of synchronization with the license file on the primary unit.
4. When the **Effective Operation Mode** on the secondary unit displays **out of sync**, then go to **Dashboard > Status**.
5. In the **License Information** widget, click **Update License**.
6. Locate the license file that you previously downloaded to your computer and click **Open**.
7. To confirm the upload, click **Yes**.
8. After successfully uploading the license file, go to **System > High Availability > Status**.
9. Click the link **Click HERE to restart the HA system**.

Enabling high availability activity logging

Use this procedure to enable the high availability (HA) activity logging. This logging is disabled by default.

1. Go to **Log & Report > Log Setting > Local**.
2. Under **Logging Policy Configuration**, expand **System** and enable **HA**.
3. Click **Apply**.

Displaying the high availability status

Use this procedure to display the high availability (HA) status of a FortiVoice unit.

1. Go to **System > High Availability > Status**.
2. You can review the following settings:
   - **Refresh** section lets you set a timer for how often you want this page to check for a status update automatically. To manually refresh this page, click **Refresh**.
   - **Mode Status** lets you know what the configured mode is and the mode that it is currently using.
     - **Configured Operating Mode** is the mode that you have programmed the unit to act as with the **Configuration** tab (either as primary or secondary).
     - **Effective Operating Mode** can display one of the following modes:
       - **Master** shows that the unit is acting as the primary.
       - **Slave** shows that the unit is acting as the secondary.

    - **Failed** shows that the service or network interface monitoring has detected a failure and the diagnostic connection is currently determining whether the problem has been corrected or a failover is required.
    - **Off** is a mode used by both units. For a primary unit, this mode indicates that the service or interface monitoring has detected a failure, taken the primary unit offline, and triggered a failover. For a secondary unit, this mode indicates that the synchronization has failed once; a subsequent failure will trigger a failover.
- **Daemon status** is only available on the secondary unit. The following updates are available:
    - **Monitor** shows when the secondary unit will check the primary unit to make sure that it is still active. If the system detects any errors, this section will show how many errors were detected.
    - **Configuration** shows the last time the configuration was updated from the primary unit to the secondary unit.
    - **Data** shows the last time the data was synchronized between the primary and secondary units. The **Configuration** and **Data** section may display different times. This is normal. Synchronizing data can take longer to complete.
    - **Database** shows the database status such as Checking Status, Stopped, Running (in sync), and Syncing Data.
- **Actions**
    - **Click HERE to Start a Configuration/Data Sync**: For details about this action, see Synchronizing configuration and data in a FortiVoice HA group on page 64.
    - **Click HERE to Restore Configured Operating Mode**: If a failover is triggered and the issue has been resolved, you can click this link to tell the unit that it can resume the mode it was originally configured to be.
    - **Click HERE to Switch to SLAVE Mode**: This action is available on the primary unit only. If you want to change the mode of operation of the primary unit to secondary, click the link.
    - **Click HERE to Switch to MASTER Mode**: This action is available on the secondary unit only. If you want to change the mode of operation of the secondary unit to primary, click the link.

Hotel management

This section shows how to configure hotel management settings in FortiVoice.

After configuring FortiVoice, you will need to configure your own property management software (PMS) and ensure it is properly connected to FortiVoice. FortiVoice, in this manner, acts as a supplement. Consult your property management software manual for more details.

FortiVoice requires a hotel management license for this configuration.

This section includes the following recipes:

- Configuring PMS settings on page 67
- Configuring hotel management options on page 68
- Defining minibar codes on page 69
- Configuring room status on page 69

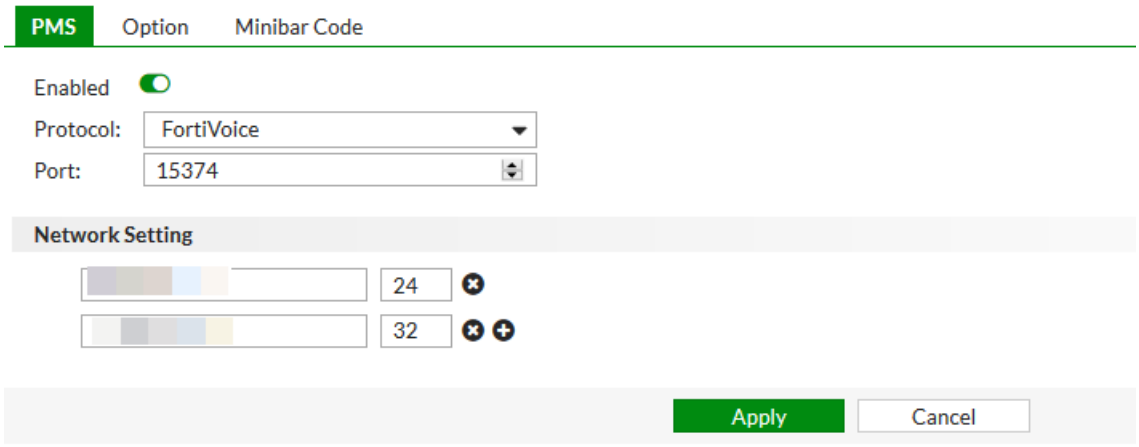
Configuring PMS settings

Configure settings for connecting to the PMS on the FortiVoice.

The connection between FortiVoice and the PMS requires the use of an adapter. The Precedia iPocket 232 is recommended.

1. Go to **Hotel Management > Setting > PMS** and click **Enabled**.
2. Set **Protocol** to **FortiVoice**, and enter the port number used to connect to the PMS (by default, 15374).
3. Under **Network Setting**, enter the IP address and netmask of the PMS.
   You can enter multiple trusted hosts if you have multiple property management systems.

4. Click **Apply**.

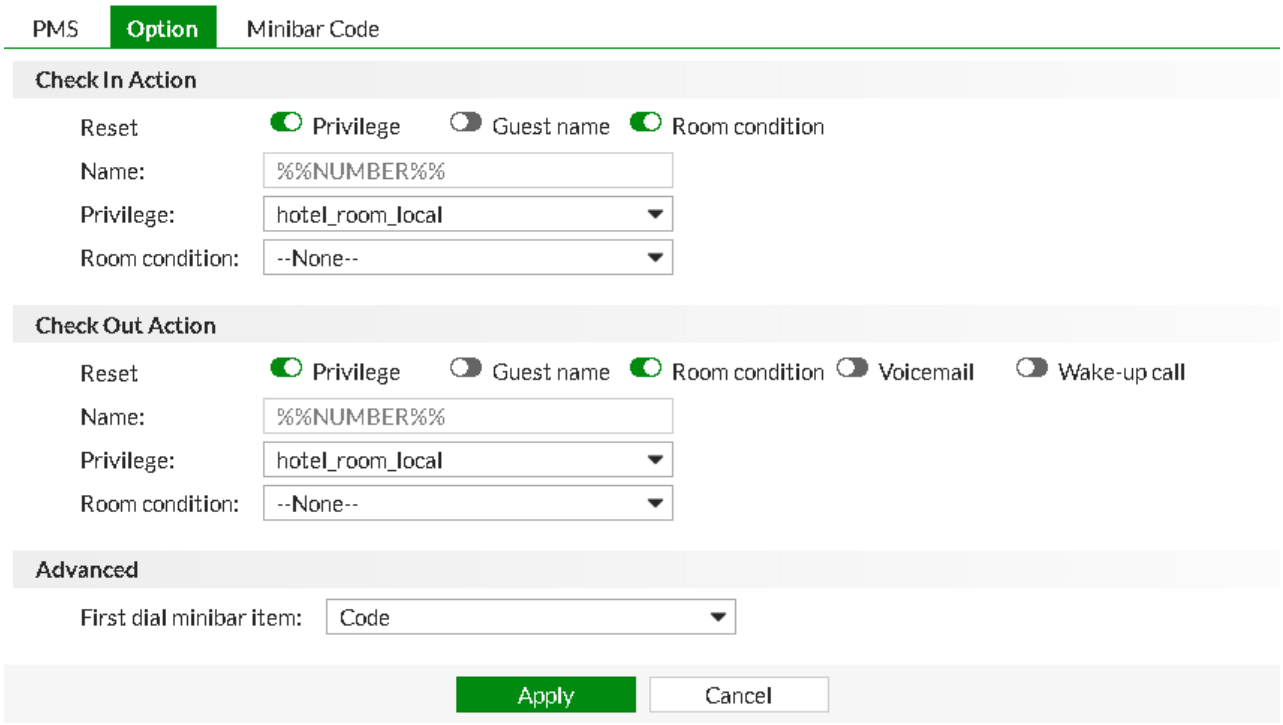


Configuring hotel management options

Check in and check out actions can be configured.

1. Go to **Hotel Management > Setting > Option**.
2. Under **Check In Action**, select the appropriate guest information to make a room check-in ready:
   - **Privilege**: Enable phone call restrictions and user privileges for the room extension.
   - **Guest name**: Display either the room number or guest name on the extension in the room. This is configured in the **Name** field as %%NUMBER%% to display the room number or %%NAME%% to display the guest name.
   - **Room condition**: Clear any condition set for the room.
3. Under **Check Out Action**, select the appropriate guest information to make a room check-out ready. In addition to the options available for check-in, check-out options also include the following:
   - **Voicemail**: Clear all voicemails for the room extension.
   - **Wake-up call**: Clear all wake-up call setups for the room extension.
4. Under **Advanced**, set **First dial minibar item** to either **Code** or **Number**, to determine how guests place an order from the front desk. For example, if **Code** is selected, and the guest wants two waters (code 1), the guest would enter **1*2**. If **Number** is selected, and the guest wants the same order, they would instead enter **2*1**.

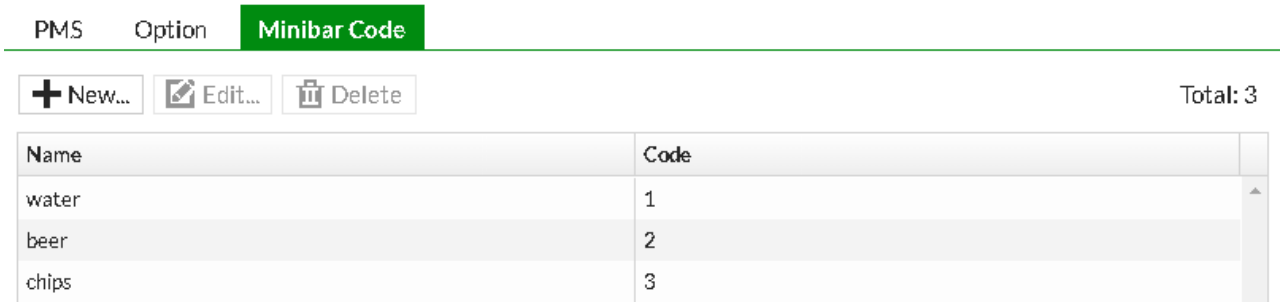
5. Click **Apply**.



Defining minibar codes

In the previous step, an example was given of the guest entering a number code of 1 for water. The **Minibar Code** tab is where codes are associated with minibar items. Codes assigned to minibar items must be configured to allow guests to place minibar orders using the key pad.

1. Go to **Hotel Management > Setting > Minibar Code** and click **New**.
2. To create the water code used in the previous step, set **Name** to **water** and **Code** to **1**, and click **OK**.
3. Create other minibar codes for other minibar items as necessary.

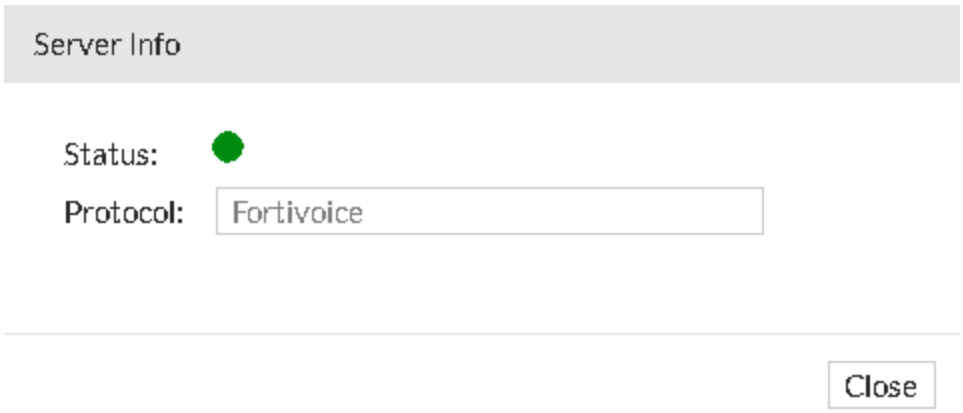


In this example, water, beer, and chips have been assigned codes 1, 2, and 3 respectively. If the guest wants two waters, two beers, and one order of chips, and assuming **First dial minibar item** under **Hotel Management > Setting > Option** is set to **Code**, the guest would enter **1*2*2*2*3*1**.

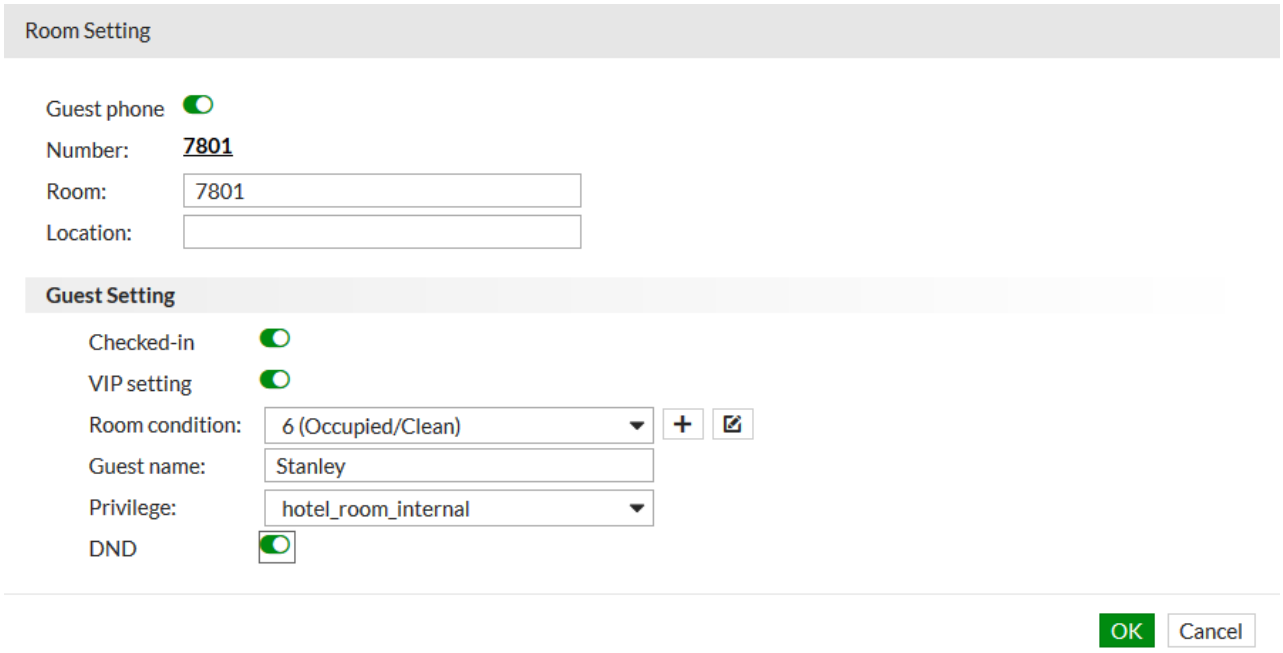
Configuring room status

Once the PMS and FortiVoice device are properly connected, hotel room statuses can be configured.

1. Go to **Hotel Management > Room Status > Room Status** and click **Server Info**.
   A green dot indicates that the FortiVoice device is connected with the PMS.



2. Select the **Room** you wish to edit and click **Edit**.
3. Enable **Guest phone** to make the room a guest room. **Guest Setting** will appear.
4. If the guest is checked-out, set the appropriate **Room condition** from the drop-down menu. If the guest is checked-in, enable **Checked-in**, set the appropriate **Room condition**, **Guest name**, and **Privilege** option.
5. Additionally, enable **VIP setting** if the guest should receive special treatment, and enable **DND** if the guest does not want to be disturbed.



Licensing

This section includes the following recipes:

- Purchasing a FortiVoice product license on page 71
- Registering a FortiVoice product and downloading the license file on page 71
- Uploading the license file to FortiVoice on page 72

Purchasing a FortiVoice product license

Before you begin

- Make sure to know the order information (such as stock keeping unit (SKU) code) of the FortiVoice product that you want to order. For details, see the FortiVoice Enterprise Phone Systems Data Sheet or FortiFone IP Telephones Data Sheet.
- Make sure to know how to contact a Fortinet partner to obtain licenses. If you do not have a partner, you can visit the Find a Partner portal or contact evac@fortinet.com.

Procedure steps

1. Contact a Fortinet-authorized reseller in your region.
2. Place your order.
3. After your order is processed, Fortinet sends you an email that includes the support contracts and registration codes for the FortiVoice or FortiFone licenses.
4. Download the files to a convenient location on your computer or network.
5. Know how to access and copy the registration codes. You will need those codes during the registration process.
6. To continue with the registration process, go to Registering a FortiVoice product and downloading the license file on page 71.

Registering a FortiVoice product and downloading the license file

Before you begin

Make sure that you have the license registration code for the FortiVoice product that you want to register (see Purchasing a FortiVoice product license on page 71).

Procedure steps

1. Log in to your FortiCloud account or register for an account.
2. To start the registration process, click **Register Product**.
3. In **Registration Code**, enter your product serial number, service contract registration code or license certificate number.
4. In **End User Type**, choose the type of user as either government or non-government.
5. To continue the product registration, click **Next**.
6. Provide registration details and click **Next**.

7. Read and accept the terms and conditions of the product registration agreement, and click **Next**.
8. On the Verification page, review and accept the product entitlement, and click **Confirm**.
9. When the registration is complete, download the license file file (.lic) to your computer:
   a. Go to **Products > Product List**.
   b. Click the **Serial Number** for your product.
   c. In **Product Information**, go to **License File** and click **License File Download**.
   d. Take note of the location where you save the license file.

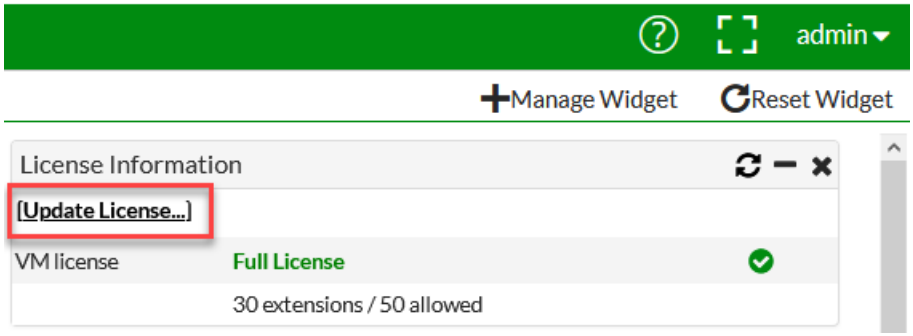
Uploading the license file to FortiVoice

Before you begin

You know where the license is stored on your computer. For more details, see Registering a FortiVoice product and downloading the license file on page 71.

Procedure steps

1. Go to **Dashboard > Status**.
2. In the **License Information** widget, click **Update License**.



3. In the **File Upload** dialog box, locate the license (.lic) file, select the file, and click **Open**.
4. To confirm t he upload, click **Yes**.

Managed system

This section contains information about configuring system management settings including gateways, survivability, and FortiVoice and FortiFone firmware.

This section includes the following topics:

- Gateway management on page 73
- FortiVoice units as survivable branches on page 73
- FortiFone firmware upgrades on page 74

Gateway management

FortiVoice can manage the following three types of gateways:

- **FortiVoice foreign exchange office (FXO) gateway** - This gateway works in conjunction with the FortiVoice phone system, an IP private branch exchange (IP PBX), to expand resources and support additional analog phone lines. With the FortiVoice FXO gateway, you connect your analog phone lines to your FortiVoice phone system. For details about deploying an FXO gateway, see the FortiVoice FXO Gateway Deployment Guide.
- **FortiVoice foreign exchange subscriber (FXS) gateway** - This gateway works in conjunction with the FortiVoice phone system to expand resources and support additional analog phone extensions. With the FXS gateway, you can connect your traditional analog phones and fax machines to a FortiVoice phone system. For details about deploying an FXS gateway, see the FortiVoice FXS Gateway Deployment Guide.
- **FortiVoice primary rate interface (PRI) gateway** - This gateway works in conjunction with your FortiVoice phone system to expand resources and support additional phone lines. With a PRI gateway, you connect your legacy telephony infrastructure composed of PRI (T1 or E1) digital lines to a FortiVoice phone system. For details about deploying a PRI gateway, see the FortiVoice PRI Gateway Deployment Guide.

FortiVoice units as survivable branches

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

Local survivability provides centralized management and branch office resiliency.

For details about deploying a FortiVoice LSG unit, see the FortiVoice Local Survivable Gateway Deployment Guide.

FortiFone firmware upgrades

This cookbook recipe guides you through the process of upgrading FortiFone firmware using FortiVoice 6.0. It details how to review current FortiFone firmware, upload new firmware files, schedule firmware upgrade jobs, and confirm firmware upgrades.

Prior to deploying FortiFone firmware upgrades, make sure to meet the following requirements:

- The network connectivity is available between the target FortiFone devices and the FortiVoice unit.
- You have downloaded the latest FortiFone firmware files from the Fortinet Support website.

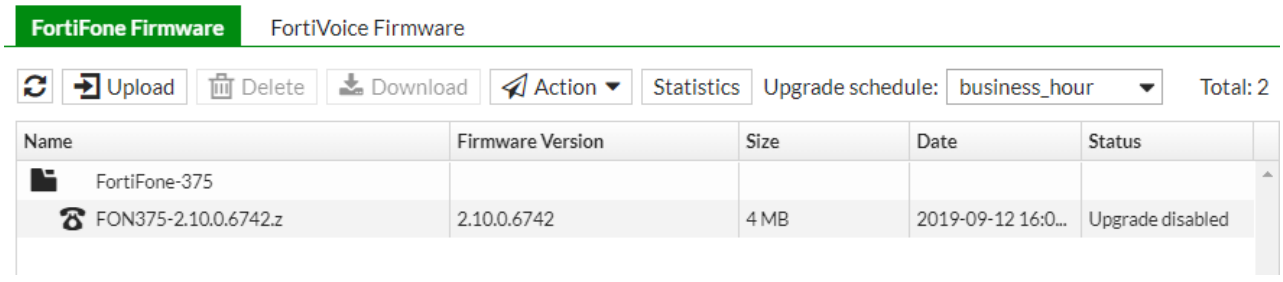
Reviewing the current FortiFone firmware

Before updating FortiFone firmware, you can review the firmware currently installed on all FortiFone devices connected to the network.

1. From the FortiVoice UI, navigate to **Managed System > Firmware > FortiFone Firmware** and click **Statistics**. The **Firmware Upgrade Status** window opens listing the phone model and firmware version details of phones currently connected to the network. The **Phone Number** column provides the number of phones in each particular grouping.
2. When you are finished reviewing the status of the phones, click **Close**.

Uploading the FortiFone firmware to FortiVoice

1. Go to **Managed System > Firmware**.
2. In the **FortiFone Firmware** tab, click **Upload**.
   The **FortiFone Firmware Upload** window opens.
3. For **Phone model**, select the phone type that will be the target of the firmware upgrade.
4. For **Firmware file**, click **Select**. Select the firmware file for the selected FortiFone model and click **Open**.
   The firmware file uploads to FortiVoice.
5. In the **Firmware version** field, type the firmware version number.
6. In the **Comments** field, provide a comment if necessary.
7. Click **OK**.
   The uploaded firmware file appears in the list of **FortiFone Firmware** files.

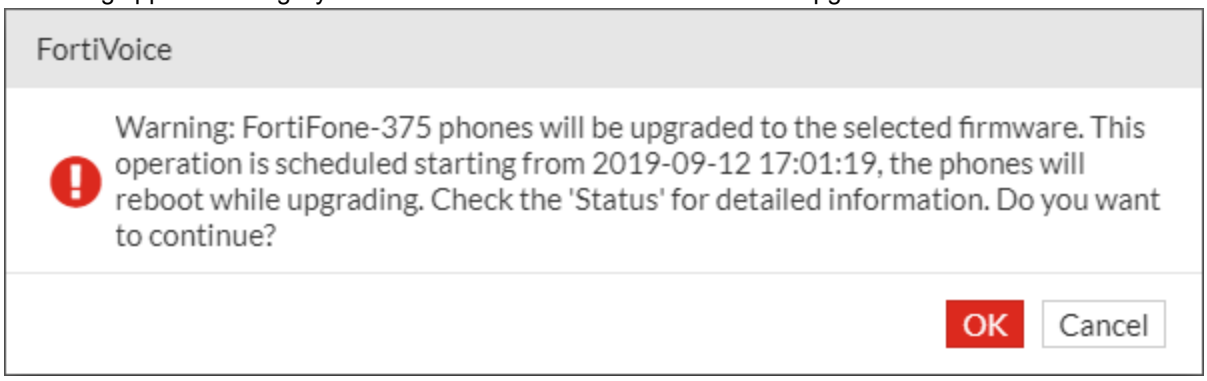


Scheduling the firmware upgrade

1. From the **Upgrade schedule** drop-down list, select a time period for the firmware upgrade to take place.

   You can edit the phone firmware upgrade schedule options or create your own. To do this, go to **System > Advanced > Auto Provisioning**.

2. From the list of FortiFone firmware files, select the firmware file to schedule for upgrade.
3. Click **Action**, then click **Schedule Upgrade**.
   A warning appears asking if you would like to continue with the firmware upgrade.



4. Click **OK**.
   The firmware upgrade is scheduled to run.

Confirming the firmware upgrade

1. To confirm that the firmware has been successfully installed on targeted FortiFone devices, from the **FortiFone Firmware** tab, click **Statistics**.
   The Firmware Upgrade Status window opens. Review the firmware version of applicable phone models to confirm that the new firmware is installed.
2. If necessary, click **Refresh** to view updates.
3. Click **Close**.
4. The scheduled firmware upgrade can be disabled after the firmware upgrade process is complete. From the list of FortiFone firmware files, select the firmware file that you want to disable scheduling for.
5. Click **Action**, then click **Disable Upgrade**.
   The firmware upgrade is disabled.

Phone system

This section includes information about the following phone system features:

- Emergency numbers on page 76
- LDAP authentication configuration for extension users on page 77
- Schedules – best practices on page 79

Emergency numbers

This recipe guides you through the process of establishing an emergency contact number for your office.

An emergency call, such as 911 in North America, is first routed to a Public Safety Answering Point (PSAP). The PSAP will look up the Automatic Number Identification (ANI), or calling number, from Automatic Location Information Database (ALI database) to determine the caller's physical address. The ALI database is updated by the PSTN service provider when a customer subscribes to its trunk service. A record in the ALI database is a mapping between a phone number (or trunk) and its physical address.

For each emergency call, the PBX is responsible for setting the correct ANI for the PSAP.

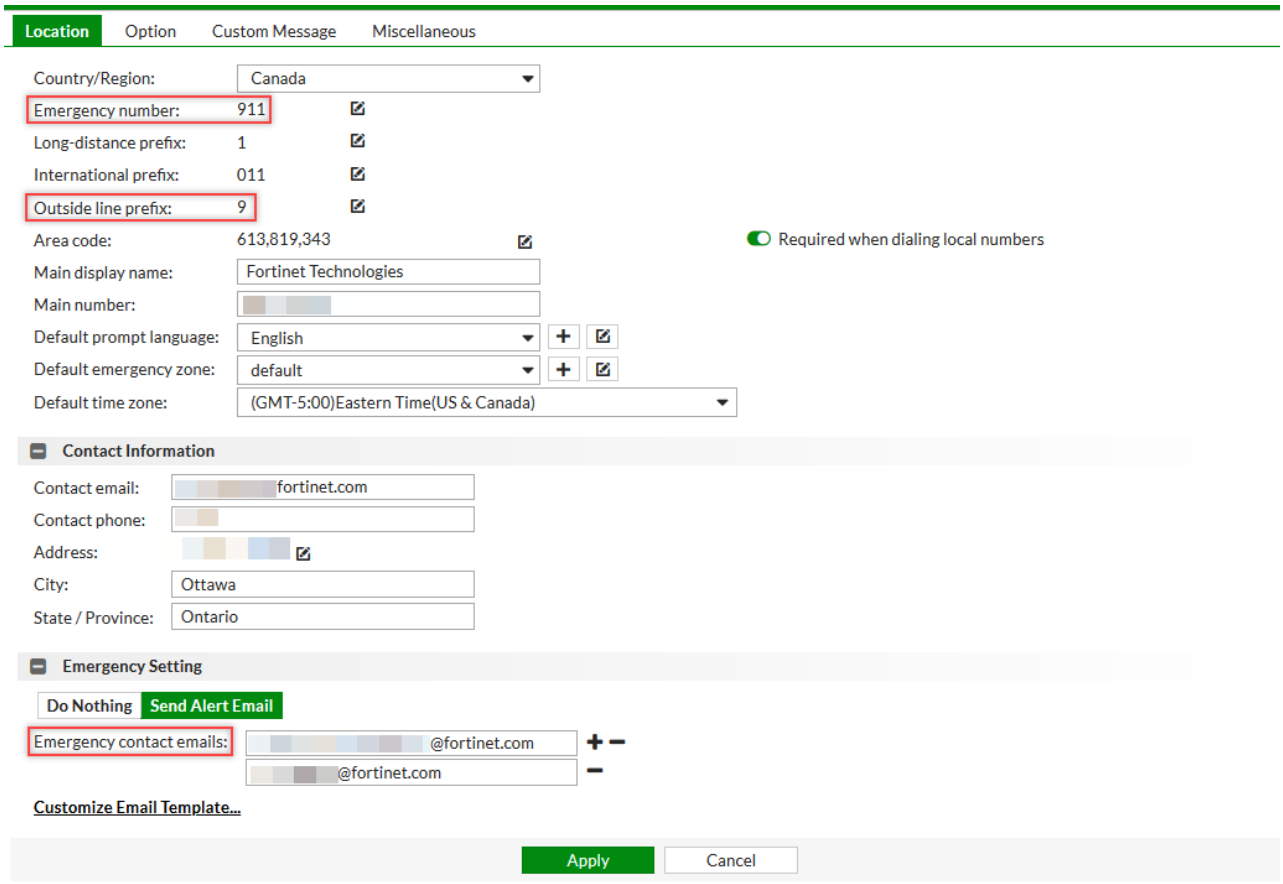
This recipe includes the following topics:

- Configuring the emergency number on page 76
- Configuring an outbound dialplan for emergency calls on page 77

Configuring the emergency number

1. Go to **Phone System > Setting > Location**.
2. Select the appropriate **Country/Region** (in this example, **Canada**).
3. Configure the **Emergency number** and **Outside line prefix**. Check with your PSTN service provider for the appropriate area code. Configure the remaining settings as required.
   It is especially important to note the **Outside line prefix**, as internal callers will need to append this to the configured emergency number (in this example, **9 911**).
4. Under **Emergency Setting**, select **Send Alert Email** and enter **Emergency contact emails** as necessary.
   The email addresses specified here will receive an alert email any time an emergency call is made, including the location of the caller and the time of the call.

5. Click **Apply** when finished.



Configuring an outbound dialplan for emergency calls

1. Go to **Call Routing > Outbound > Outbound** and click **New**.
2. Enter a **Name** for the dialplan, and enable **Emergency Call**. This dialplan ensures that the FortiVoice unit bypasses privilege checks and grants the highest priority to all emergency calls.
3. Leave **Caller ID Match** and **Dialed Number Match** as you do not want to impose any kind of restrictions to who can make an emergency call.
4. Under **Call Handling**, click **New**.
5. For an outbound dialplan as important as facilitating emergency calls, set **Schedule** to **any_time** and **Action** to **Allow**.
6. Select an **Outgoing trunk** or **Caller ID modification** profile from the drop-down menus provided.

LDAP authentication configuration for extension users

The FortiVoice unit works with LDAP servers to authenticate extension users accessing the unit. This recipe guides you through the process of configuring LDAP authentication on the FortiVoice unit for extension users.

This recipe uses MS Server 2012 Active Directory as an example LDAP server.

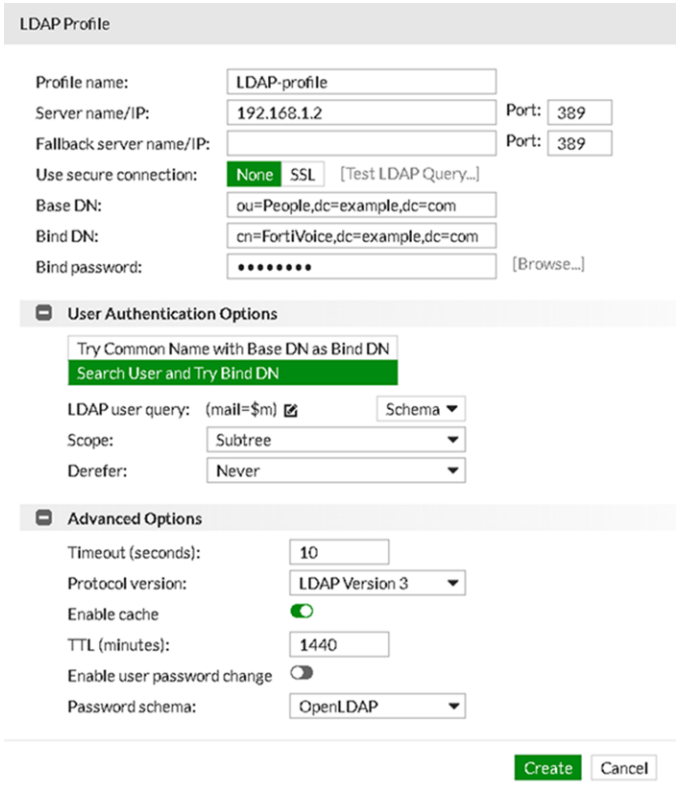
This recipe includes the following tasks:

- Creating an LDAP profile on page 78
- Applying the LDAP profile to an extension on page 79

Creating an LDAP profile

1. Go to **Phone System > Profile > LDAP** and click **New**, or edit an existing profile.
2. Enter a **Profile name**.
3. Set **Server name/IP** to the FQDN or IP address of the LDAP server.
4. Set **Port** to the port that the LDAP server will use to communicate with the FortiVoice unit.
   Note that the default port number depends on whether the LDAP server uses an encrypted connection (see the next step).
5. Set **Use secure connection** to **None** or **SSL**. Port 389 is typically used for non-secure connections, and port 636 is typically used for SSL-secured (LDAPS) connections.
6. Set **Base DN** to the distinguished name (DN) of the LDAP directory tree within which the FortiVoice unit will search for user objects, such as `ou=People,dc=example,dc=com`.
7. Set the **Bind DN** of an LDAP user account who has permissions to query the base DN, such as `cn=FortiVoice,dc=example,dc=com`.
   Note that this is only necessary if your LDAP server requires the FortiVoice unit to authenticate when performing queries.
8. Enter the **Bind password**, if applicable.
9. Under **User Authentication Options**, enable one of the following:
   - **Try Common Name with Base DN as Bind DN**: Enable to form the user's bind DN by prepending a common name to the base DN. Also enter the name of the user objects' common name attribute, such as `cn` or `uid` into the field.
   - **Search User and Try Bind DN**: Select to form the user's bind DN by using the DN retrieved for that user.
     For more information about configuring the LDAP query filter and schema required for this option, see the FortiVoice Phone System Administration Guide.
10. Under **Advanced Options**, enter a **Timeout** in seconds that the FortiVoice unit will wait for query responses from the LDAP server.
11. Set **Protocol version** to the protocol used by the LDAP server.
12. Click **Enable cache** to cache LDAP query results.
13. Set **TTL** to the number of minutes that the FortiVoice unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiVoice unit to query the LDAP server, refreshing the cache.
    Note that if caching is enabled, but queries are not being cached, review the value entered for **TTL**. Setting a **TTL** of **0** effectively disables caching.
14. Click **Enable user password change** to allow users of the FortiVoice user portal to change their password.
15. Set **Password schema** to your LDAP server's user schema style, either **OpenLDAP** or **Active Directory**.

16. Click **Create** or **OK**.



Applying the LDAP profile to an extension

1. Go to **Extension > Extension > IP Extension** and click **New**, or edit an existing extension.
2. Under **User Setting**, in the **Web Access** tab, set **Authentication type** to **LDAP**.
3. Set **LDAP profile** to the newly created profile.
4. Leave the **Authentication ID** field empty, and click **Create** or **OK**.

Schedules – best practices

Each schedule you create can be used within the call handling of the FortiVoice to direct calls during various times of the day, such as your business hours, after hours and holidays. Schedules can easily be edited to change hours, include specific days with modified hours, or even add new holidays.

Schedules are used for handling calls in the following features:

- Inbound call handling
- Outbound call handling
- Extension call handling
- Ring groups call handling
- Virtual number call handling

As schedules for these features are all added in the same way, this best practice covers an efficient way to create three schedules and how to edit them that works for most businesses.

This section include the following recipes:

- Creating schedules on page 80
- Configuring call handling with schedules on page 87

Creating schedules

FortiVoice has two methods for creating a schedule, **Calendar** and **Standard**, both of which are used to create the schedules outlined within this recipe. FortiVoice contains three example schedules (**business_hours**, **after_hours**, and **holiday**) and a schedule called **any_time** which can be used to handle calls for any time that is not configured within a separate schedule. As a best practice, the following is recommended:

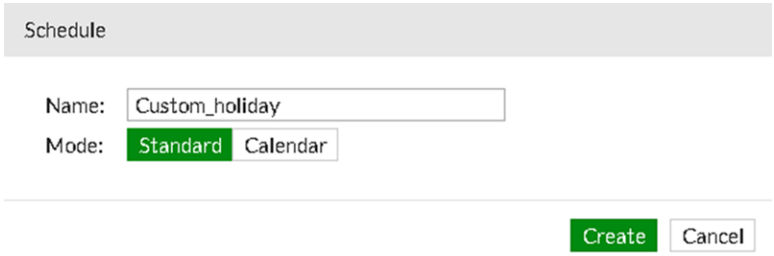
- Create a **Standard** schedule to handle your holidays.
- Create a **Calendar** based schedule for your business hours.
- Use the **any_time** schedule to handle time outside of business hours.

A holiday schedule should use the **Standard** based schedule, which allows for the quick addition of holidays. The holiday schedule will run for the entire day so no time ranges are required.

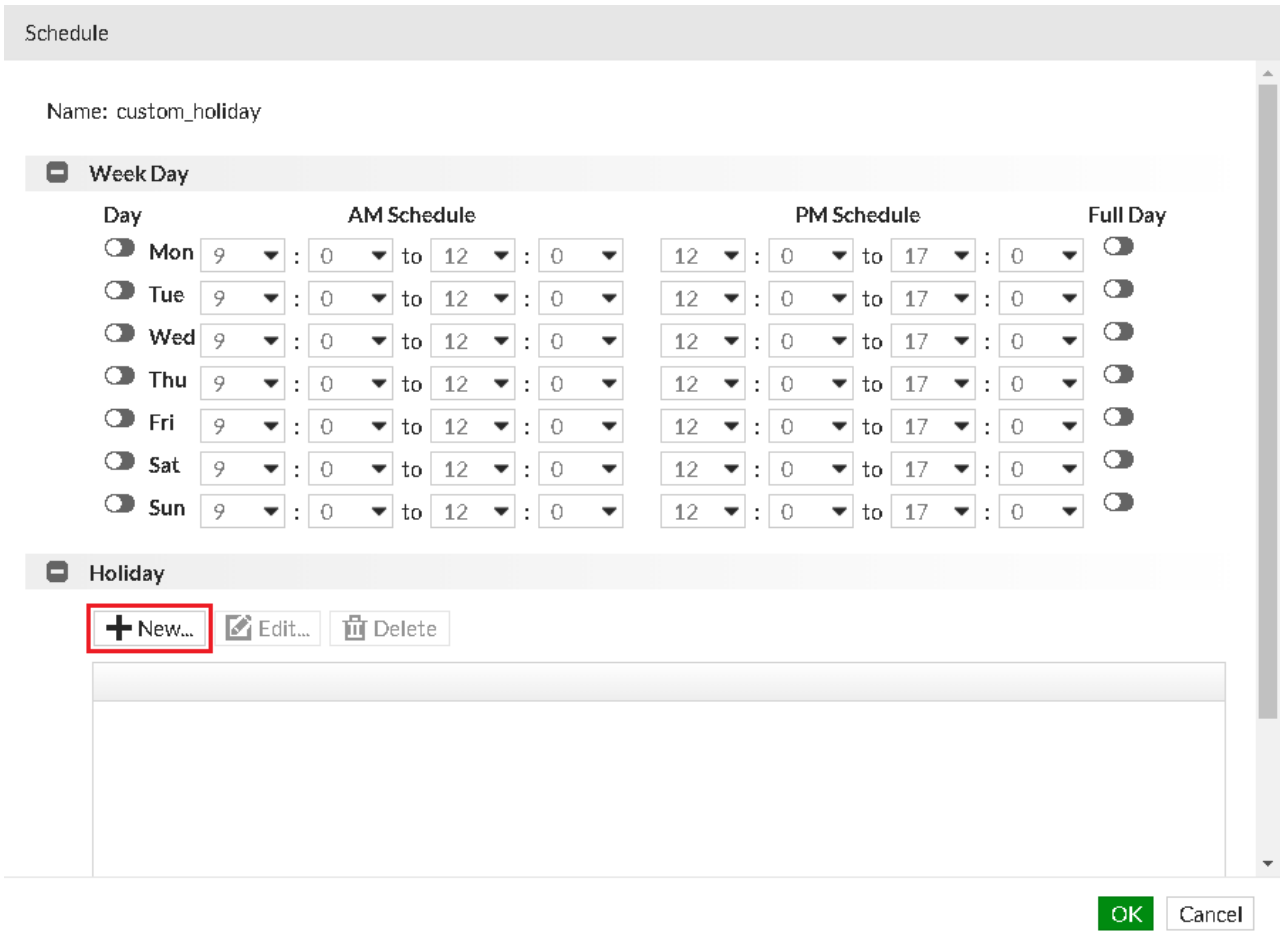
By default, FortiVoice uses a schedule called **any_time** to handle hours that have not already been configured within a schedule. For example, if you have a business hours schedule for 10 AM to 6 PM but no other schedule created, the hours outside that schedule (6 PM to 9 AM the next day) will be handled by the **any_time** schedule.

To add holiday dates in a Standard based schedule:

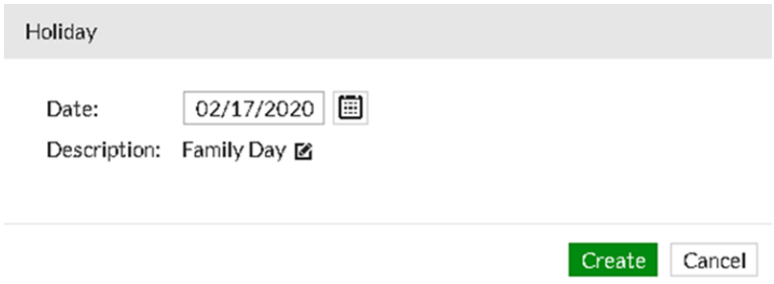
1. Go to **Phone System > Profile > Schedule** and click **New**.
2. Enter a **Name** (in this example, **Custom_holiday**), set **Mode** to **Standard**, and click **Create**.



3. Once created, select the schedule from the list and click **Edit**.
4. Expand **Holiday** and click **New**.

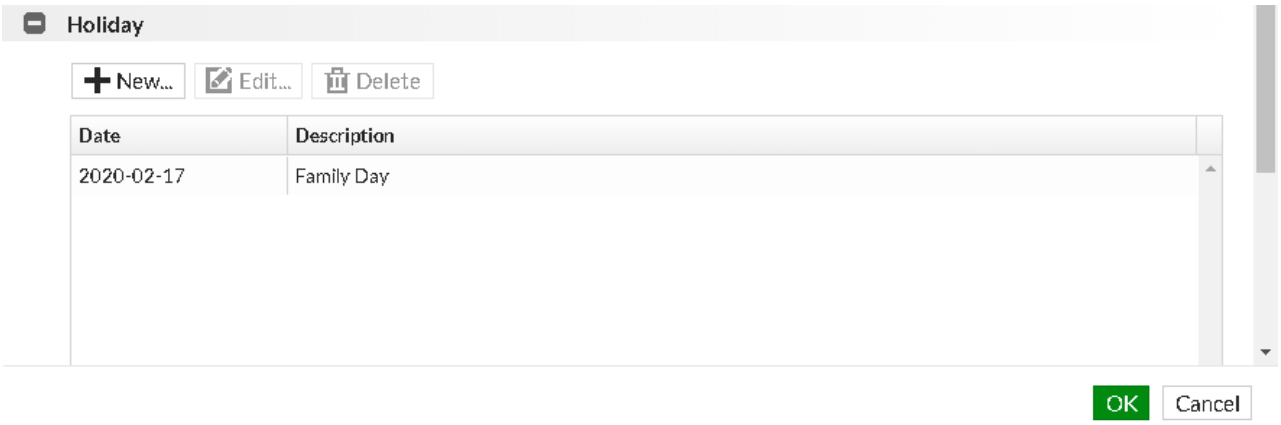


5. Select the **Date** and enter a **Description**, and click **Create**.



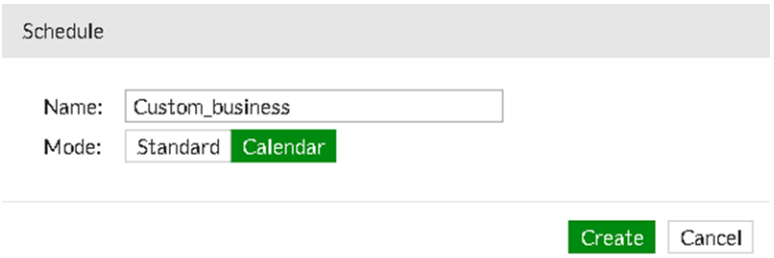
The new holiday is added to the list.

6. Click **OK**.

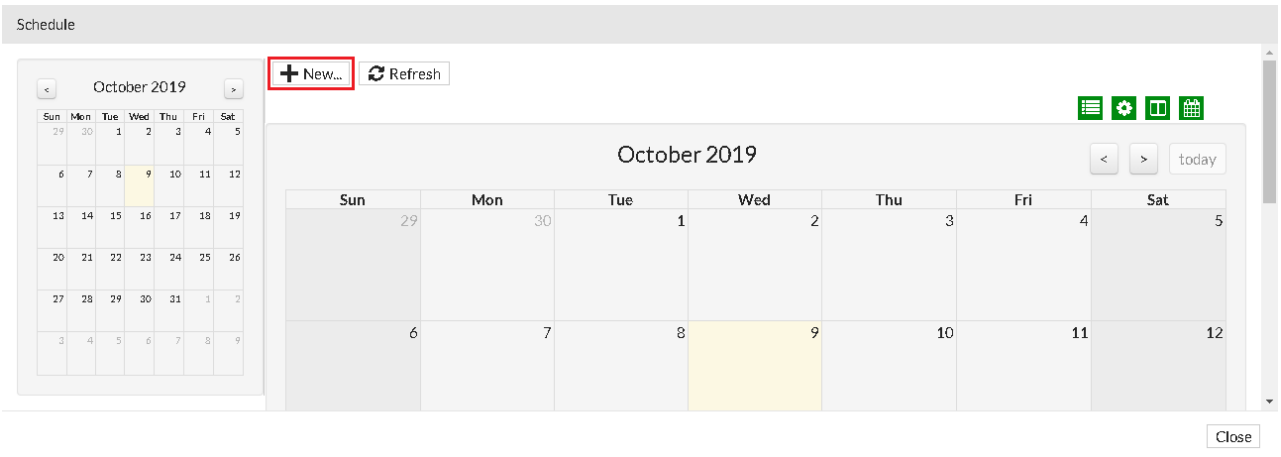


To create a Calendar based schedule for your business hours:

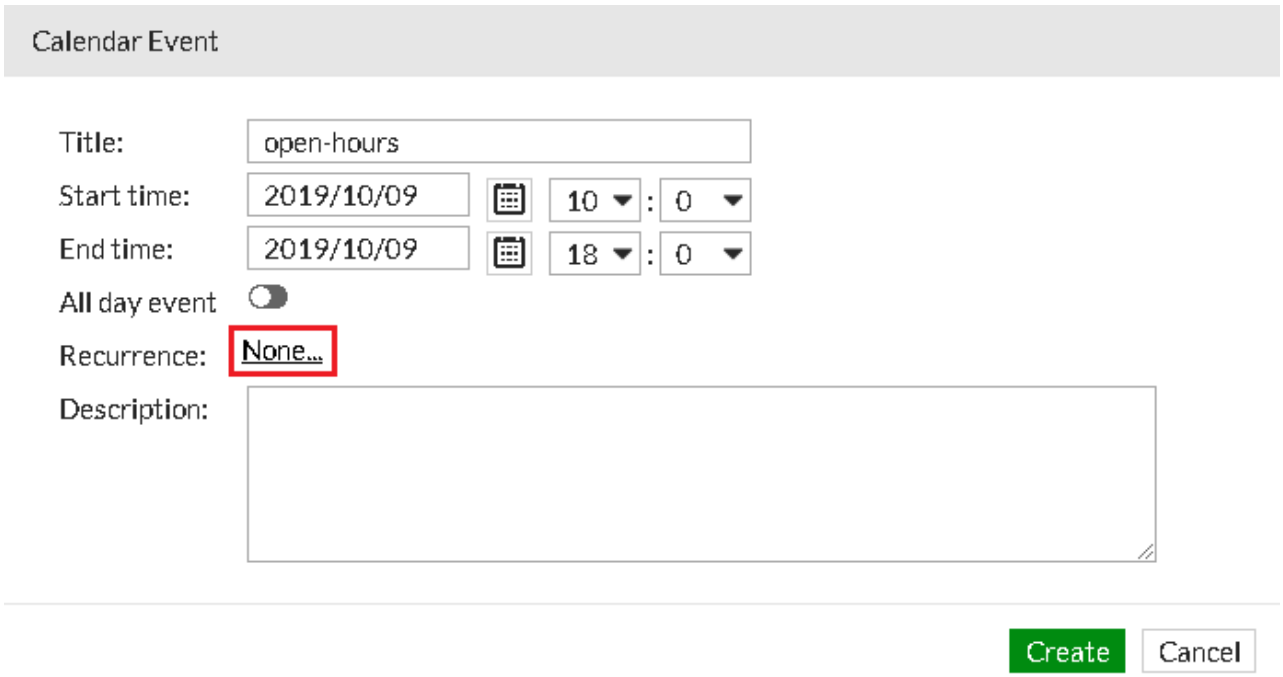
1. Go to **Phone System > Profile > Schedule** and click **New**.
2. Enter a **Name** (in this example, **Custom_business**), set **Mode** to **Calendar**, and click **Create**.



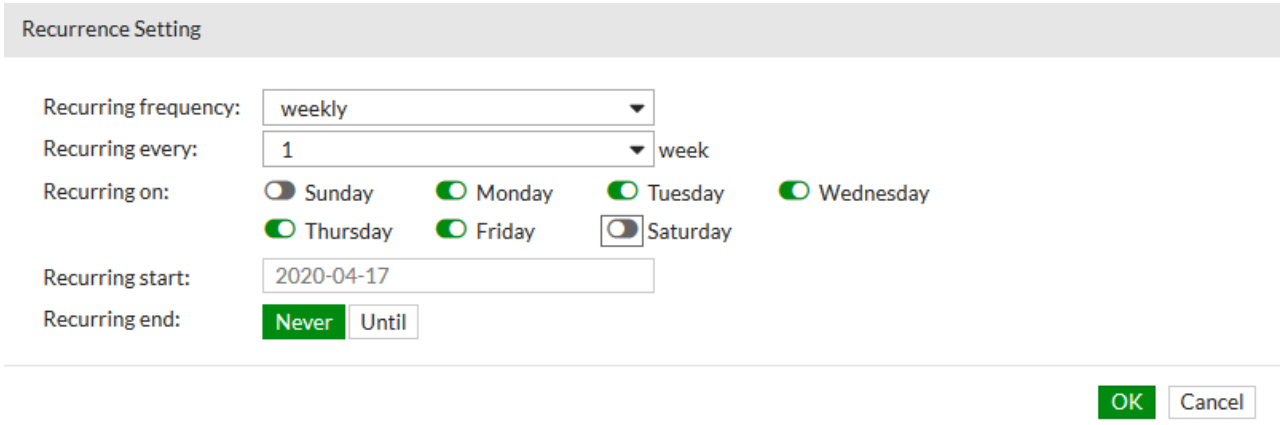
3. Once created, select the schedule from the list and click **Edit**.
4. You will be presented with the calendar view. Click **New**.



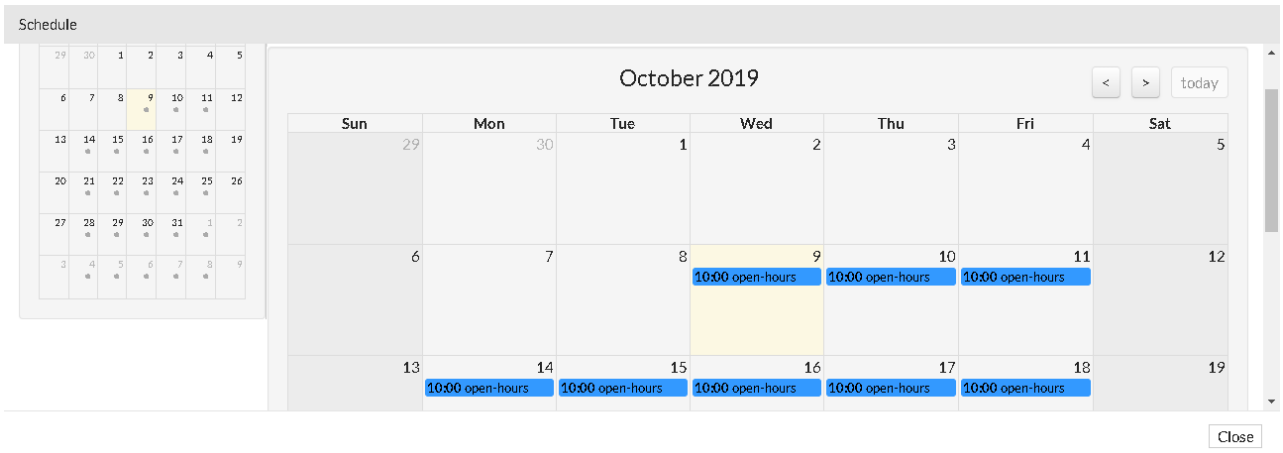
5. Enter a **Title**, a **Start time**, and an **End time**. These are your business operation hours (in this example, 10 AM to 6 PM). Then click **None** next to **Recurrence** to configure a recurrent frequency.



6. Set the following **Recurrence Setting**. In this example, an indefinite weekday-only schedule that occurs every week.
7. Click **OK**, and then **Create**.



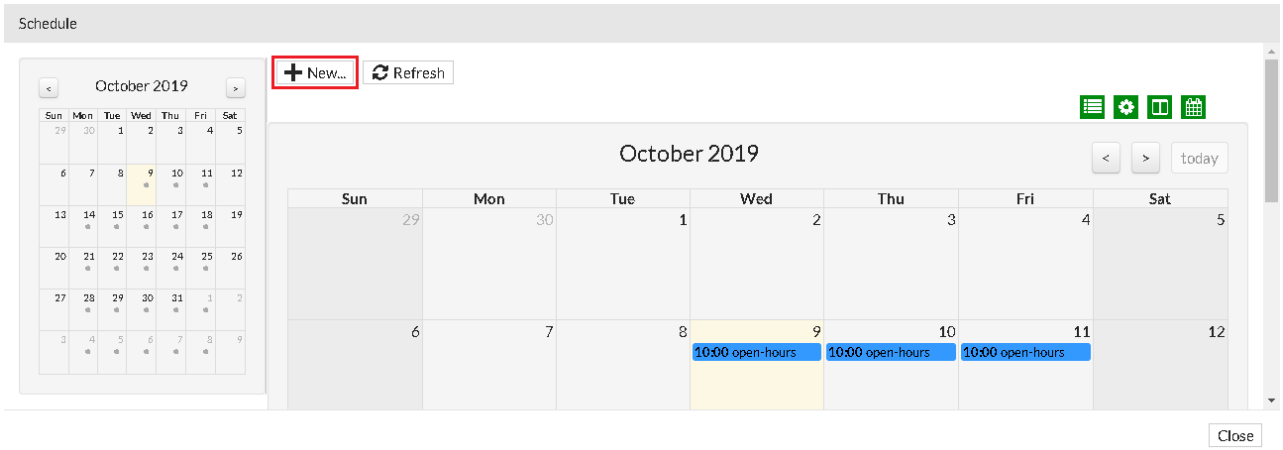
The calendar view shows the business hours schedule automatically populated for each day that was selected.



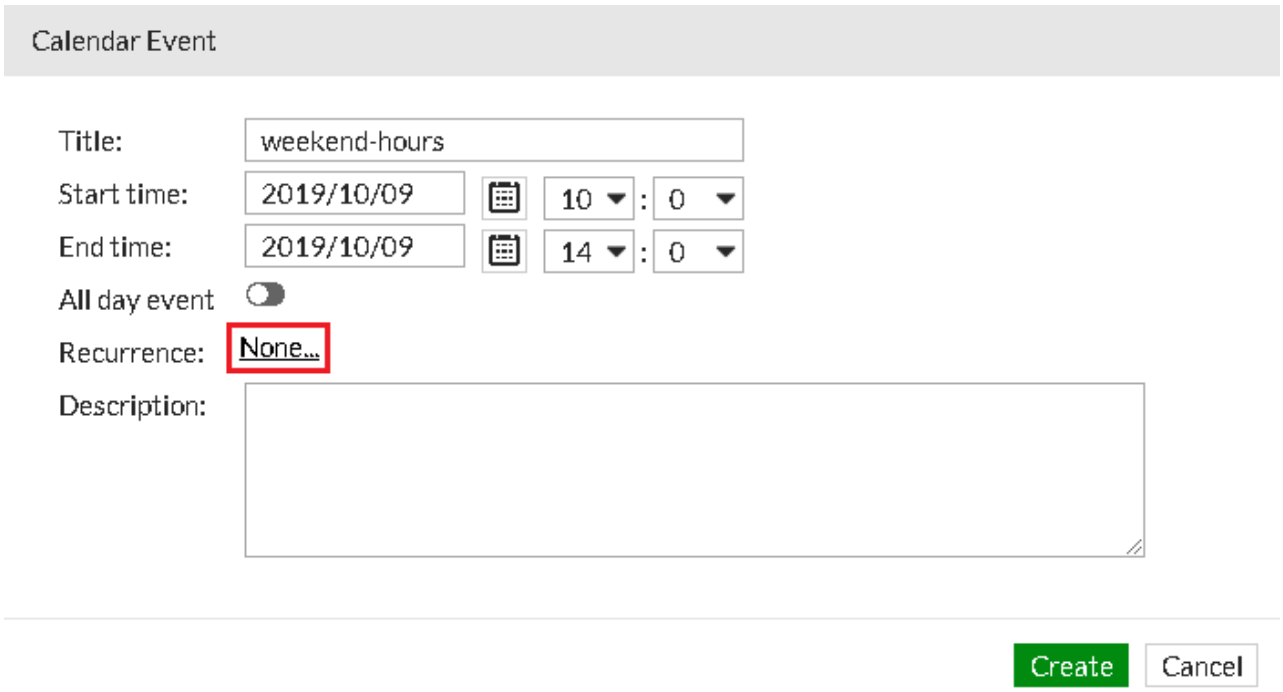
To define different hours for the weekend:

In this example, weekends will be defined as reduced-hour workdays.

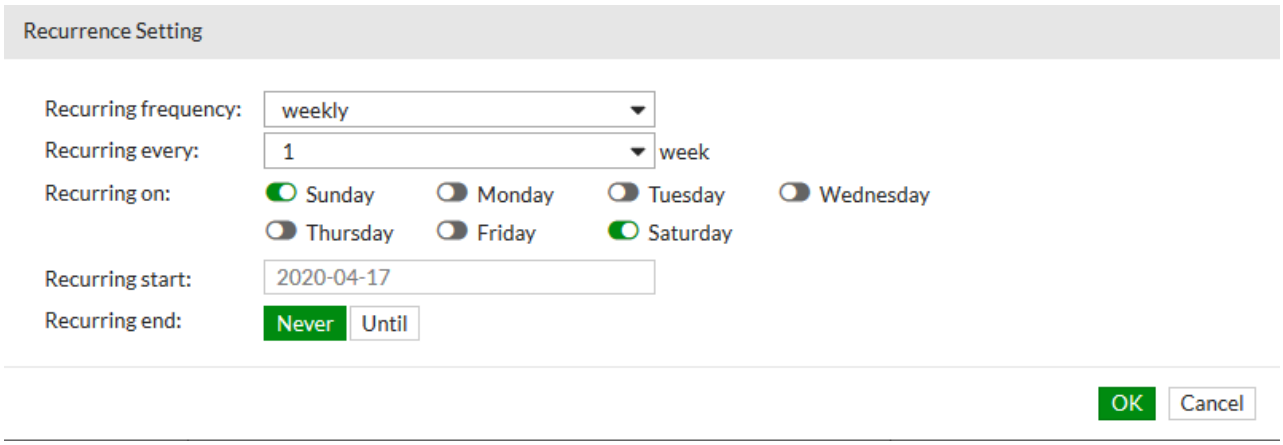
1. Within your existing business calendar, click **New**.



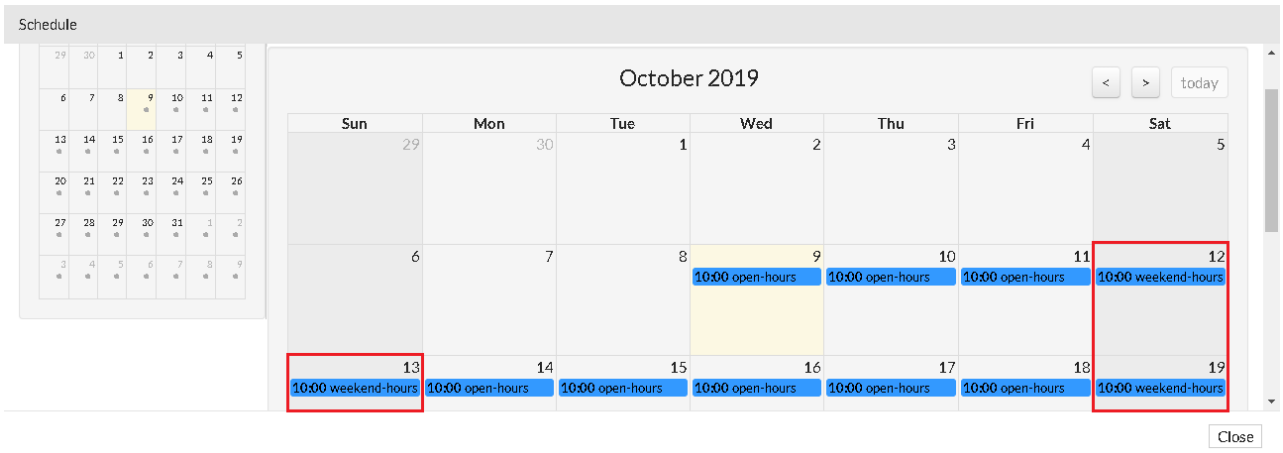
2. Enter a **Title**, a **Start time**, and an **End time**. This is your reduced operation hours (in this example, 10 AM to 2 PM). Note that the date shown here is today/the day you are creating this schedule, and happens to be a weekday. Leave this as it is. Then click **None** next to **Recurrence** to configure a recurrent frequency.



3. Set the following **Recurrence Setting**. In this example, an indefinite weekend-only schedule that occurs every week. Note that **Recurring start** is greyed-out, and is again set to today. This does not matter, as only the days specified in the **Recurring on** fields will be affected by this schedule.
Click **OK**, and then **Create**.



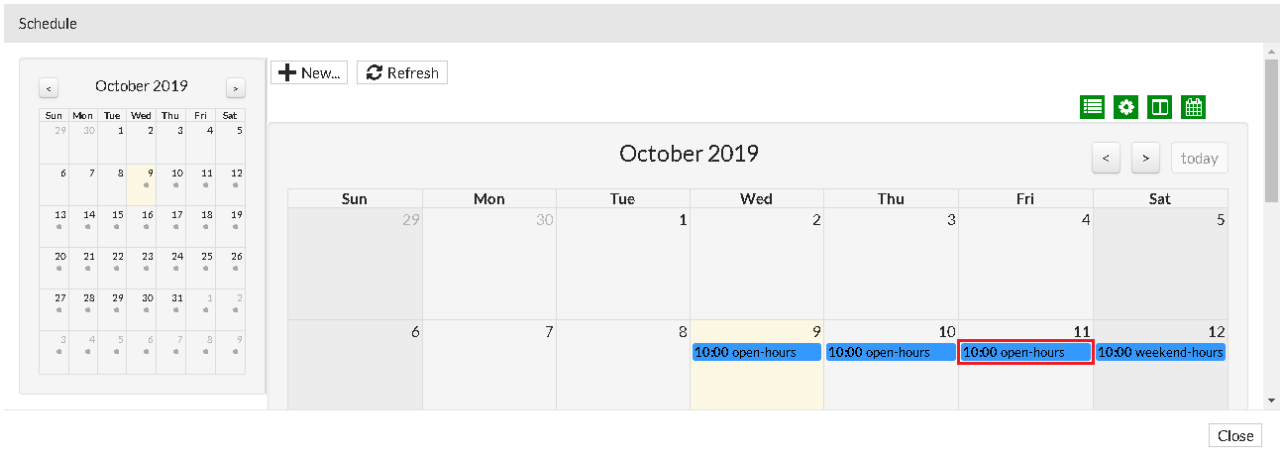
The calendar view shows the newly created weekend hours automatically populated alongside the regular business hours.



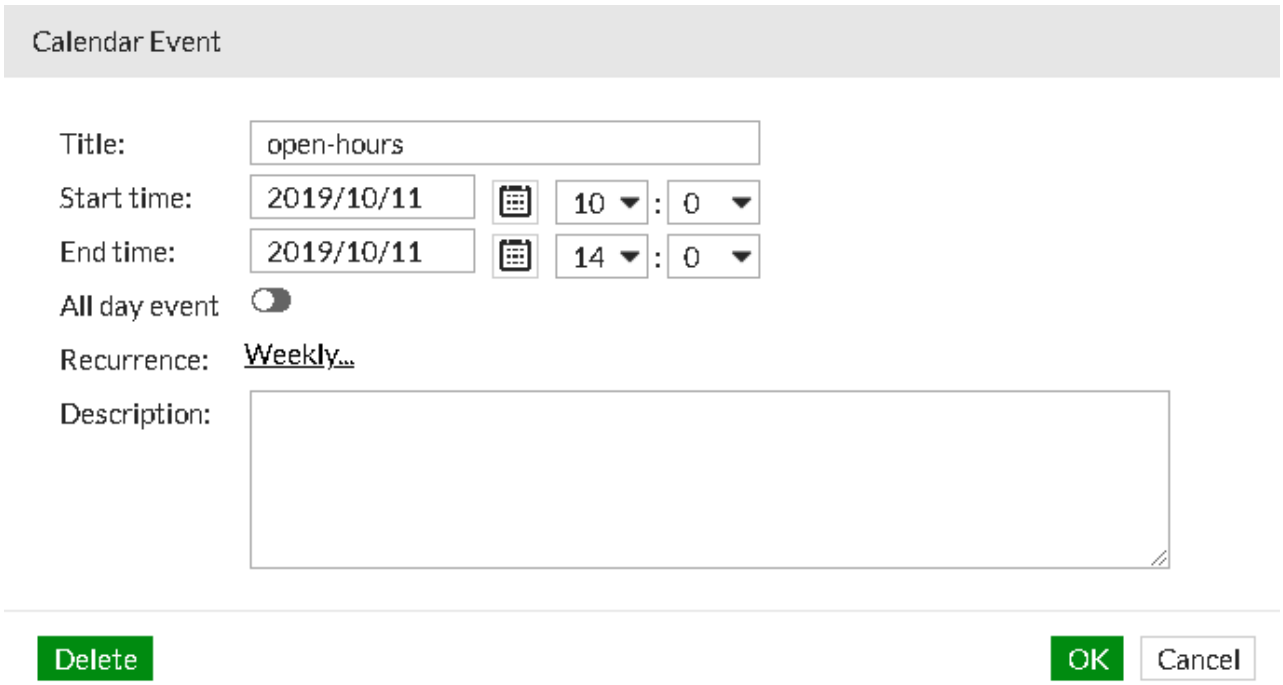
To define unique hours for a specific date:

The benefit to using calendar-based schedules is that they are perpetual schedules that can be easily edited. For example, you may want to edit your business hours for one specific date.

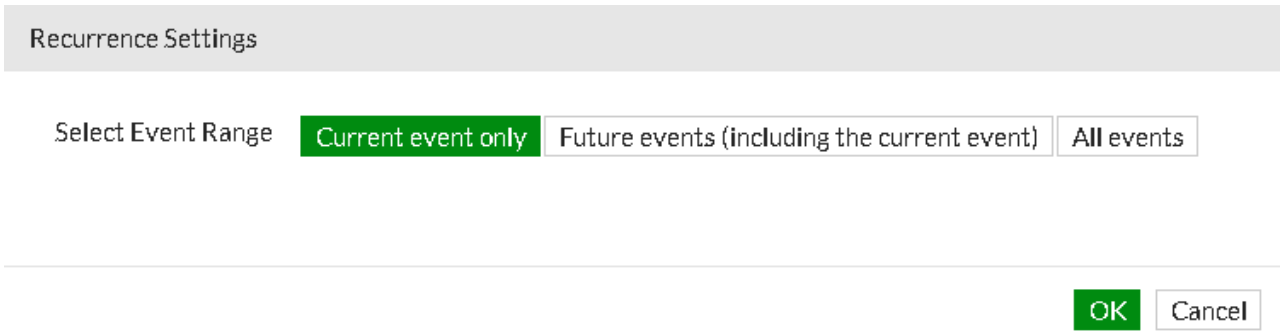
1. Go to **Phone System > Profile > Schedule** and edit your existing calendar-based business schedule.
2. Click the calendar event on the date that you would like to edit (for example, this coming Friday, October 11th). Be sure to click the event itself and not the area surrounding the event, otherwise a new event will be created instead.



3. Change the hours as necessary, and click **OK**. In this example, the **End time** has been reduced from 6 PM to 2 PM.



4. Before the new time can take effect, set **Select Event Range** to **Current event only**, meaning that only this specific day will be affected. Click **OK**.



Configuring call handling with schedules

When you have schedules ready to use, they can be added to the call handling of any of the FortiVoice features. As the configuration for adding a schedule is the same for all features, one call handling example will be used for inbound calls.

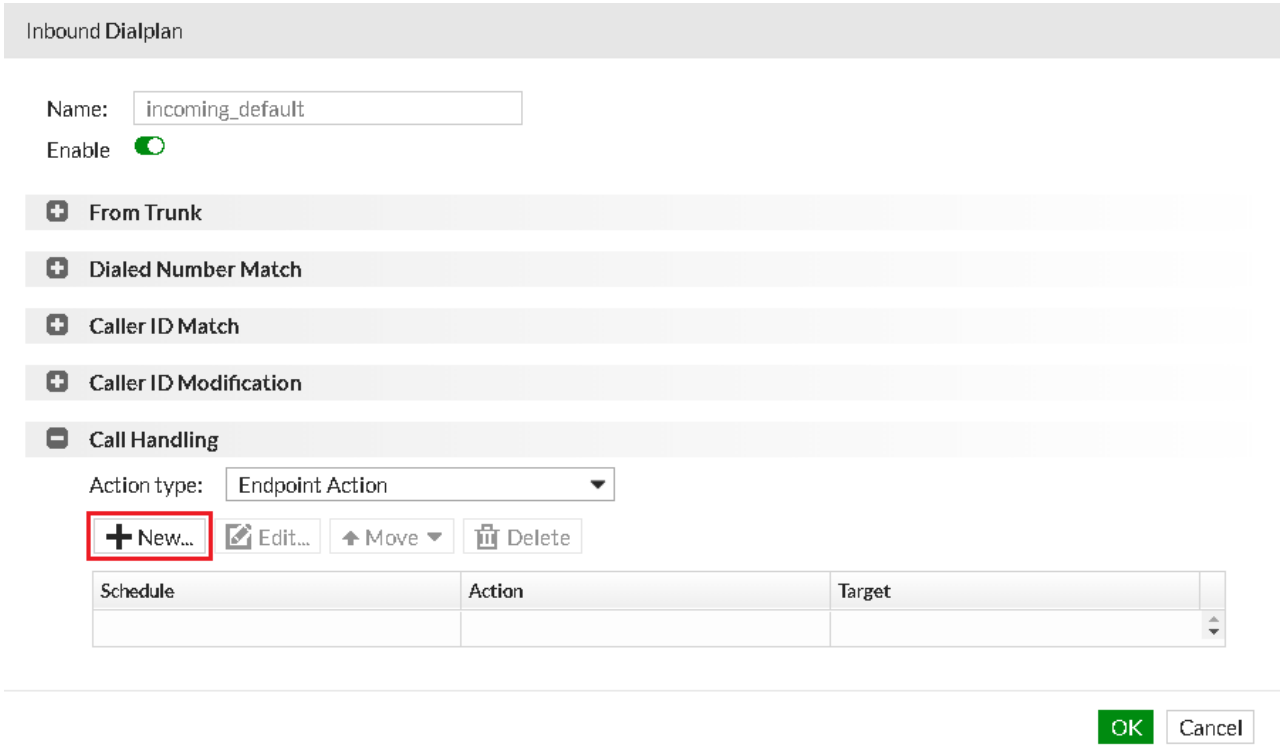
In this example the schedules will be put in a specific order as the FortiVoice checks schedules in the list from first to last. The order of the schedules will be:

- **Custom_holiday**: Checked first to see if the calls are coming in during a scheduled holiday.
- **Custom_business**: Checked second to ensure the call is coming in during scheduled business hours.
- **Any_time**: Checked last to handle any calls that fall outside of the business hours.

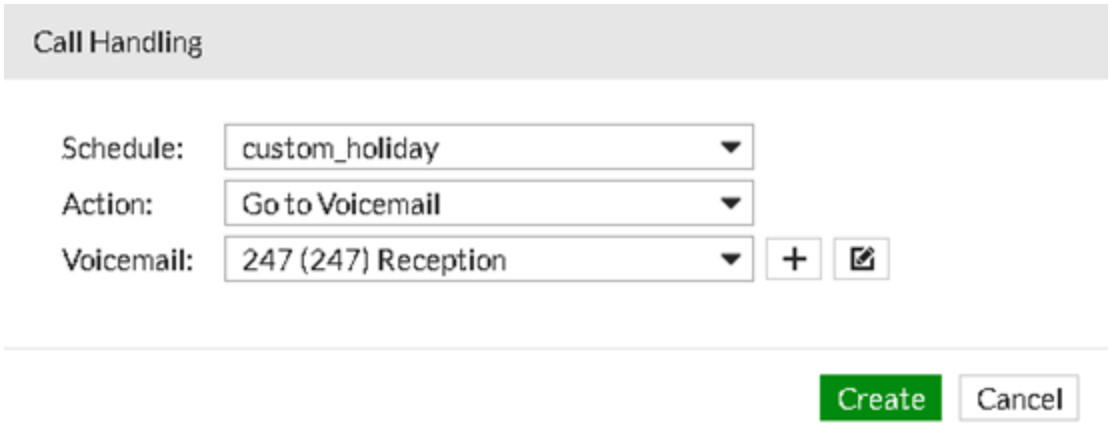
To configure inbound call handling with a schedule:

1. Go to **Call Routing > Inbound > Inbound**.
2. Select your inbound call routing rule and click **Edit**.

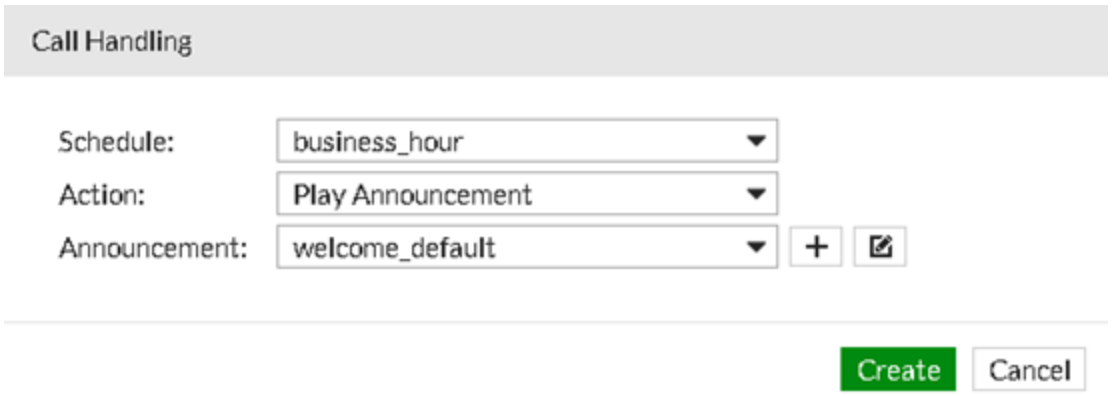
3. Under **Call Handling** click **New**.



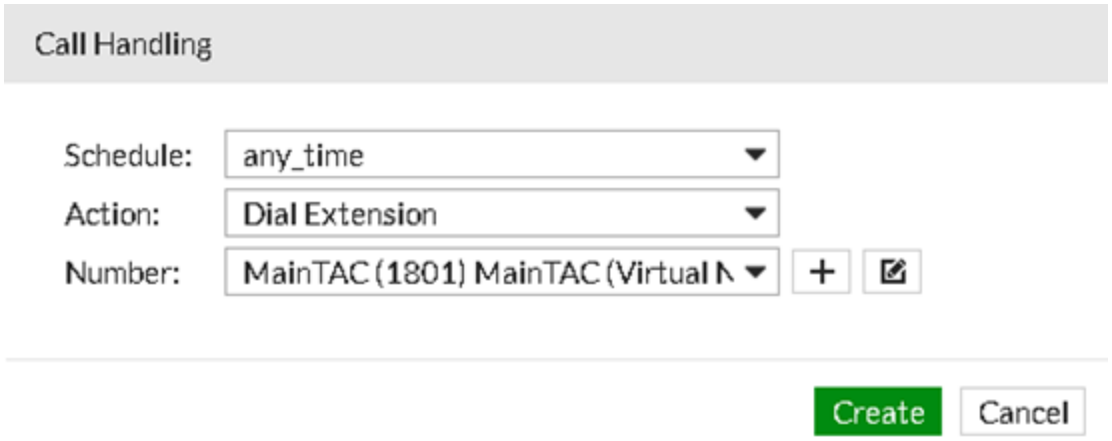
4. Set **Schedule** to the holiday schedule, and set an appropriate **Action** to perform on holidays. Click **Create**.



5. Click **New** to create a second **Call Handling** action.
6. Set **Schedule** to the business schedule, and set an appropriate **Action** to perform during business hours. Click **Create**.



7. Click **New** to create a third **Call Handling** action.
8. Set **Schedule** to the default any_time schedule, and set an appropriate **Action** to perform outside of business hours. Click **Create**.



9. Click **OK** to finish the inbound dial plan configuration.

Security

This section contains information about establishing and maintaining a secure phone system.

As with network security, make sure that FortiGate manages your phone system.

Before your begin, make sure that you have the latest software running on your FortiVoice phone system to take advantage of the latest features and enhancements that are available to you.

This section includes the following recipes:

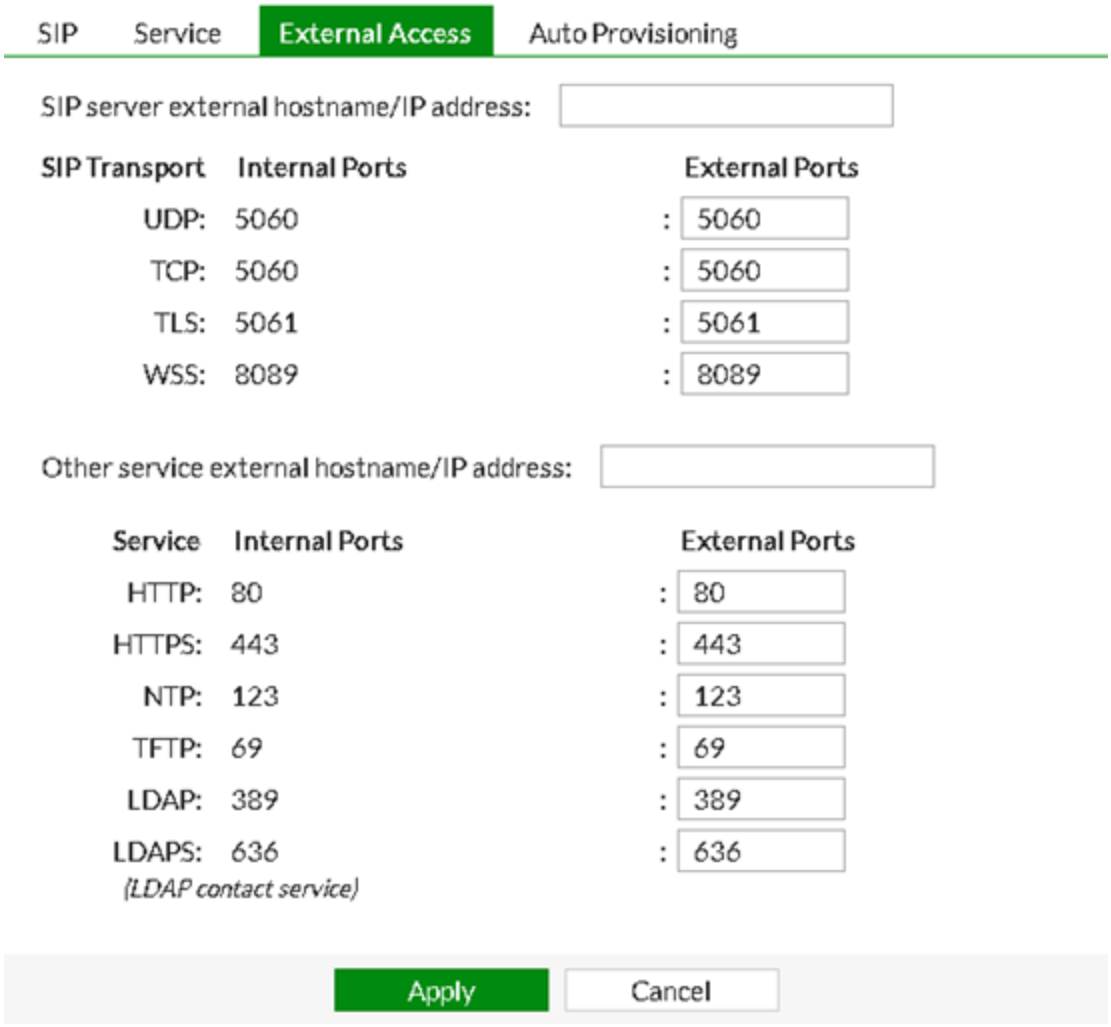
- Changing the default external access ports on page 90
- Changing the default passwords on page 91
- Disabling recommended features on page 96
- Configuring additional settings on page 97
- Monitoring and reporting on page 102

Changing the default external access ports

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

Avoid changing any of the protocol ports to four digit numbers, such as 5065 or 5070, as those are used by other brands and are commonly scanned port numbers.

1. Go to **System > Advanced > External Access**.
2. You have the option to change the following SIP transport protocol ports:
   - **UDP**: This is the default signaling port used for external extensions, VoIP trunking, and office peers. Choose a five digit number.
   - **TCP**: This is the default signaling port used for the FortiFone softclient. Choose a five digit number.
   - **TLS**: This is the default port for SIP sessions encrypted with Transport Layer Security (TLS). Choose a five digit number.
   - **WSS**: WebSocket Secure is used to support the FortiFone desktop application. Choose a five digit number.
3. Additionally, you can configure the service external ports. Click **Apply** when finished.



Changing the default passwords

Many of the default passwords are too simple and are therefore more susceptible to compromise. It is recommended to take the time to change the default passwords to more secure passwords.

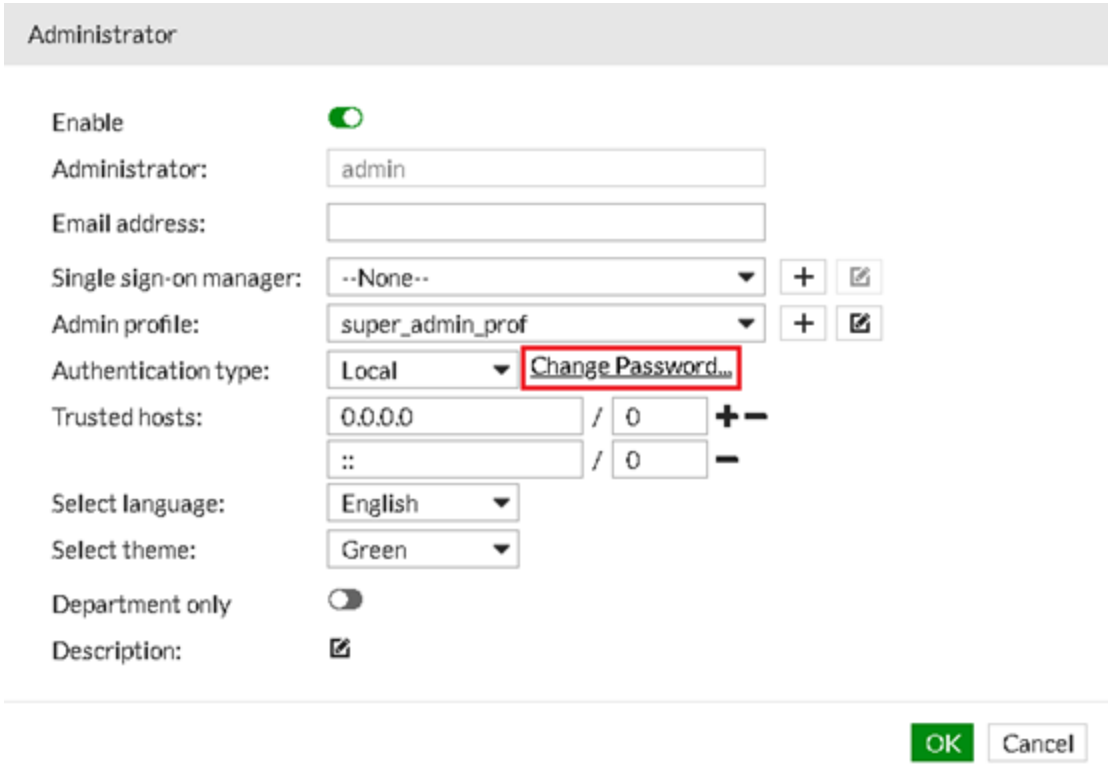
This section includes the following topics:

- Administrator password on page 91
- Administrator PIN on page 92
- Call Bridge (DISA) account code on page 92
- User voicemail PIN on page 93
- Password and PIN policy on page 94
- Office peers on page 95

Administrator password

Establish a more secure administrator password on the system.

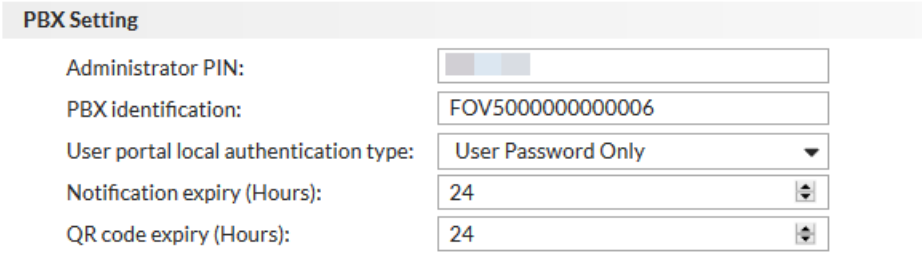
1. Go to **System > Administrator > Administrator**.
2. Select the **admin** account and click **Edit**.
3. Click **Change Password**, enter and confirm a new password, and click **OK**.



Administrator PIN

The administrator PIN allows the owner of the PIN to change extension assignments and modes from any phone or auto attendant.

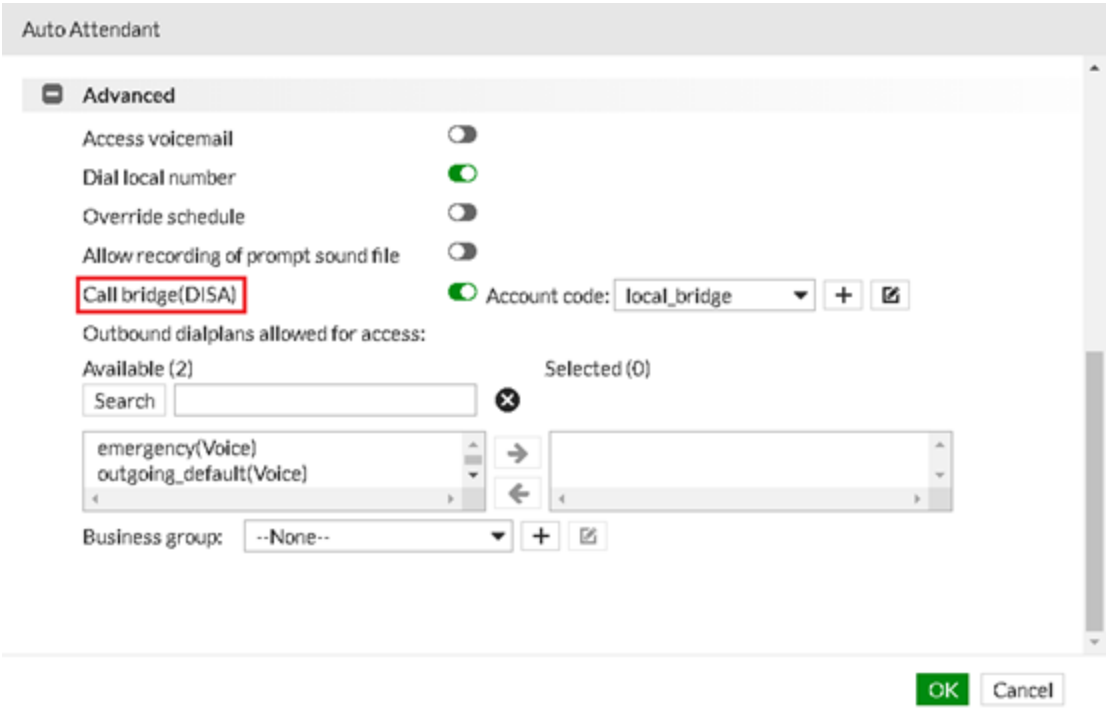
1. Go to **Phone System > Setting > Miscellaneous**.
2. Under **PBX Setting**, enter a new **Administrator PIN**, and click **Apply**.



Call Bridge (DISA) account code

The Call Bridge Direct Inward System Access (DISA) feature allows callers to make outgoing calls from the auto attendant. If enabled, configure this feature to use an account code.

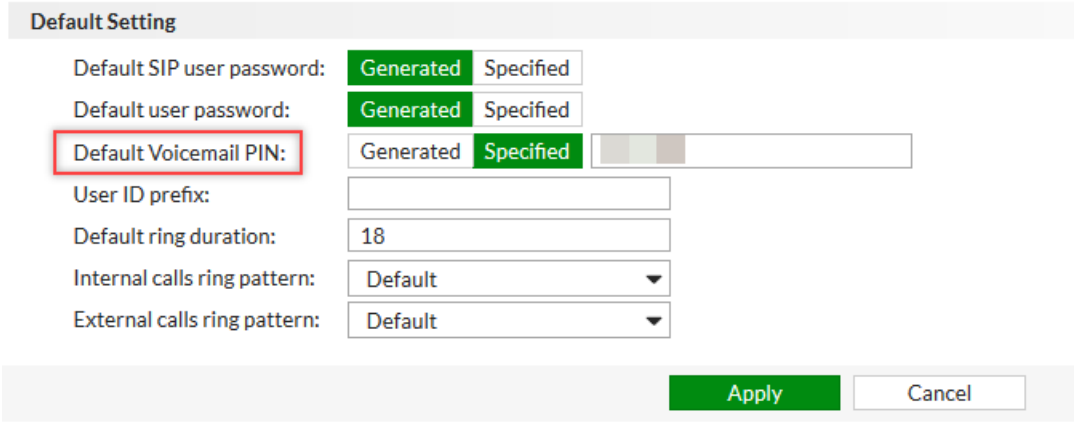
1. Go to **Call Feature > Auto Attendant > Auto Attendant**.
2. Select an auto attendant and click **Edit**.
3. Under **Advanced**, enable **Call bridge (DISA)** and select the appropriate **Account code**, or create a new one.
4. Click **OK**.



User voicemail PIN

The default user voicemail PIN is **123123**. It is highly recommended to change this default PIN.

1. Go to **Phone System > Setting > Option**.
2. Under **Default Setting**, enter a new **Default Voicemail PIN**. Select either **Specified** and enter your own PIN or **Generated** to generate a random PIN, and click **Apply**.



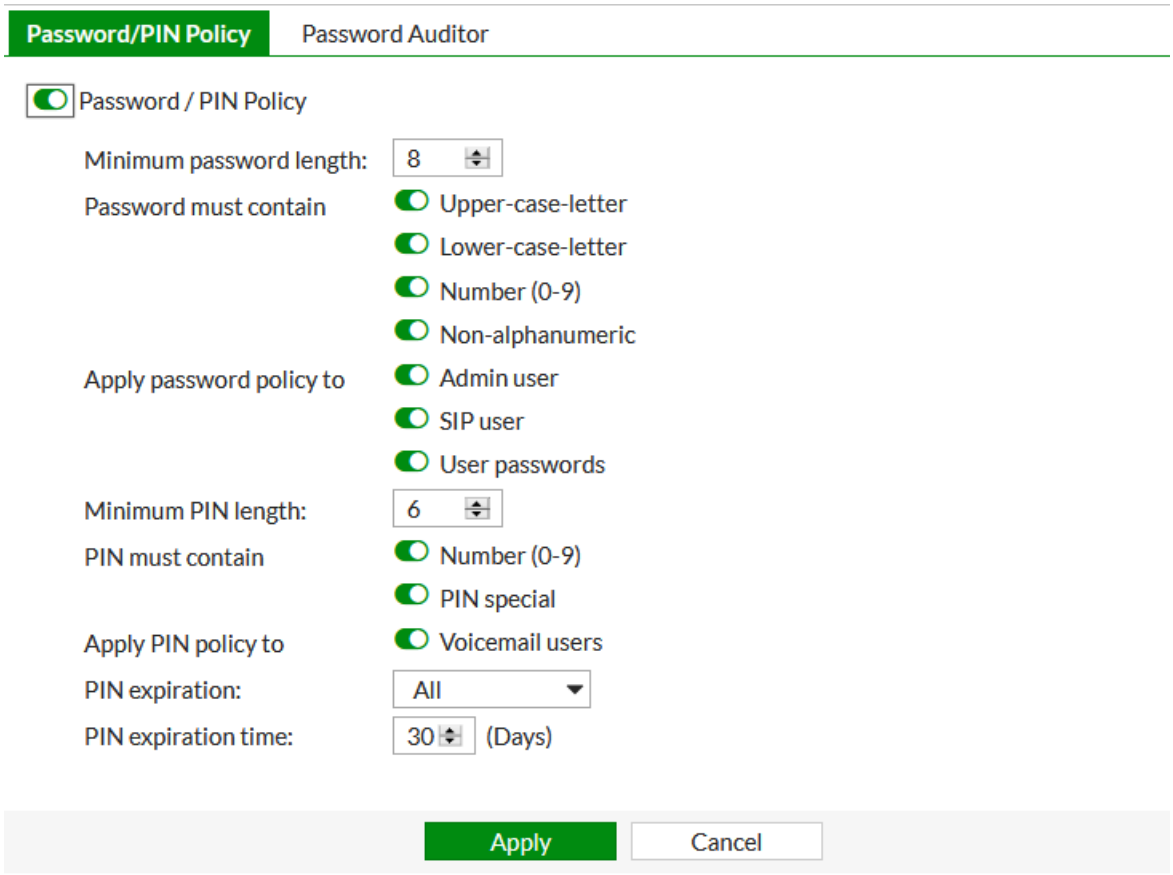
Password and PIN policy

Set a secure password policy that requires upper and lower case characters and alpha numerical characters for administrator passwords and SIP passwords.

1. Go to **Security > Password Policy > Password/PIN Policy**.
2. Configure the following settings, as required.

GUI field	Description
Password / PIN policy	Select to enable or disable the SIP password and user PIN policy for administrators and extension users.
Minimum password length	Set the minimum acceptable length for passwords. The default is 8 characters.
Password must contain	Select any of the following special character types to require in a password. Each selected type must occur at least once in the password. • **Upper-case-letter** — A, B, C, ... Z • **Lower-case-letter** — a, b, c, ... z • **Number** — 0 ... 9 • **Non-alphanumeric** — punctuation marks, @,#, ... %
Apply password policy to	Make sure to select the users that you want to apply this policy to. • **Admin user**: Apply to administrator web-based manager passwords. If any password does not conform to the policy, require that administrator to change the password at the next login. • **SIP users**: Apply to FortiVoice SIP phone users' passwords. If any password does not conform to the policy, require that user to change the password at the next login. • **User passwords**: Apply to user portal access passwords. If any password does not conform to the policy, require that user to change the password at the next login.
Minimum PIN length	Set the minimum acceptable length for the user PIN. The default is 6 characters.
PIN must contain	**Number**: Allows the use of numbers (0 to 9) in the PIN. **PIN special**: Allows the use of the ***** and **#** special characters.
Apply PIN policy to	Select to enable or disable the PIN policy for voicemail users.
PIN expiration	Select one of the following options to apply to the voicemail PIN policy: • **Never**: Specifies that users set their voicemail PIN and this PIN never expires. • **Default Only**: Specifies that users using the default voicemail PIN are prompted to set a new PIN when accessing their voicemail for the first time. • **All**: Specifies that the FortiVoice unit prompts users to set a new PIN when they access their voicemail for the first time and any time after the **PIN expiration time**.

GUI field	Description
PIN expiration time	If you selected **All** in **PIN expiration**, then update the **PIN expiration time** to specify the number of days a PIN can be used. After the expiration time, the user must enter a new PIN.



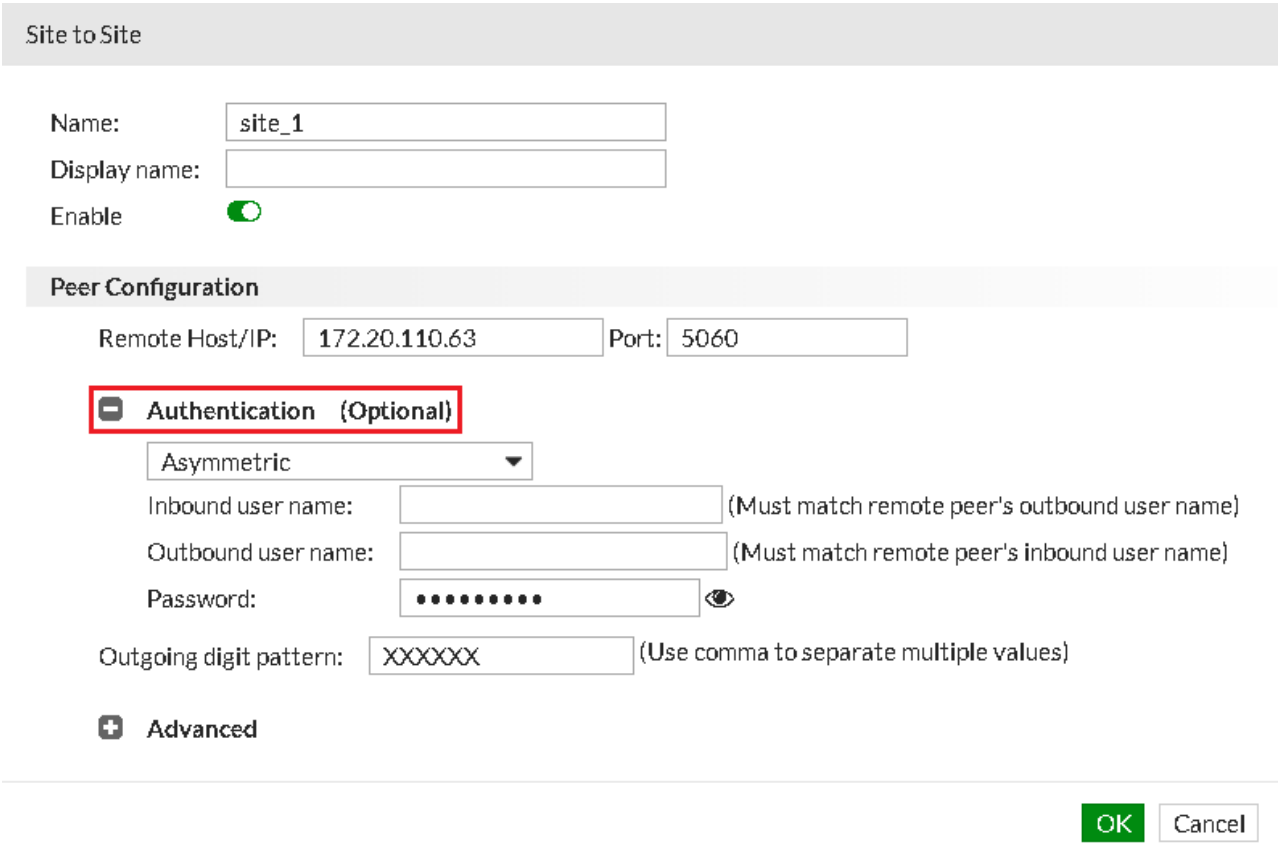
3. Click **Apply**.

Office peers

Authentication can be configured for inbound and outbound calls on office peer trunks.

1. Go to **Trunk > Office Peer > Office Peer**.
2. Create a new **Site to Site** or **Custom** office peer or select an existing one.
3. Under **Peer Configuration**, expand **Authentication (Optional)** and select one of the following options from the drop-down menu:
   - **Symmetric**: Both PBX devices will use the following information to form the office peer trunk and authenticate each other. The defined **User name** and **Password** must be the same on both PBX devices forming the office peer trunk.
   - **Asymmetric**: Used to authenticate incoming and outgoing calls. Enter the **Inbound user name**, **Outbound user name**, and **Password**. These settings must be the same on both PBX devices forming the office peer trunk.

4. Define an **Outgoing digit pattern** (set to **XXXXXX** by default, or a six-digit code), and click **OK** or **Create**.



Disabling recommended features

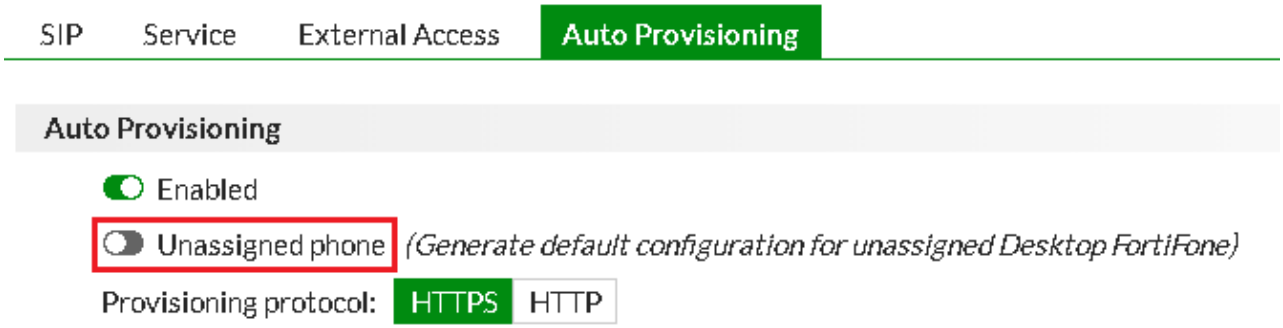
Many features are enabled by default to assist with the initial setup. After setup, however, we recommend disabling any features that you feel are unnecessary.

Generate default configuration

After the initial setup, disable the **Unassigned phone** option. When you disable this feature, FortiVoice does not automatically create a default configuration file when it receives a request from an unassigned phone.

1. Go to **System > Advanced > Auto Provisioning**.
2. Under **Auto Provisioning**, disable **Unassigned phone**. Automatic default configurations for unassigned phones will no longer be generated.

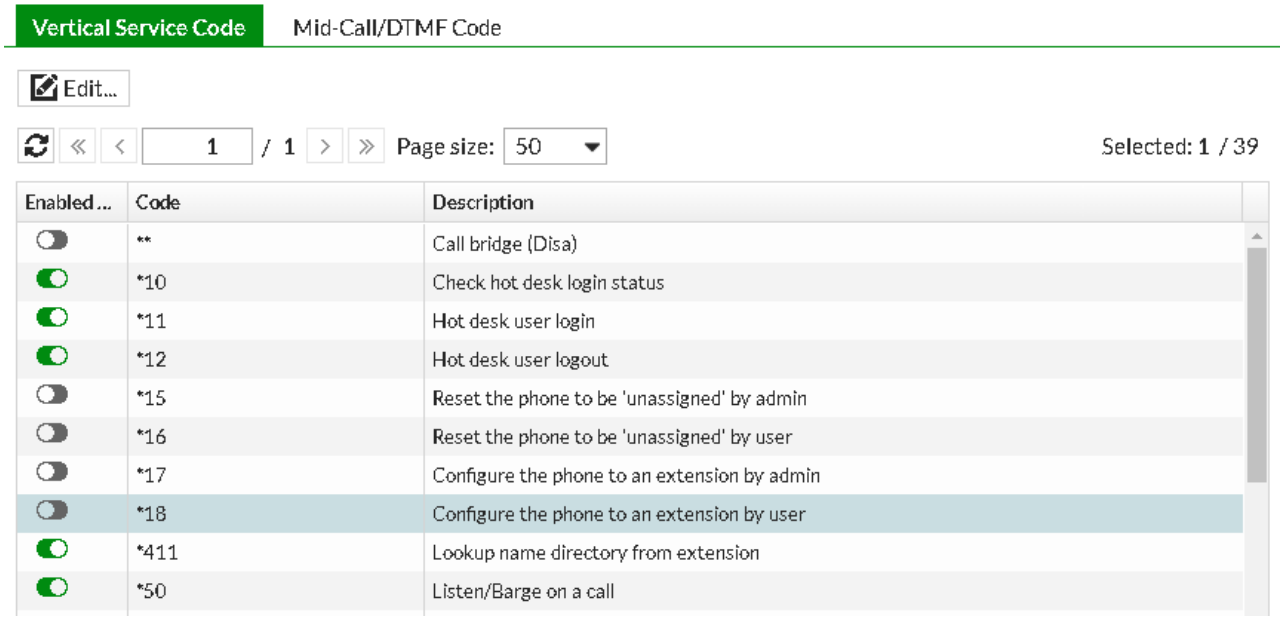
3. Click **Apply**.



Vertical service codes

Disable any service codes that you do not use.

1. Go to **Call Feature > Feature Code > Vertical Service Code**.
2. Disable the codes that you will not be requiring, such as the following:
   - **: Call bridge (DISA).
   - ***15**: Reset the phone to be "unassigned" by admin.
   - ***16**: Reset the phone to be "unassigned" by user.
   - ***17**: Configure the phone to an extension by admin.
   - ***18**: Configure the phone to an extension by user.



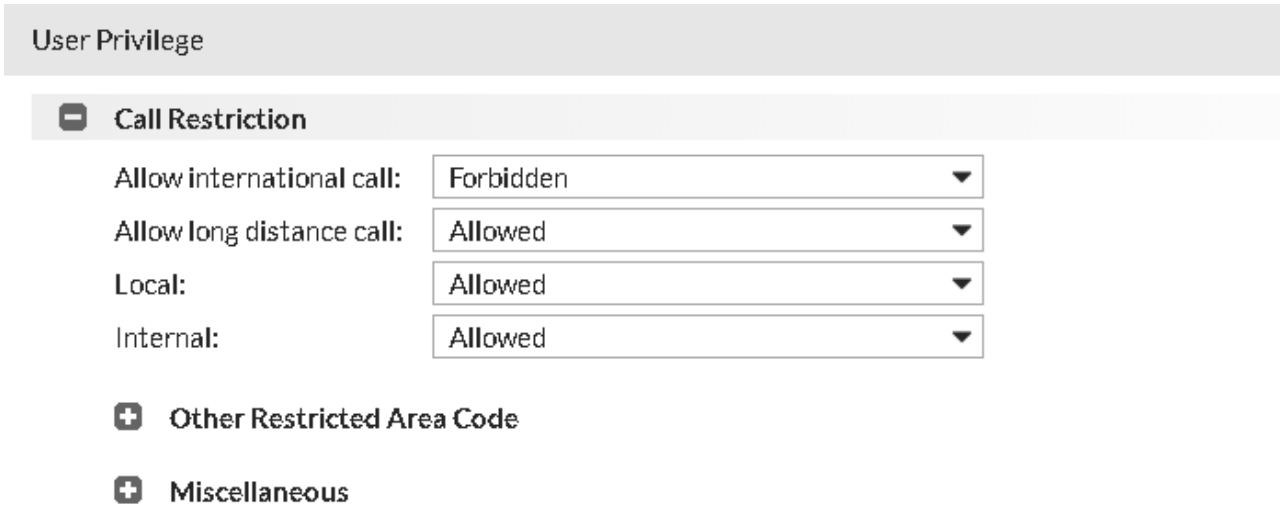
Configuring additional settings

In order to provide another level of protection beyond external abuse, there are a number of settings that you can enable to protect the FortiVoice phone system from internal abuse.

Call restrictions and common phones

Restrictions can be put in place based on call types, such as blocking international or toll calls.

1. Go to **Security > User Privilege > User Privilege**.
2. Select a user privilege and click **Edit**.
3. Expand **Call Restriction** and configure the settings accordingly.



Extensions that are placed in common areas, such as store floors and kitchens, should have the highest restriction levels, which include a PIN code to make calls.

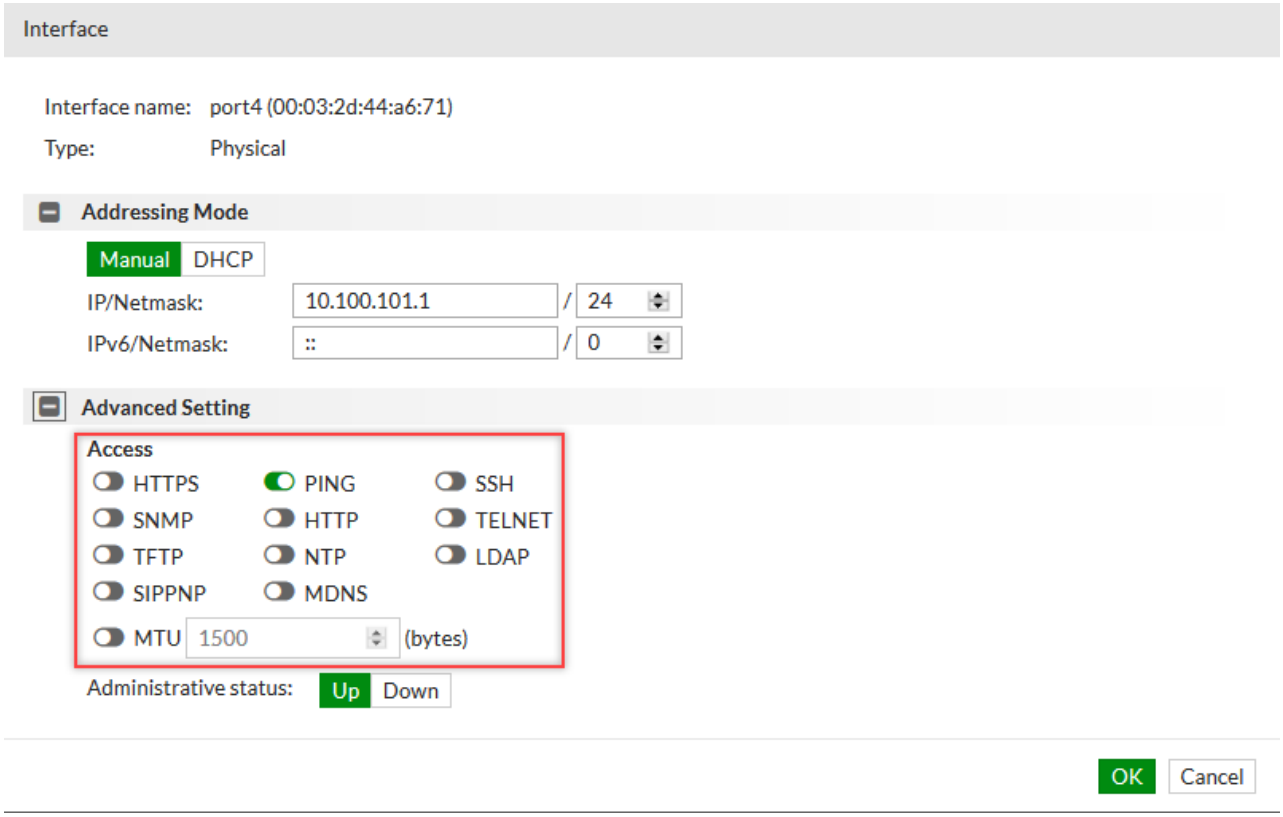
4. Set the appropriate call type to **Allowed with Account Code**, **Allowed with Personal Code**, or **Allowed with Account and Personal Code**.

Interface access

Any access methods that are not being used on the FortiVoice device should be disabled.

1. Go to **System > Network > Network**.
2. Select an interface and click **Edit**.

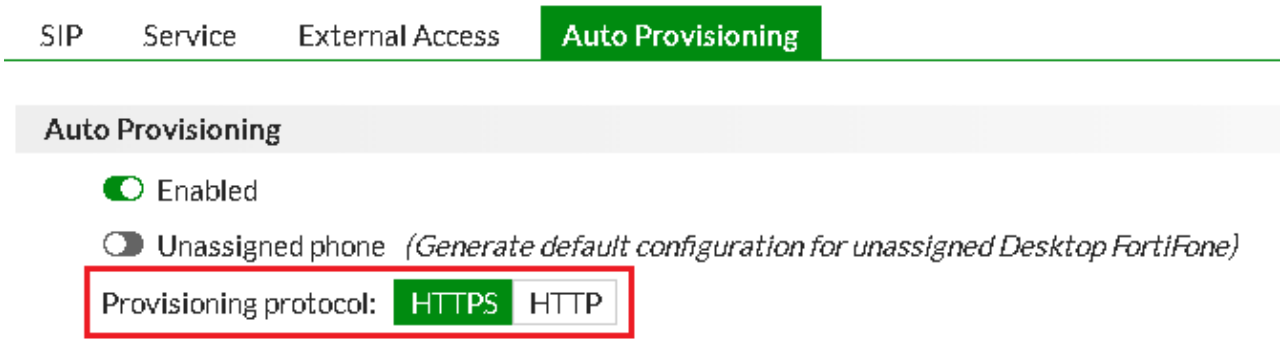
3. Under **Advanced Setting**, disable any unused **Access** protocols.



Guest provision protocol

Using HTTPS to provision FortiFone devices with FortiVoice is recommended.

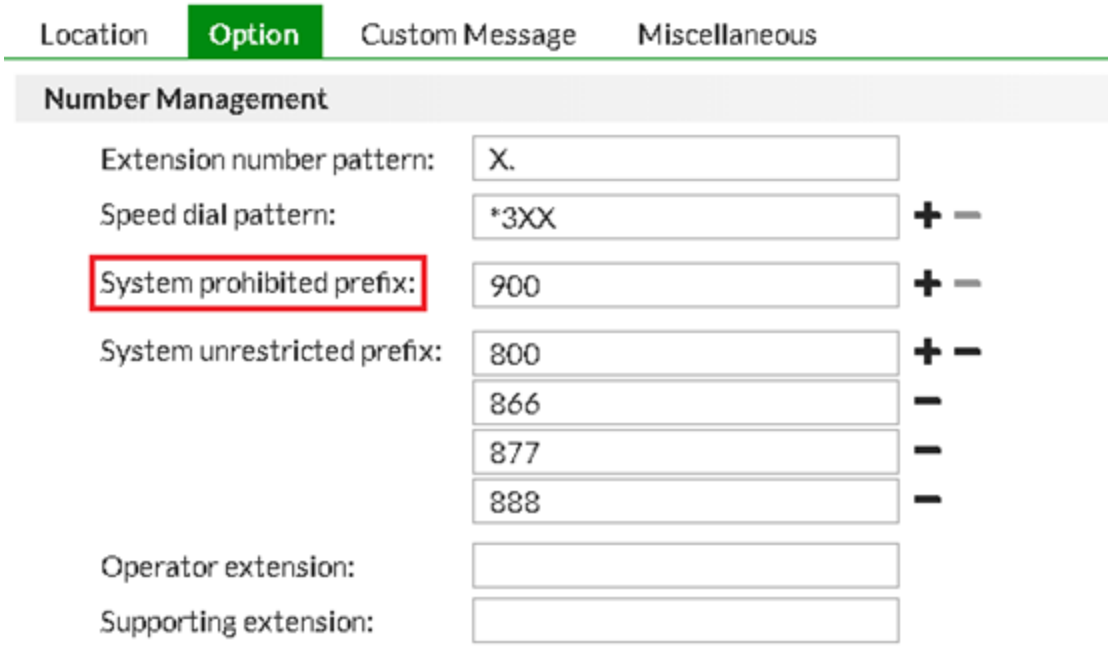
1. Go to **System > Advanced > Auto Provisioning**.
2. Under **Auto Provisioning**, set **Provisioning protocol** to **HTTPS**.



Prohibited prefixes

You may want to outright block certain phone number prefixes, such as 900 (blocked by default) which is commonly used for premium-rate calls, or phone calls with area codes originating from certain regions.

1. Go to **Phone System > Setting > Option**.
2. Under **Number Management**, add all undesirable prefixes to the **System prohibited prefix** section.

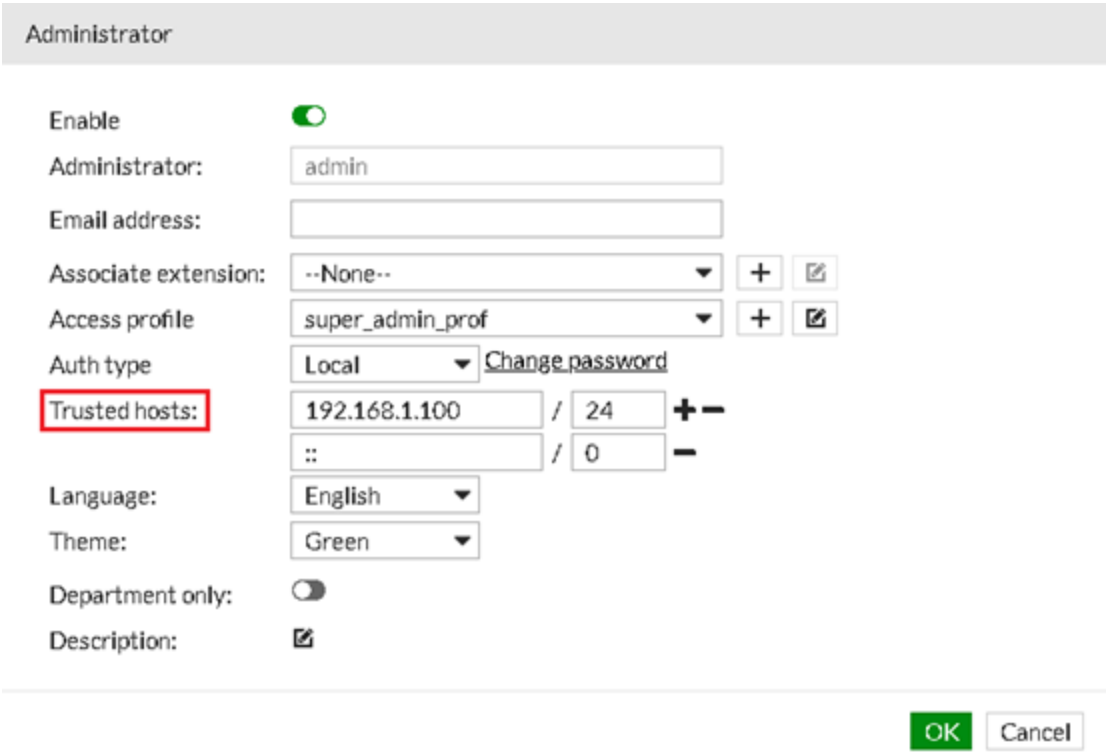


Trusted hosts for administrators

Certain IP subnets can be designated as allowed or trusted for administrators to log into FortiVoice. This configuration can allow local networks to access the system but restrict remote access to the system and restrict remote access to the system.

1. Go to **System > Administrator > Administrator**.
2. Select the administrator and click **Edit**.

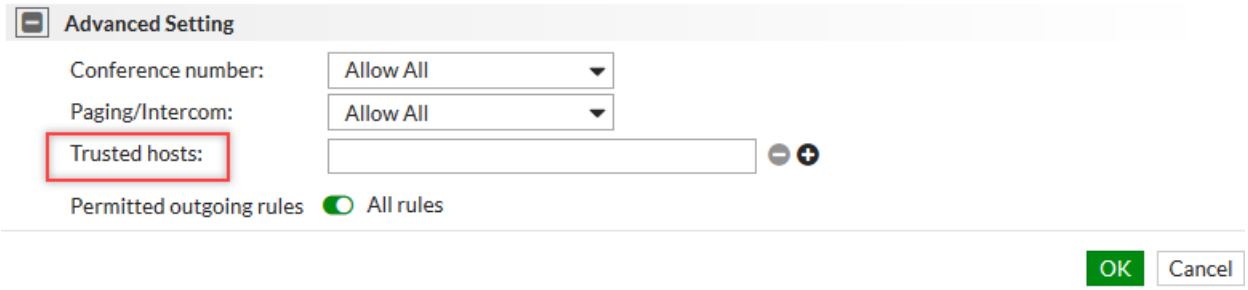
3. Set **Trusted hosts** to the local trusted IP subnet (define as many as required).



Trusted hosts for extensions

Certain IP subnets can also be designated as trusted for extensions to register to FortiVoice. This configuration can allow local networks to access the system but restrict remote access to the system and restrict remote access to the system.

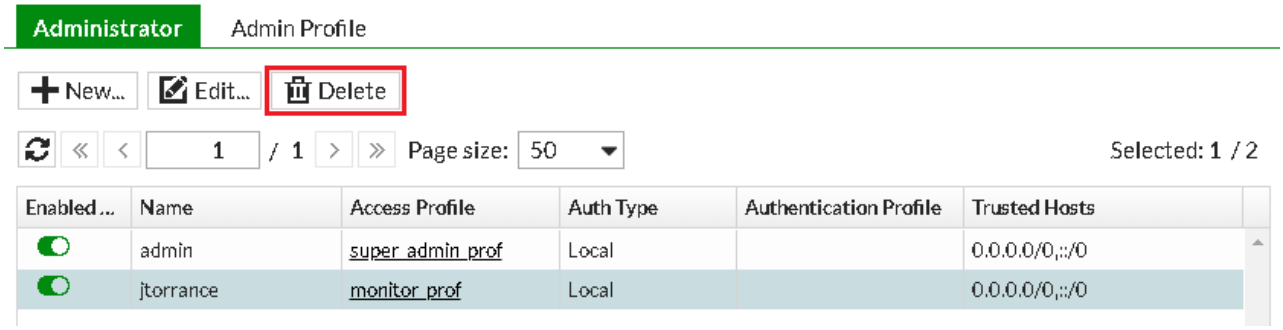
1. Go to **Phone System > Profile > User Privilege**.
2. Select a user privilege and click **Edit**.
3. Expand **Advanced Setting**, and set **Trusted hosts** to the local trusted IP subnet (define as many as required).



Unused administrators

Remove administrator profiles that are not in use.

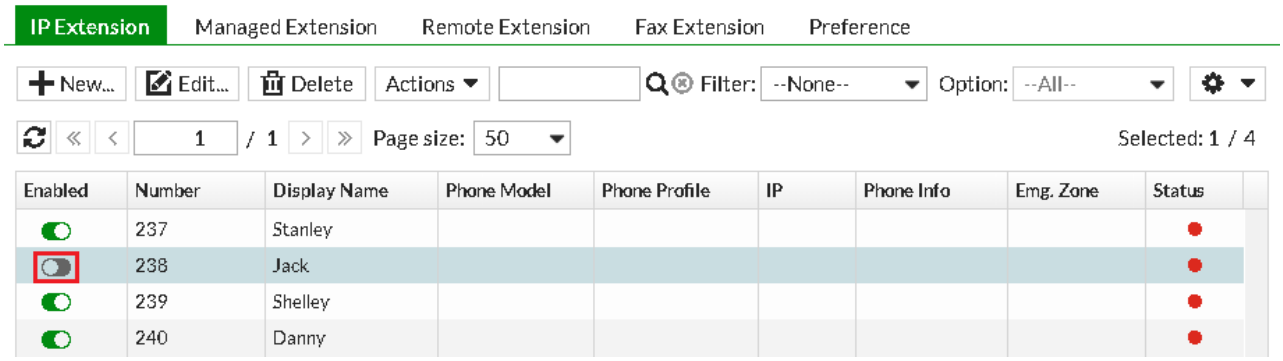
1. Go to **System > Administrator > Administrator**.
2. Select the administrators that are not active and click **Delete**.



Unused extensions

To avoid the unintentional use of unused extensions, remove those extensions.

1. Go to **Extension > Extension > IP Extension**.
2. Disable the extensions that are not active.



Verify SIP user agent

Restrict phone registration so only phone requests that match the system configured phone type are allowed.

1. Go to **Dashboard > Console** and click inside the window to connect to the CLI console.
2. Enter the following commands:

```
config system sip-setting
   set verify-user-agent enable
end
```

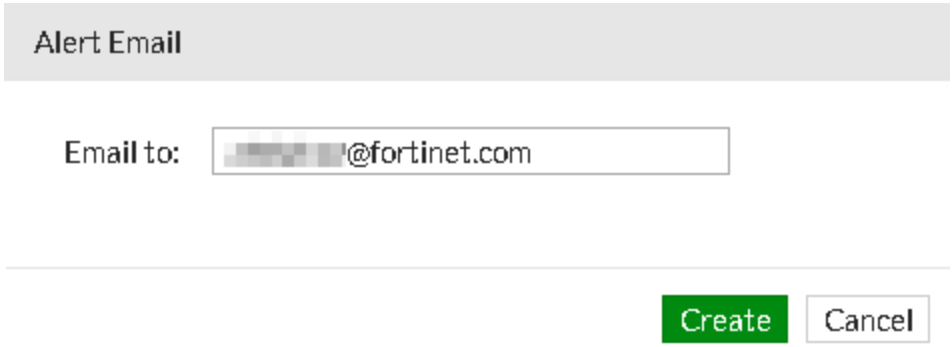
Monitoring and reporting

There are many tools within FortiVoice to help manage your security settings and help protect your system.

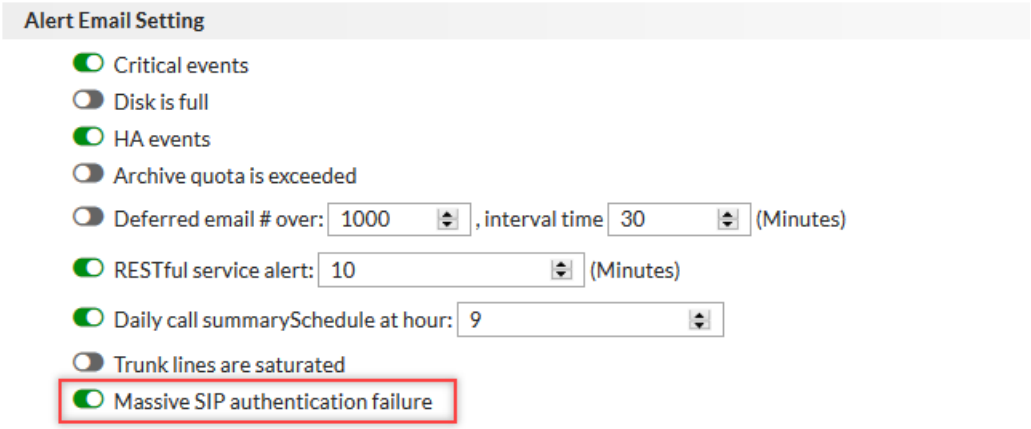
Administrator alerts

Administrators can be notified by email of system alerts when FortiVoice detects suspicious activity, such as a SIP attack.

1. Go to **Log & Report > Alert > Configuration** and click **New**.
2. Enter the administrator's email address and click **Create**.



3. Go to **Log & Report > Alert > Category**.
4. Under **Alert Email Setting**, enable **Massive SIP authentication failure**, and click **Apply**.

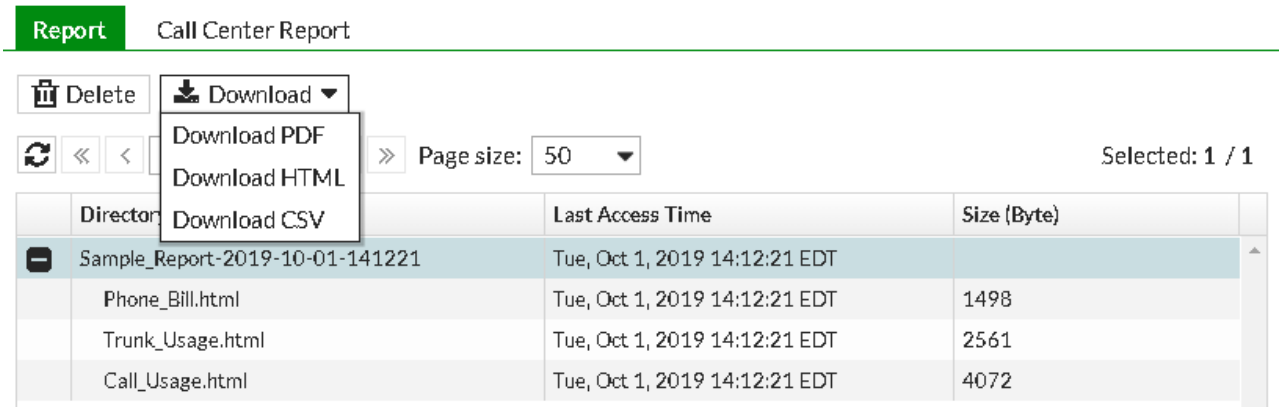


Call detail reports

Reports can be generated and downloaded for greater call inspection, such as for looking into details concerning blocked or denied calls.

1. Go to **Log & Report > Call Report > Call Report**.
2. Select the appropriate call report and click **Generate**.
3. A dialog window appears letting you know that the report has been started. Click **OK**.
4. Click **View Report**, where you are redirected to **Monitor > Call Report > Report**.
5. Expand the report generated to view the various components of the report. Select the whole report and click

Download and either **Download PDF**, **Download HTML**, or **Download CSV**.



SIP password auditor

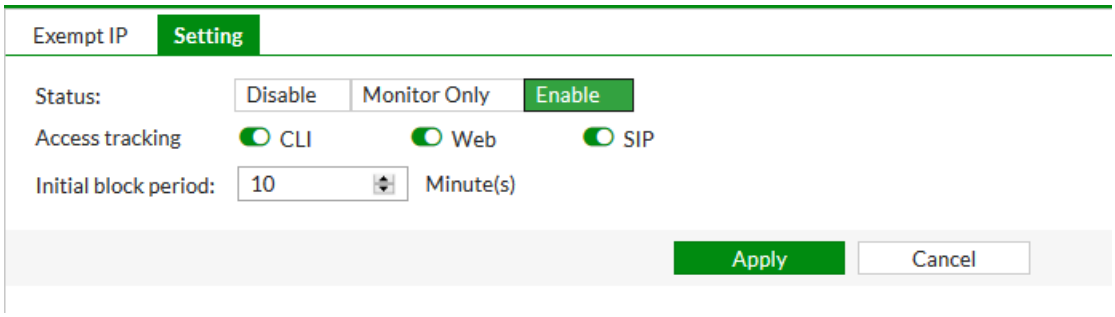
Frequently review the SIP password audits to make sure that SIP passwords for extensions are secure. Make sure that **Password/PIN Policy** is enabled under **Security > Password Policy > Password/PIN Policy**, and that the password policy is applied to SIP users.

1. Go to **Security > Password Policy > Password Auditor**.
2. Review the list of extensions to see whether their password and PIN strengths meet the password policy requirements.

Intrusion detection

Intrusion detection lets you manually add IPs to be exempted from being blocked, remove system added exempt IPs if you find them suspicious, and configure intrusion detection settings.

1. Go to **Security > Intrusion Detection > Setting** and set **Status** to **Enable**.



Softclient

With the FortiFone softclient, you stay connected to the office, never missing an important call. You transform your mobile device into an extension connected to the FortiVoice phone system. The Fortinet business communications solution enables you to manage calls, check voicemail messages, and quickly view the company directory.

This section includes the following topics:

- Deployment of FortiFone softclient for mobile on page 105
- Deployment of FortiFone softclient for desktop on page 129

Deployment procedures use FortiGate as an example firewall. If your deployment does not use FortiGate, then follow the instructions provided by the firewall manufacturer.

Deployment of FortiFone softclient for mobile

In a typical deployment scenario, the FortiVoice phone system is located behind an internet facing firewall. If a customer has deployed a FortiFone softclient, this softclient is usually behind another firewall when the customer's cell phone is using the data service of a cellular network or the Wi-Fi of a home network. Signaling and two-way audio through a firewall requires the network address translation (NAT) traversal for the session initiation protocol (SIP). When the deployment is using either SIP over the transmission control protocol (TCP) or the user datagram protocol (UDP), the SIP application layer gateway (ALG) with hosted NAT traversal enabled on FortiGate can translate the internal IP address of a session description protocol (SDP) payload properly to allow media flow. If the deployment is using SIP over transport layer security (TLS), the SIP traffic is encrypted end-to-end. With this encryption, FortiGate is unable to translate the internal IP address in the SDP payload, which then causes a one-way audio or no audio at all. Fortunately, FortiGate supports SSL inspection and is able to decrypt the encrypted SIP traffic and translate the SDP address to resolve the NAT-traversal issue.

This section describes how to configure the FortiVoice phone system and FortiGate to use the FortiFone softclient as a remote SIP client, and install and configure the FortiFone softclient.

Protocols

The communication between the FortiFone softclient and FortiVoice uses the following protocols and server:

- HTTPS for softclient login, auto-provisioning, download of contacts, call logs, and voicemails
- SIP for signaling
- RTP or secure RTP (SRTP) for audio
- Android and iOS push server for outbound calls

Call flows

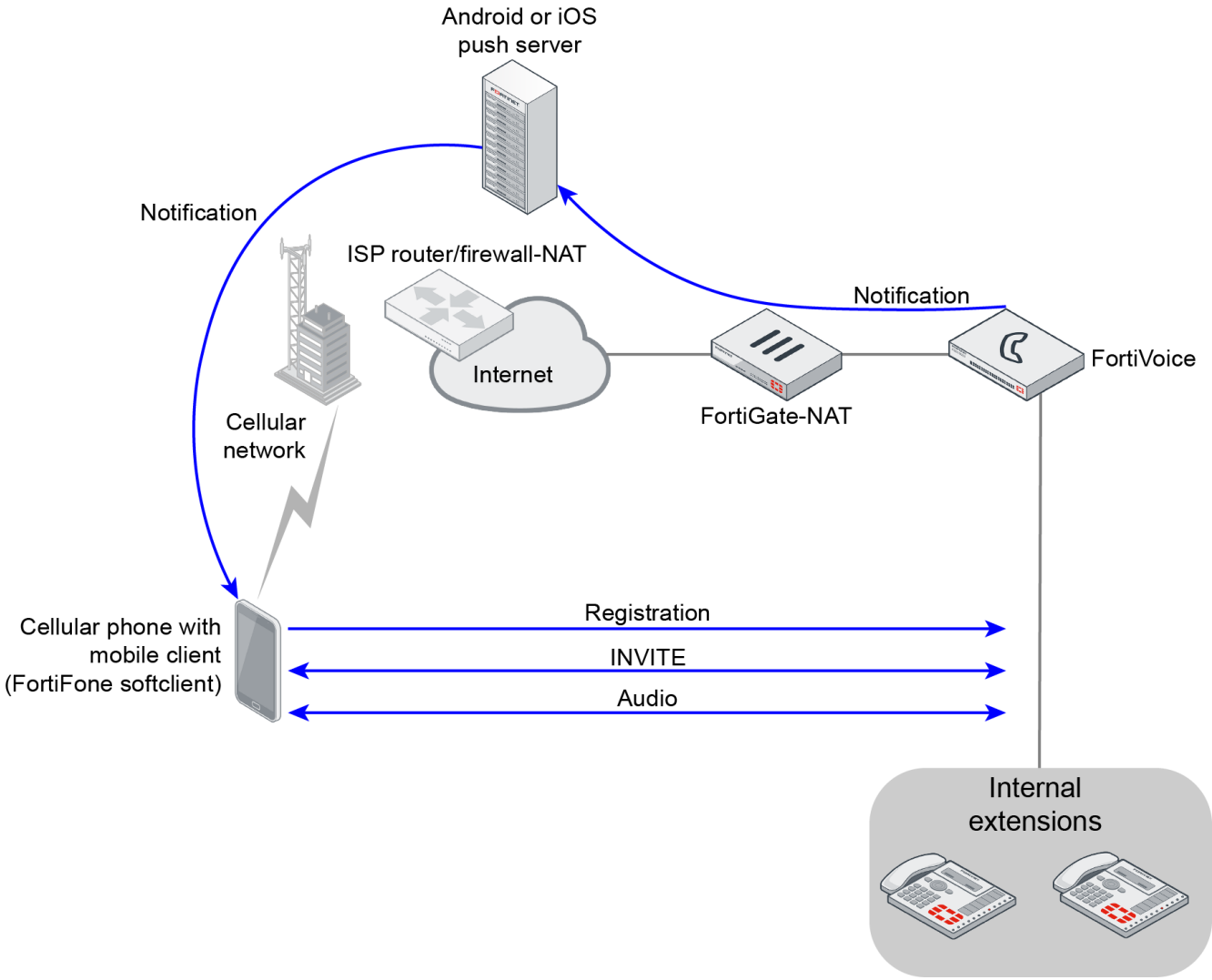
The inbound call flow includes the following steps:

1. A caller dials an extension to connect to the FortiFone softclient.
2. FortiVoice sends the push request to the Android or iOS push server which relays the request to the mobile client (cellular phone).
3. If the mobile client is in sleep mode, the request wakes up the mobile client.
4. The FortiFone softclient registers with FortiVoice and then receives the inbound call.
5. After the signaling is complete, FortiVoice sends the audio to the mobile client using RTP or SRTP.

The outbound call flow includes the following steps:

1. The user initiates an outbound call using the mobile client.
2. The FortiFone softclient sends a SIP invite directly to FortiVoice.
3. After the signaling is complete, FortiVoice sends the audio to the destination phone using RTP or SRTP.

Topology



Workflow for deployment using SIP over TLS

For a deployment with FortiFone softclient for mobile that uses SIP over TLS, perform the following tasks:

1. Configuring FortiFone softclient for mobile on FortiVoice on page 108
2. Configuring FortiGate for SIP over TLS on page 113
3. Installing and configuring the FortiFone softclient for mobile on page 128

Workflow for deployment using SIP over TCP or UDP

For a deployment with FortiFone softclient for mobile that uses SIP over TCP or UDP, perform the following tasks:

1. Configuring FortiFone softclient for mobile on FortiVoice on page 108
2. Configuring FortiGate for SIP over TCP or UDP on page 121

3. Installing and configuring the FortiFone softclient for mobile on page 128

Configuring FortiFone softclient for mobile on FortiVoice

Perform the following procedures to configure FortiFone softclient for mobile settings on the FortiVoice phone system:

- Load the FortiFone softclient license on FortiVoice on page 108
- Configure external access settings on page 108
- Configure a SIP profile on page 109
- Assign the FortiFone softclient to a FortiVoice extension on page 111
- Export the FortiVoice server certificate for SIP over TLS on page 112

Unless otherwise specified, steps in this FortiFone softclient section apply to SIP over TCP, UDP, and TLS.

Load the FortiFone softclient license on FortiVoice

Before you begin

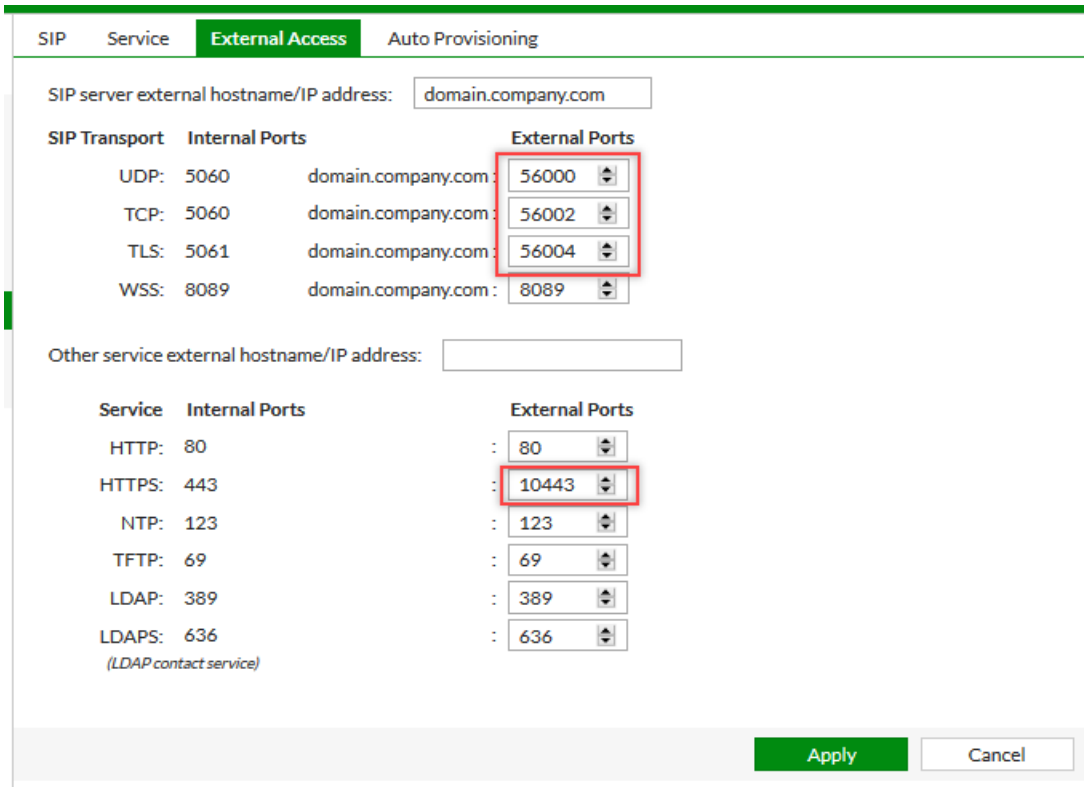
- Purchase and download a FortiFone softclient license. For details, see Licensing on page 71.

Procedure steps

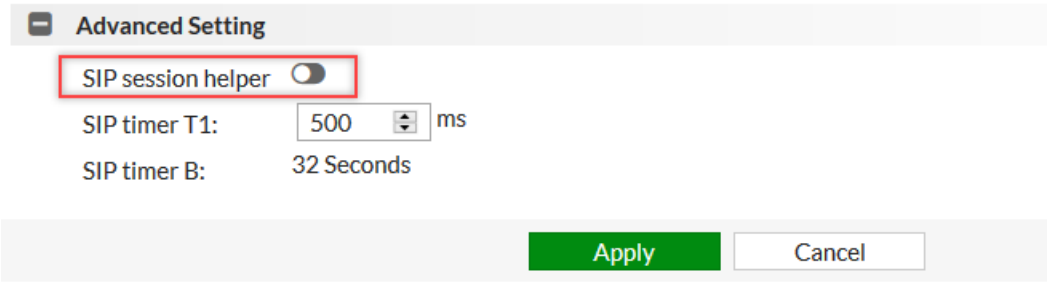
1. On FortiVoice, go to **Dashboard > Status**.
2. In the **License Information** widget, load the FortiVoice softclient license file to allow activation and registration of softclients on the system.

Configure external access settings

1. On FortiVoice, go to **System > Advanced > External Access**.
2. Set **SIP server external hostname/IP address** to the IP address or FQDN of the FortiVoice device and configure the following external access ports.



3. Go to **System > Advanced > SIP**.
4. Under **Advanced Setting**, make sure that **SIP session helper** is disabled.



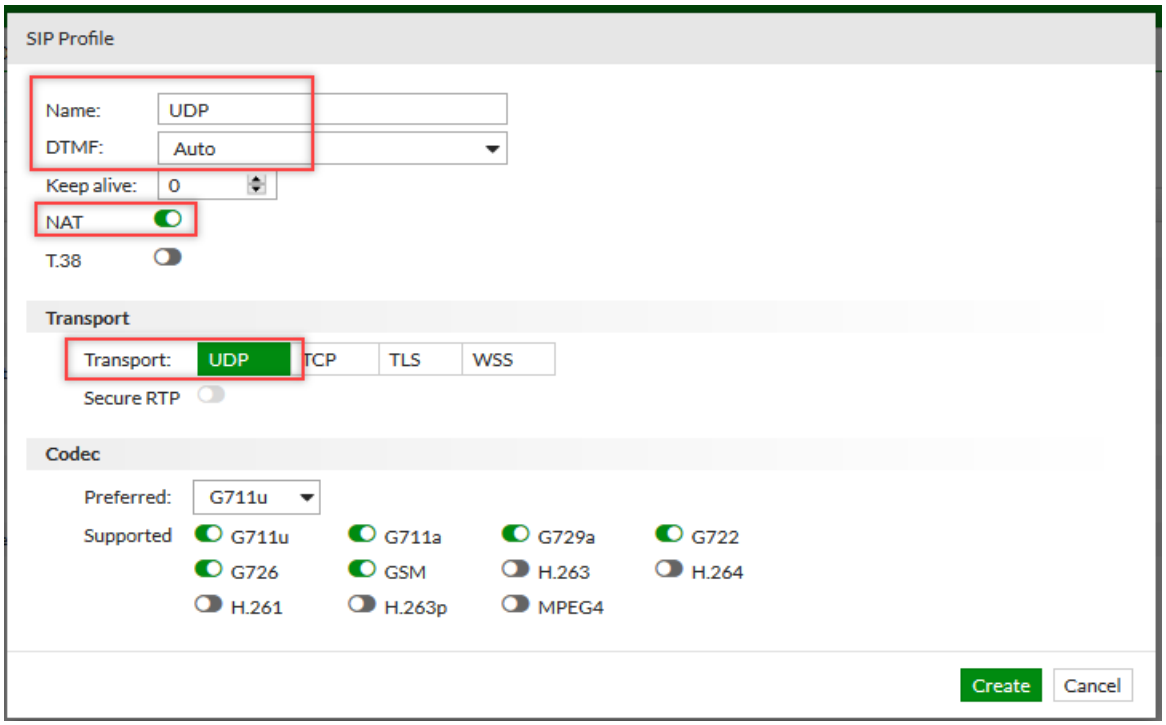
Configure a SIP profile

Perform this procedure to create a new SIP profile.

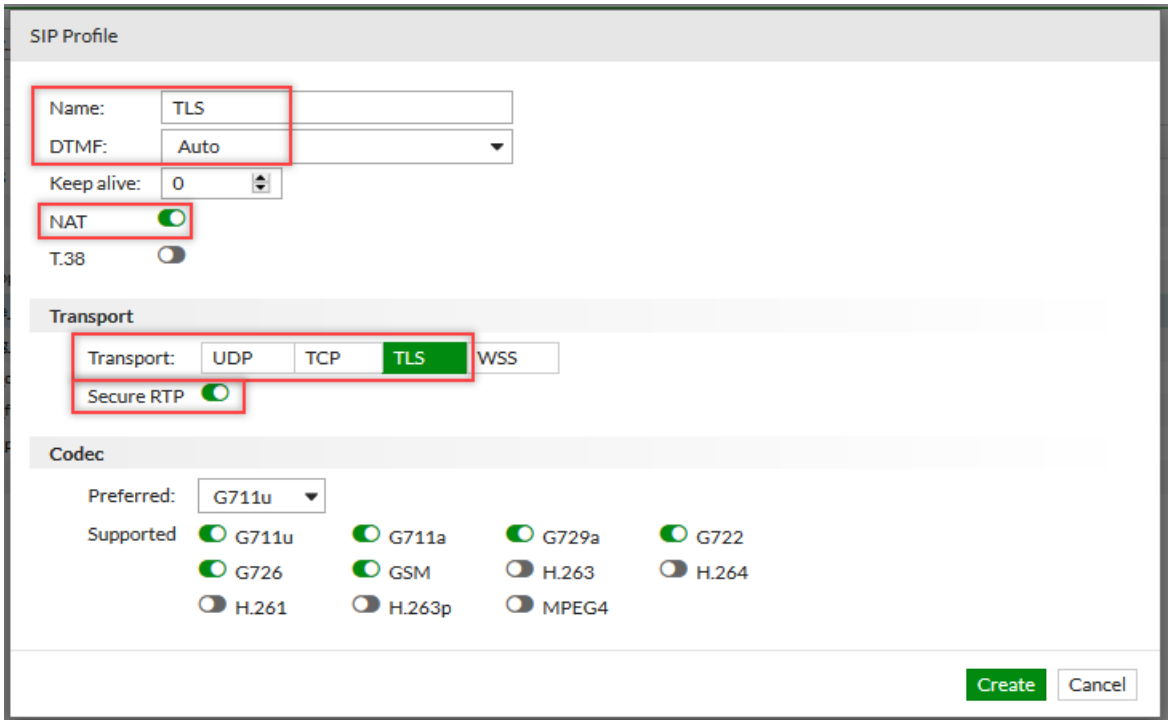
The default SIP profile (sip_mobile_default) is set for SIP over TCP. If you want, you can update this profile to set it to the protocol used by your deployment.

1. On FortiVoice, go to **Phone System > Profile > SIP**.
2. Click **New**.
3. In **Name**, enter a name for this SIP profile.
4. In **DTMF**, select **Auto**.
5. Enable **NAT**.
6. In **Transport**, select the protocol. If you set **Transport** to **TLS**, enable **Secure RTP**.

7. Click **Create**.
   Example for configuring a SIP profile for UDP:

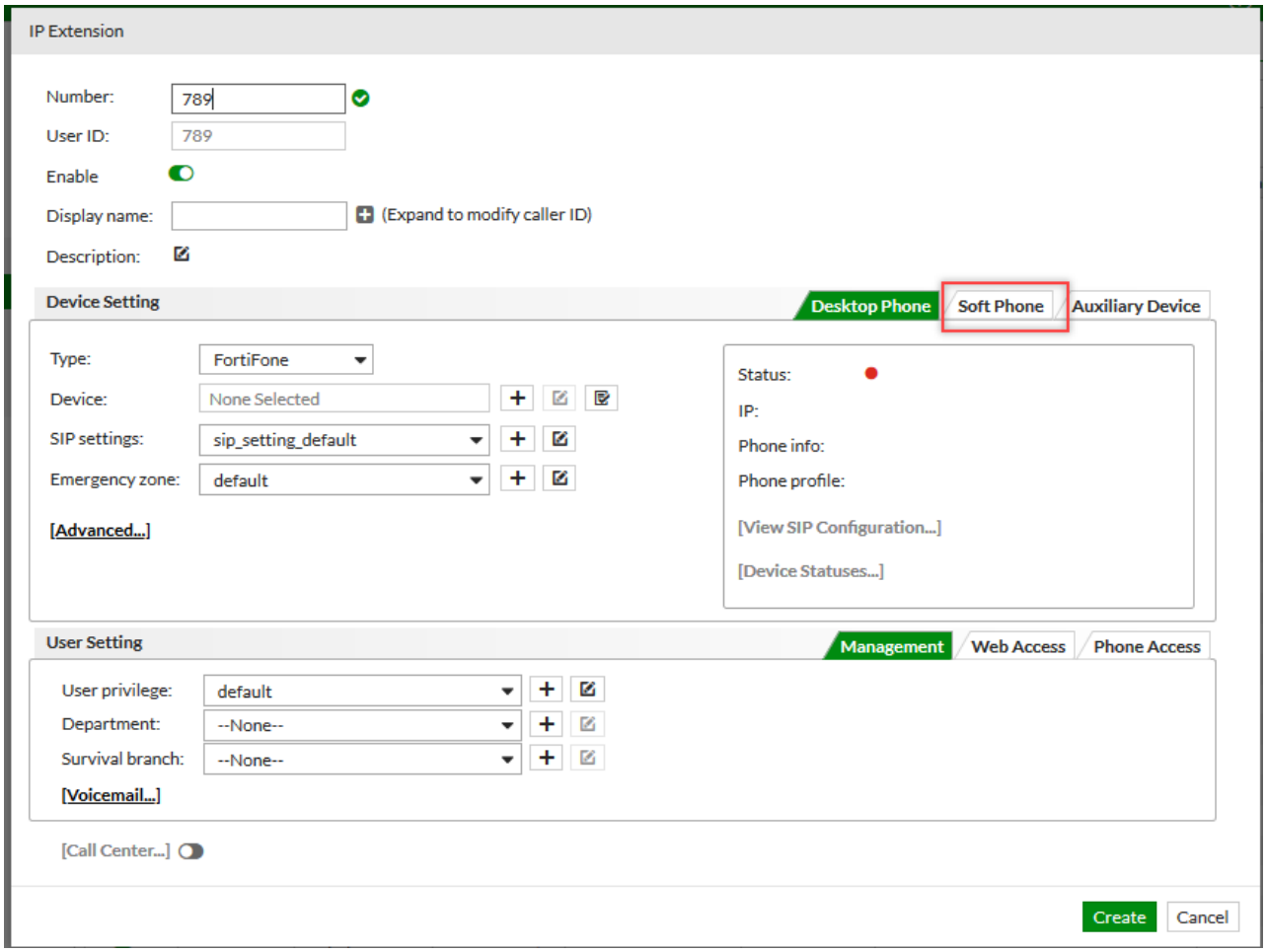


   Example for configuring a SIP profile for TLS:

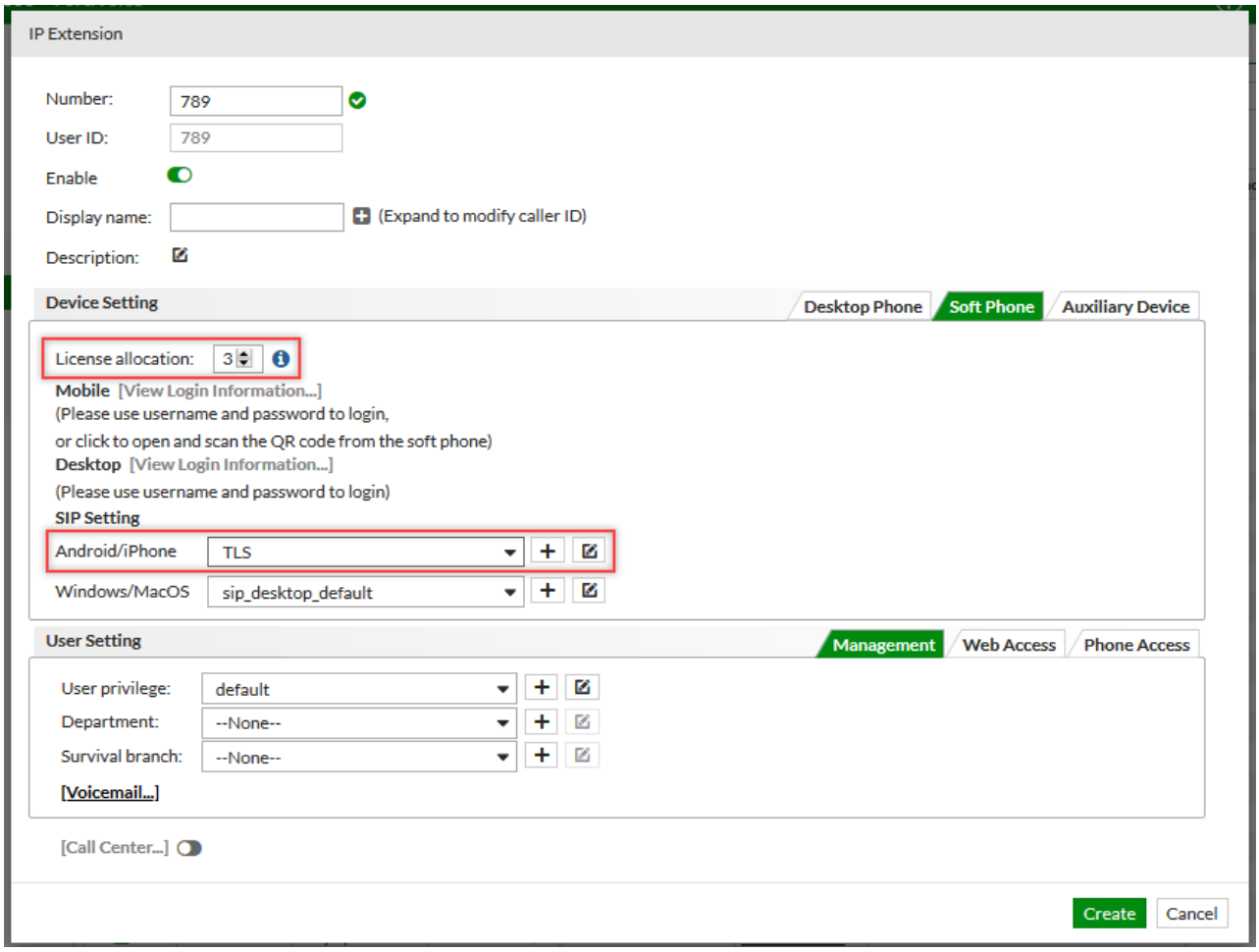


Assign the FortiFone softclient to a FortiVoice extension

1. On FortiVoice, go to **Extension > Extension > IP Extension** and click **New**.
2. Enter a **Number**.
3. Under **Device Setting**, click the **Soft Phone** tab.



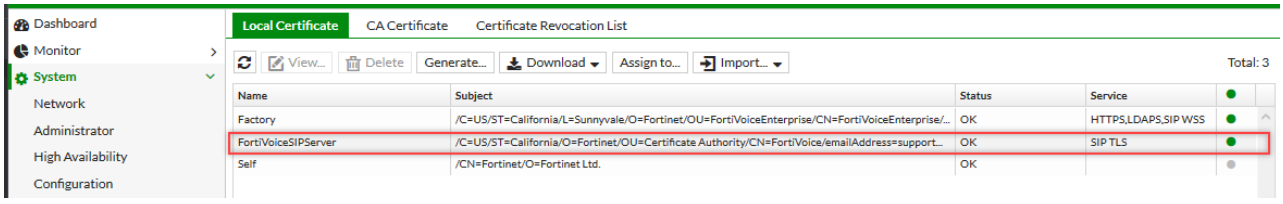
4. In **License allocation**, specify the value to configure.
5. In **Android/iPhone**, select a default profile or the profile that you configured in Configure a SIP profile on page 109.



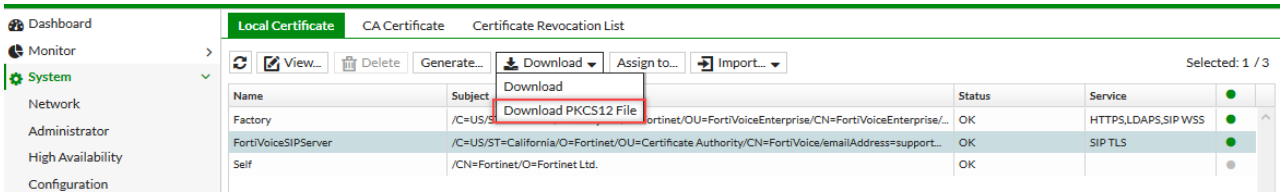
6. Click **Create**.
7. If your deployment uses SIP over TLS, go to Export the FortiVoice server certificate for SIP over TLS on page 112.
   If your deployment uses SIP over TCP or UDP, go to Configuring FortiGate for SIP over TCP or UDP on page 121.

Export the FortiVoice server certificate for SIP over TLS

1. On FortiVoice, go to **System > Certificate > Local Certificate**.
2. In the list, select **FortiVoiceSIPServer**. This is the default certificate for the SIP service. If you are using a custom certificate, select that one instead of the default.



3. Click **Download** and select **Download PKCS12 File**.



   The PKCS12 Certificate Download dialog opens.
4. In **Password** and **Confirm password**, enter a password to encrypt the key.
5. To download the file, click **OK**.
6. To save the file locally, click **OK**.
7. Take note of the location where you save the file.
8. Go to Configuring FortiGate for SIP over TLS on page 113.

Configuring FortiGate for SIP over TLS

After Configuring FortiFone softclient for mobile on FortiVoice on page 108, perform the following procedures to configure a FortiGate device for SIP over TLS:

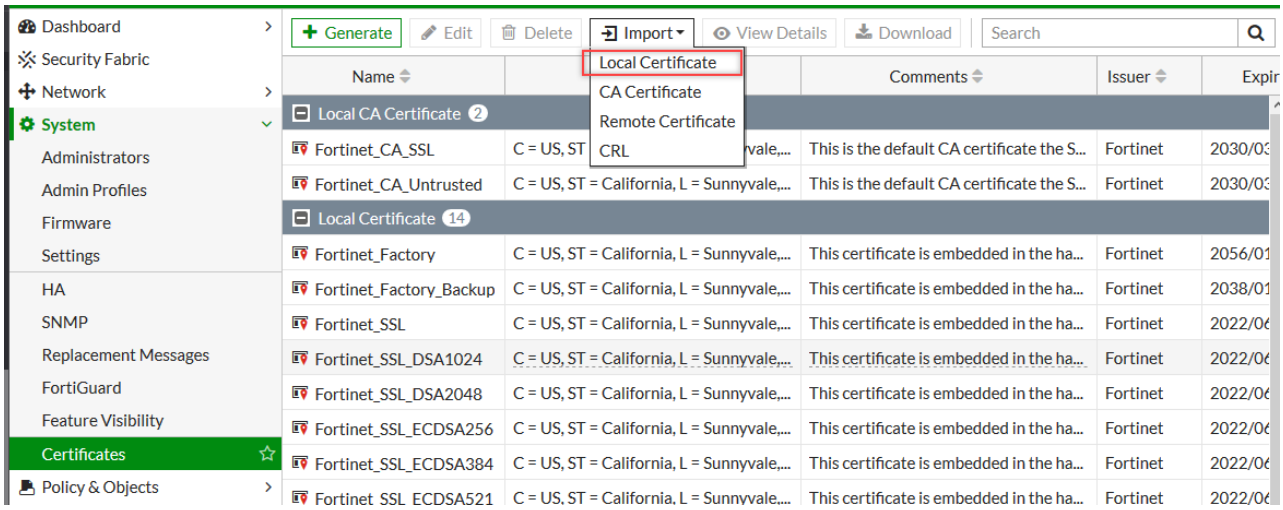
- Import the downloaded FortiVoice server certificate for SIP over TLS on page 113
- Configure system settings for SIP over TLS on page 115
- Create virtual IP addresses for SIP over TLS on page 115
- Configure VoIP profile and NAT traversal settings for SIP over TLS on page 118
- Create an inbound firewall policy for SIP over TLS on page 119
- Create an outbound firewall policy for FortiVoice to access the Android or iOS push server on page 120

If your FortiVoice deployment is using SIP over TCP or UDP instead, go to Configuring FortiGate for SIP over TCP or UDP on page 121.

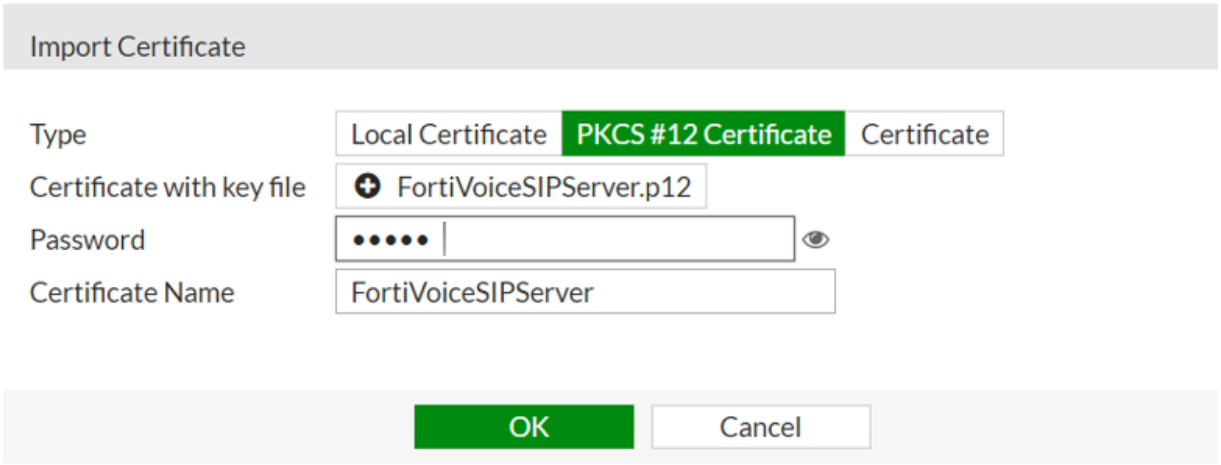
Import the downloaded FortiVoice server certificate for SIP over TLS

Perform the following steps to import the downloaded FortiVoice server certificate. The downloaded certificate is from Export the FortiVoice server certificate for SIP over TLS on page 112.

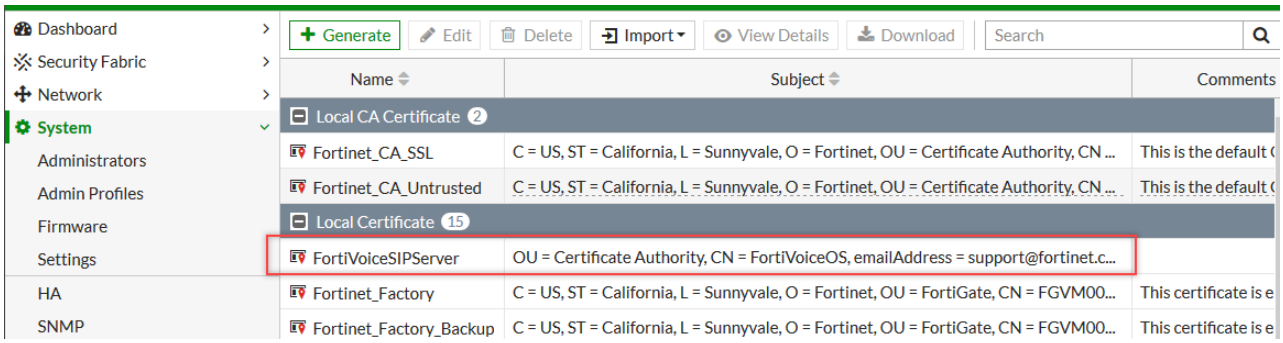
1. On FortiGate, go to **System > Certificates**.
2. Click **Import** and select **Local Certificate**.



3. Update the following fields in the Import Certificate dialog:
   a. In **Type**, click **PKCS #12 Certificate**.
   b. In **Certificate with key file**, click **Upload**.
   c. Locate the FortiVoice server certificate. This is the file from Export the FortiVoice server certificate for SIP over TLS on page 112.
   d. Click **Open**.
   e. In **Password**, enter the password associated with the FortiVoice server certificate.
   f. Click **OK**.

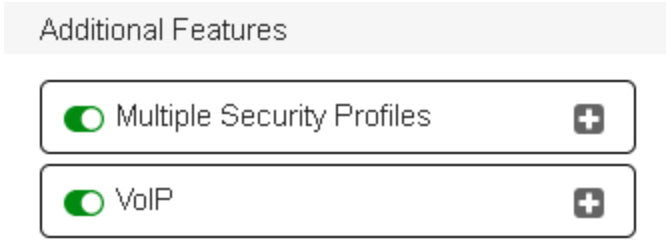


4. Verify that the list of certificates now includes the newly imported FortiVoice server certificate.



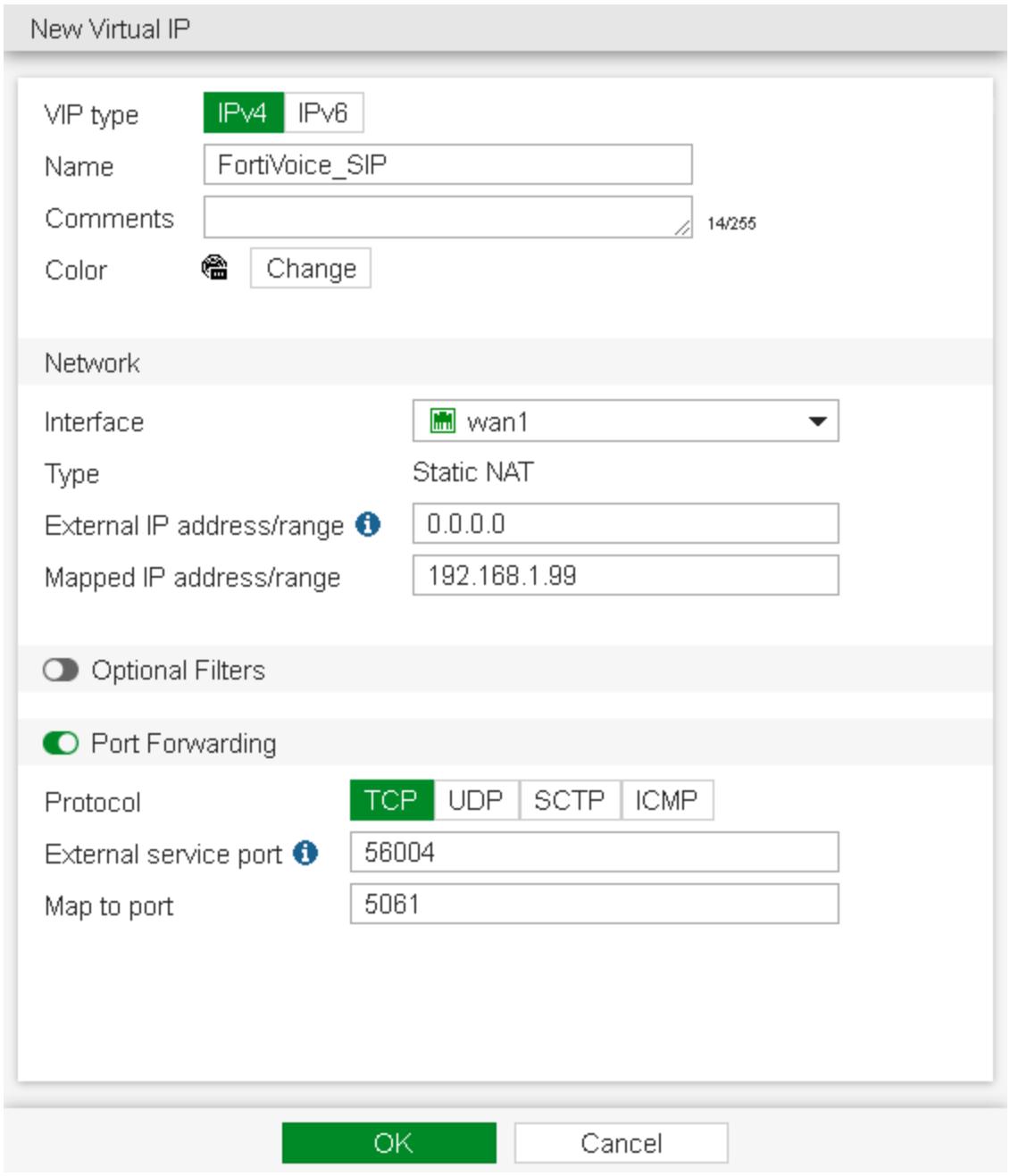
Configure system settings for SIP over TLS

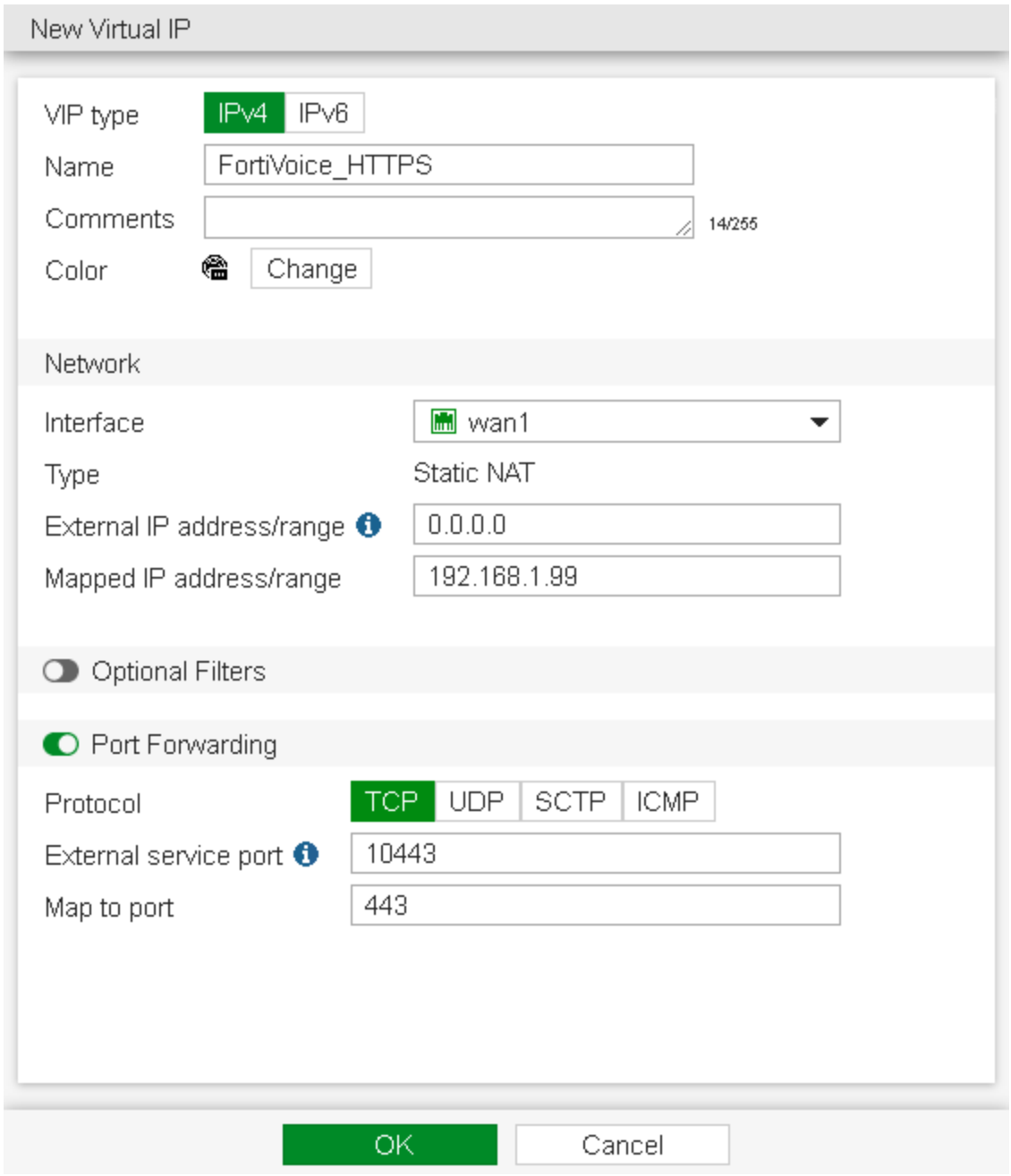
1. On FortiGate, go to **System > Feature Visibility**.
2. Under **Additional Features**, enable **Multiple Security Profiles** and **VoIP**.
3. Click **Apply**.



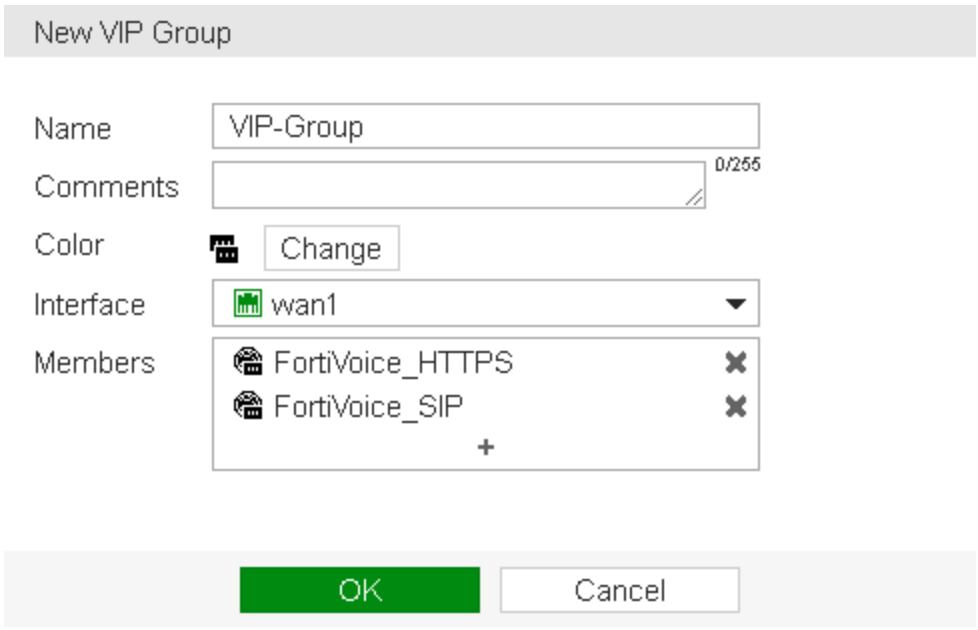
Create virtual IP addresses for SIP over TLS

1. On FortiGate, go to **Policy & Objects > Virtual IPs**.
2. Click **Create New** and select **Virtual IP**.
3. Create virtual IPs for the following services that map to the IP address of the FortiVoice:
   - External SIP TLS port of FortiVoice
   - External HTTPS port of FortiVoice. The HTTPS port is used for the softclient login, call logs, and contacts download from the FortiVoice phone system.


New Virtual IP
VIP type
IPv4
IPv6
Name
FortiVoice_SIP
Comments
14/255
Color
Change
Network
Interface
wan1
Type
Static NAT
External IP address/range
0.0.0.0
Mapped IP address/range
192.168.1.99
Optional Filters
Port Forwarding
Protocol
TCP
UDP
SCTP
ICMP
External service port
56004
Map to port
5061
OK
Cancel



4. To create a virtual IP group, click **Create New** and select **Virtual IP Group**.
5. Add the two newly created virtual IPs.



Configure VoIP profile and NAT traversal settings for SIP over TLS

1. On FortiGate, open the **CLI Console** from the GUI banner.
2. Create a VoIP protection profile and enable hosted NAT traversal (HNT) and restricted HNT source address. If the FortiVoice softclient is behind a non-SIP-aware firewall, HNT addresses the SDP local address problem. Enable SSL full inspection and refer to the imported FortiVoice server certificate for example, FortiVoiceSIPServer.
   This VoIP protection policy with hosted NAT traversal enabled will be added to the inbound firewall policy to prevent potential one way audio issues caused by NAT.

VoIP profile command example for SIP over TLS

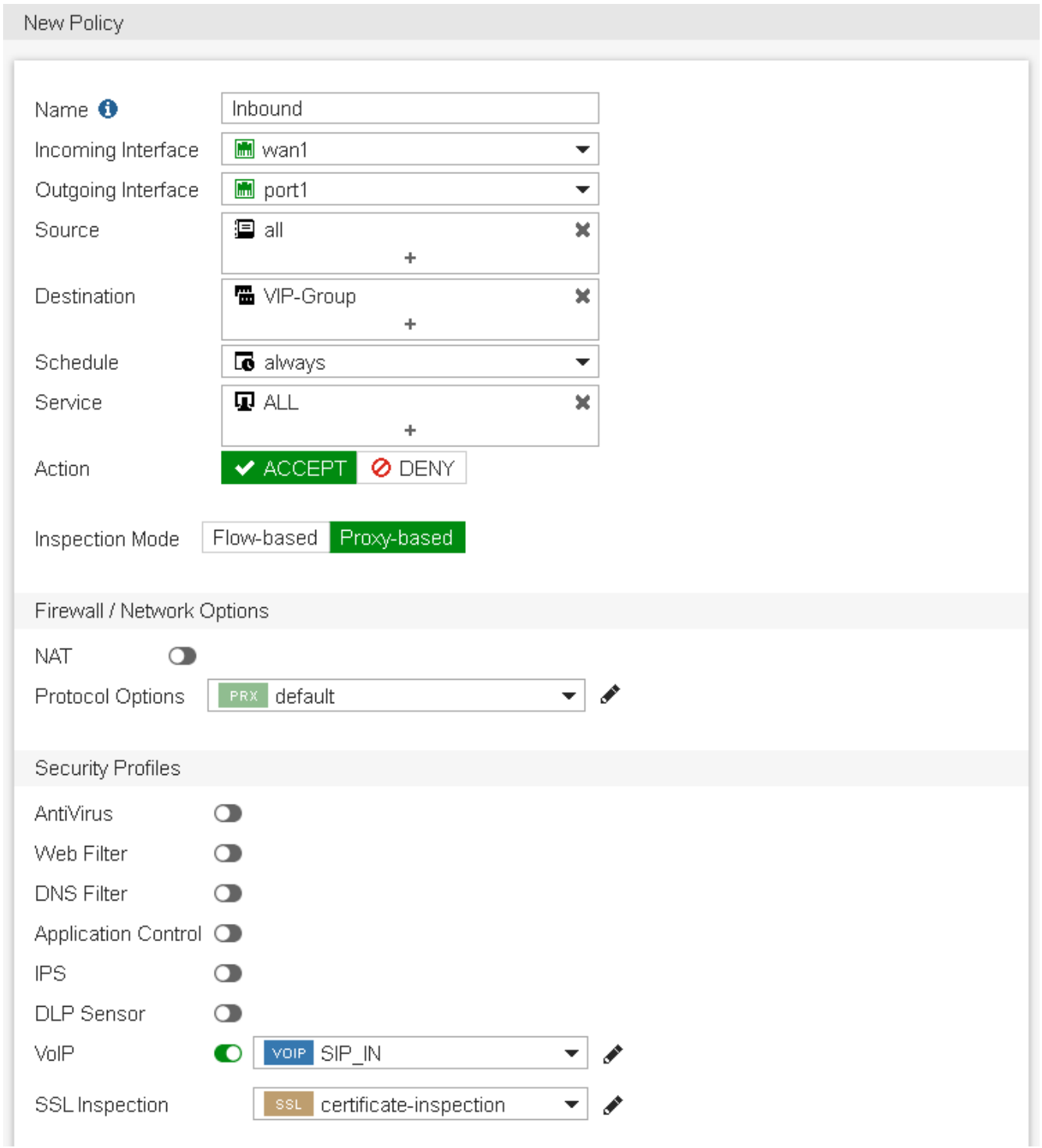
```
config voip profile
   edit "SIP_IN"
      config sip
         set hosted-nat-traversal enable
         set ssl-mode full
         set ssl-server-certificate "FortiVoiceSIPServer"
      end
   next
end
```

3. For SIP over TLS, the recommendation is to use the default SSL port for SIP (TCP 5061). Enter the following commands:
   ```
   config system settings
      set sip-tcp-port 5061
   end
   ```
4. Edit the FortiGate interface connecting to the internet and set it to external. The SIP application layer gateway (ALG) with hosted NAT traversal requires an external port to work. Enter the following commands:
   ```
   config system interface
      edit wan1
         set external enable
   ```

```
    next
end
```

Create an inbound firewall policy for SIP over TLS

1. On FortiGate, go to **Policy & Objects > Firewall Policy** and click **Create New**.
2. Set **Incoming Interface** to the internet-facing interface.
3. Set **Outgoing Interface** to the internal/LAN interface.
4. Set **Source** to **all**.
5. Set **Destination** to the virtual IP group created in Create virtual IP addresses for SIP over TLS on page 115.
6. Set **Schedule** to **always**.
7. Set **Service** to **ALL**.
8. Disable **NAT**.
9. Enable **VoIP** and select the VoIP profile created in Configure VoIP profile and NAT traversal settings for SIP over TLS on page 118.



Create an outbound firewall policy for FortiVoice to access the Android or iOS push server

FortiVoice requires outbound access to the Android and iOS push servers.

If FortiGate has an outbound firewall policy that allows FortiVoice to access everything on the internet, then you do not need to create an additional firewall policy. You have completed the FortiGate configuration for SIP over TLS. Go to Installing and configuring the FortiFone softclient for mobile on page 128.

If FortiGate does not have an outbound firewall policy that allows FortiVoice to access everything on the internet, perform the steps to create the FQDN addresses and the specific outbound firewall policies to allow FortiVoice to access the Android and iOS push servers.

To create FQDN addresses for Android and iOS push servers

1. On FortiGate, go to **Policy & Objects > Addresses** and click **Create New**.
2. In **Name**, enter a name for the Android push server address.
3. In **Type**, select **FQDN**.
4. In **FQDN**, enter **fcm.googleapis.com**.
5. Click **OK**.
6. Click **Create New**.
7. In **Name**, enter a name for the iOS push server address.
8. In **Type**, select **FQDN**.
9. In **FQDN**, enter **gateway.push.apple.com**.
10. Click **OK**.

To use the Android and iOS push server addresses in an outbound firewall policy

1. On FortiGate, go to **Policy & Objects > Firewall Policy** and click **Create New**.
2. In **Incoming interface**, enter the port connected to FortiVoice.
3. In **Outgoing interface**, enter the WAN port.
4. In **Source**, select **all**.
5. In **Destination**, select the FQDN addresses that you created for the Android and iOS push servers.
6. Configure the rest of the policy, as needed.
7. Click **OK**.
   You have completed the configuration of FortiGate for SIP over TLS.
8. Go to Installing and configuring the FortiFone softclient for mobile on page 128.

Configuring FortiGate for SIP over TCP or UDP

After Configuring FortiFone softclient for mobile on FortiVoice on page 108, perform the following procedures to configure a FortiGate device for SIP over TCP or UDP:

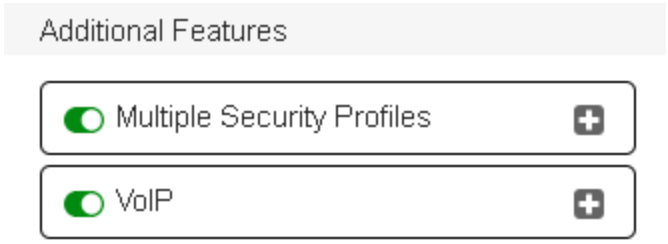
- Configure system settings for SIP over TCP or UDP on page 121
- Create virtual IP addresses for SIP over TCP or UDP on page 122
- Configure VoIP profile and NAT traversal settings for SIP over TCP or UDP on page 125
- Create an inbound firewall policy for SIP over TCP or UDP on page 126
- Create an outbound firewall policy for FortiVoice to access the Android or iOS push server on page 127

If your FortiVoice deployment is using SIP over TLS instead, go to Configuring FortiGate for SIP over TLS on page 113.

Configure system settings for SIP over TCP or UDP

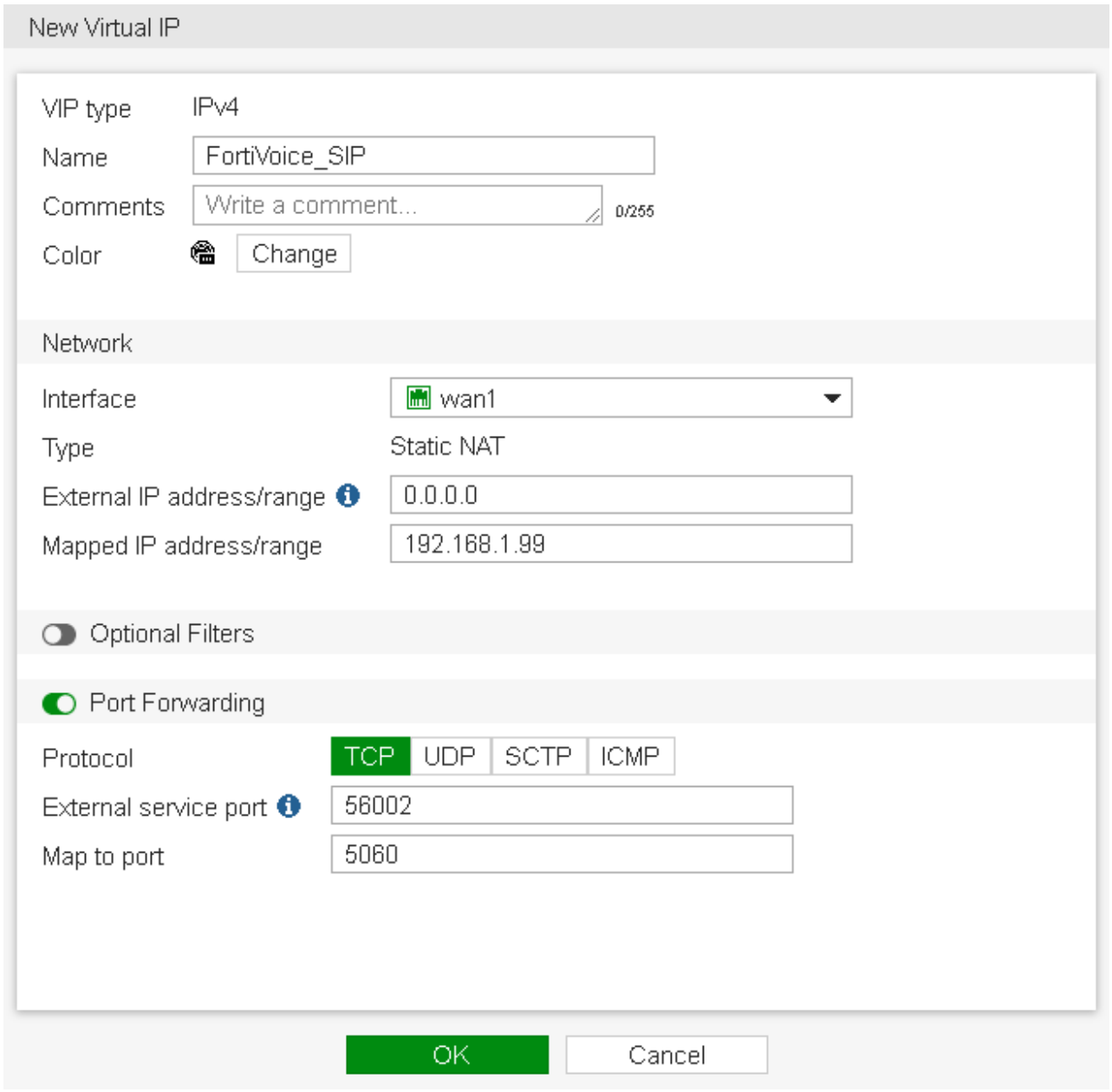
1. On FortiGate, go to **System > Feature Visibility**.
2. Under **Additional Features**, enable **Multiple Security Profiles** and **VoIP**.

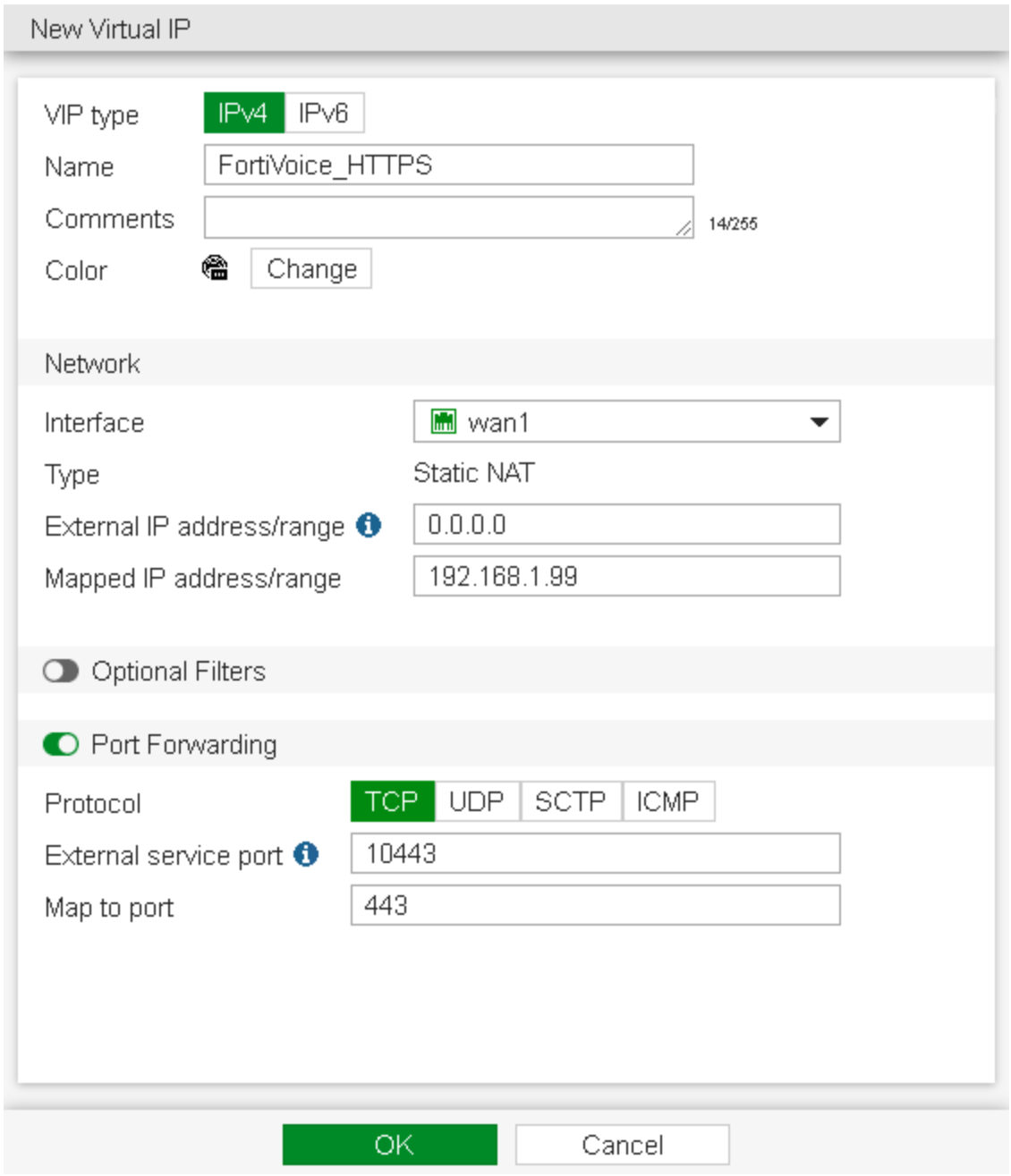
3. Click **Apply**.



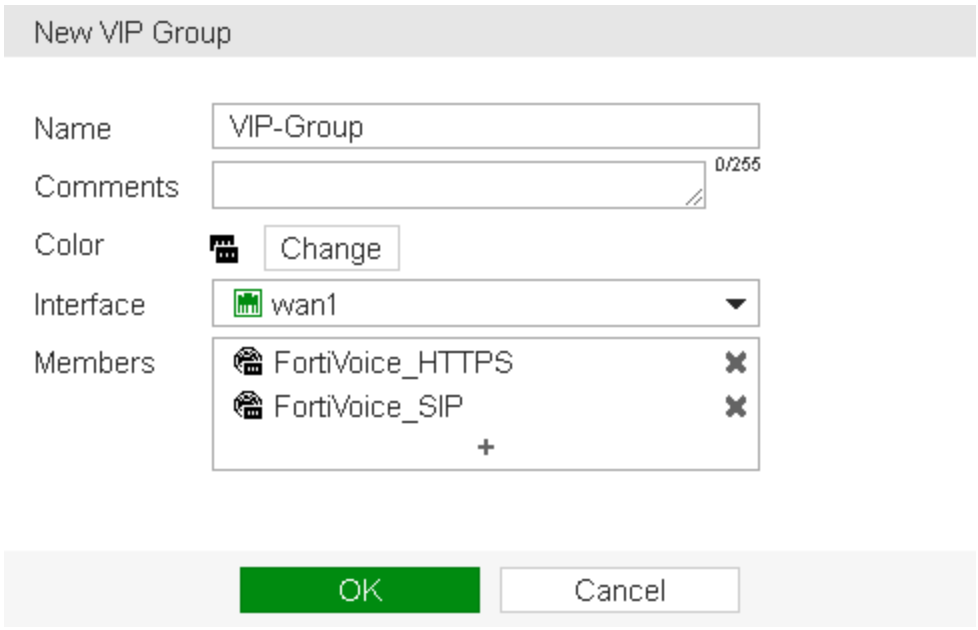
Create virtual IP addresses for SIP over TCP or UDP

1. On FortiGate, go to **Policy & Objects > Virtual IPs**.
2. Click **Create New** and select **Virtual IP**.
3. Create virtual IPs for the following services that map to the IP address of the FortiVoice:
   - External SIP TCP port of FortiVoice. If the **sip_mobile_default** profile has been modified to use UDP instead, configure the VIP for the external SIP UDP port.
   - External HTTPS port of FortiVoice. The HTTPS port is used for the softclient login, call logs, and contacts download from the FortiVoice phone system.


New Virtual IP
VIP type
IPv4
Name
FortiVoice_SIP
Comments
Write a comment...
0/255
Color
Change
Network
Interface
wan1
Type
Static NAT
External IP address/range
0.0.0.0
Mapped IP address/range
192.168.1.99
Optional Filters
Port Forwarding
Protocol
TCP
UDP
SCTP
ICMP
External service port
56002
Map to port
5060
OK
Cancel



4. To create a virtual IP group, click **Create New** and select **Virtual IP Group**.
5. Add the two newly created virtual IPs.



Configure VoIP profile and NAT traversal settings for SIP over TCP or UDP

1. On FortiGate, open the **CLI Console** from the GUI banner.
2. Create a VoIP protection profile and enable hosted NAT traversal (HNT) and restricted HNT source address. If the FortiVoice softclient is behind a non-SIP-aware firewall, HNT addresses the SDP local address problem.
   This VoIP protection profile will be added to the inbound firewall policy to prevent potential one-way audio issues caused by NAT.

   VoIP profile command example for SIP over TCP or UDP

   ```
   config voip profile
      edit "SIP_IN"
         config sip
            set hosted-nat-traversal enable
         end
      next
   end
   ```
3. If you are using a non-standard external port, update the system settings by entering the following commands. Both command examples use port 5566.

   External port setting example for TCP

   ```
   config system settings
      set sip-tcp-port 5566
   end
   ```

   External port setting example for UDP

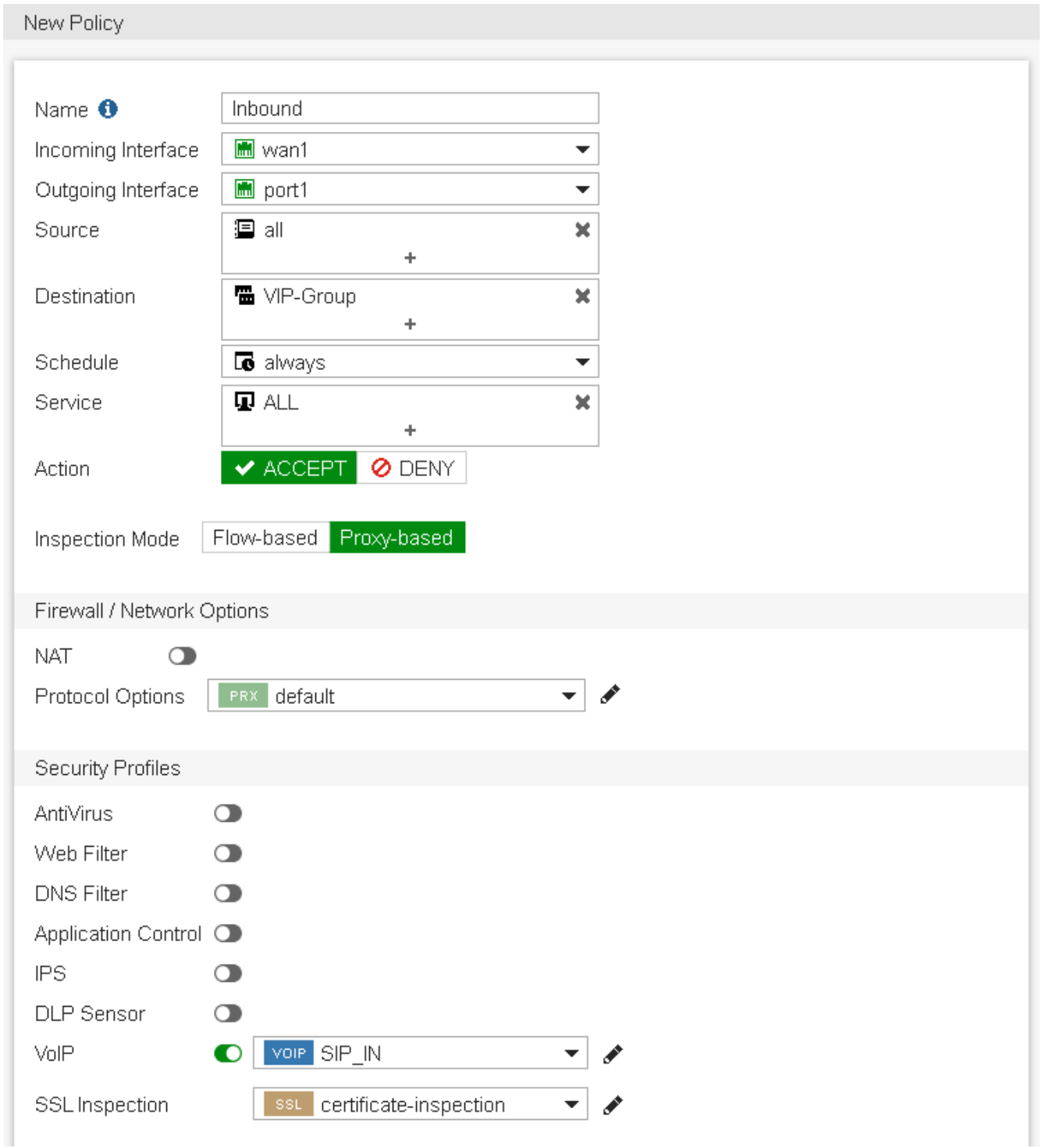
   ```
   config system settings
      set sip-udp-port 5566
   end
   ```
4. Set the internet facing interface as external. HNT requires an external port to work. The command example uses port2 as the internet facing interface.

   ```
   config system interface
      edit "wan1"
         set external enable
      next
   ```

```
end
```

Create an inbound firewall policy for SIP over TCP or UDP

1. On FortiGate, go to **Policy & Objects > Firewall Policy**.
2. Click **Create New**.
3. Set **Incoming Interface** to the internet-facing interface and **Outgoing Interface** to the internal/LAN interface.
4. Set **Source** to **all**.
5. Set **Destination** to the virtual IP group created in Create virtual IP addresses for SIP over TCP or UDP on page 122.
6. Set **Schedule** to **always**.
7. Set **Service** to **ALL**.
8. Disable **NAT**.
9. Enable **VoIP** and select the VoIP profile created in Configure VoIP profile and NAT traversal settings for SIP over TCP or UDP on page 125.



Create an outbound firewall policy for FortiVoice to access the Android or iOS push server

FortiVoice requires outbound access to the Android and iOS push servers.

If FortiGate has an outbound firewall policy that allows FortiVoice to access everything on the internet, then you do not need to create an additional firewall policy. You have completed the FortiGate configuration for SIP over TLS. Go to Installing and configuring the FortiFone softclient for mobile on page 128.

If FortiGate does not have an outbound firewall policy that allows FortiVoice to access everything on the internet, perform the steps to create the FQDN addresses and the specific outbound firewall policies to allow FortiVoice to access the Android and iOS push servers.

To create FQDN addresses for Android and iOS push servers

1. On FortiGate, go to **Policy & Objects > Addresses** and click **Create New**.
2. In **Name**, enter a name for the Android push server address.
3. In **Type**, select **FQDN**.
4. In **FQDN**, enter **fcm.googleapis.com**.
5. Click **OK**.
6. Click **Create New**.
7. In **Name**, enter a name for the iOS push server address.
8. In **Type**, select **FQDN**.
9. In **FQDN**, enter **gateway.push.apple.com**.
10. Click **OK**.

To use the Android and iOS push server addresses in an outbound firewall policy

1. On FortiGate, go to **Policy & Objects > Firewall Policy** and click **Create New**.
2. In **Incoming interface**, enter the port connected to FortiVoice.
3. In **Outgoing interface**, enter the WAN port.
4. In **Source**, select **all**.
5. In **Destination**, select the FQDN addresses that you created for the Android and iOS push servers.
6. Configure the rest of the policy, as needed.
7. Click **OK**.
   You have completed the configuration of FortiGate for SIP over TCP or UDP.
8. Go to Installing and configuring the FortiFone softclient for mobile on page 128.

Installing and configuring the FortiFone softclient for mobile

With the FortiFone softclient for mobile, you stay connected to the office, never missing an important call. You transform your mobile device into an extension connected to the FortiVoice phone system. Fortinet's business communications solution enables you to manage calls, check voicemail messages and quickly view the company directory.

For details about installing, configuring, and using the FortiFone softclient for Android or iOS, see the FortiFone Softclient User Guide (Android or iOS).

Deployment of FortiFone softclient for desktop

FortiFone softclient for desktop is a secure application designed to transform your computer into an extension on the FortiVoice phone system. Through the intuitive interface, you can conveniently take control of your calls without shifting focus away from your screen. Using the FortiFone softclient for desktop in conjunction with a desk phone allows you to manage calls, check voicemail, and quickly view the company directory.

This section describes how to configure the FortiVoice phone system to use the FortiFone softclient for desktop, and install and configure the FortiFone softclient.

Protocols

The communication between the FortiFone softclient for desktop and the FortiVoice phone system uses the following protocols:

- WSS (TCP) for signaling
- DTLS (UDP) for audio

Call flows

The inbound call flow includes the following steps:

1. The FortiFone softclient for desktop logs in and registers with FortiVoice.
2. A caller dials an extension to connect to the FortiFone softclient for desktop.
3. FortiVoice sends an Invite message to the FortiFone softclient for desktop to initiate the call.
4. When the user of the FortiFone softclient for desktop accepts the call, the signaling will be complete, and FortiVoice transmits the audio using DTLS.

The outbound call flow includes the following steps:

1. The user initiates an outbound call using the FortiFone softclient for desktop.
2. The FortiFone softclient for desktop sends an Invite message to FortiVoice. FortiVoice attempts to make the outbound call.
3. After the signaling is complete and the call is established, the audio is transmitted between FortiVoice and the FortiFone softclient for desktop using DTLS.

Workflow

For a deployment with FortiFone softclient for desktop, perform the following tasks:

1. Configuring FortiFone softclient for desktop settings on FortiVoice on page 130
2. Configuring the ICE support on page 133
3. Creating virtual IP addresses on FortiGate on page 134
4. Configuring a FortiGate firewall policy for port forwarding on page 137
5. Installing and configuring the FortiFone softclient for desktop on page 139

Configuring FortiFone softclient for desktop settings on FortiVoice

Perform the following procedures to configure FortiFone softclient for desktop settings on the FortiVoice phone system:

- Load the FortiFone softclient license on FortiVoice on page 130
- Configure external access settings on page 130
- Configure a SIP profile on page 131
- Assign the FortiFone softclient for desktop to a FortiVoice extension on page 132

Load the FortiFone softclient license on FortiVoice

Before you begin

- Purchase and download a FortiFone softclient license. For details, see Licensing on page 71.

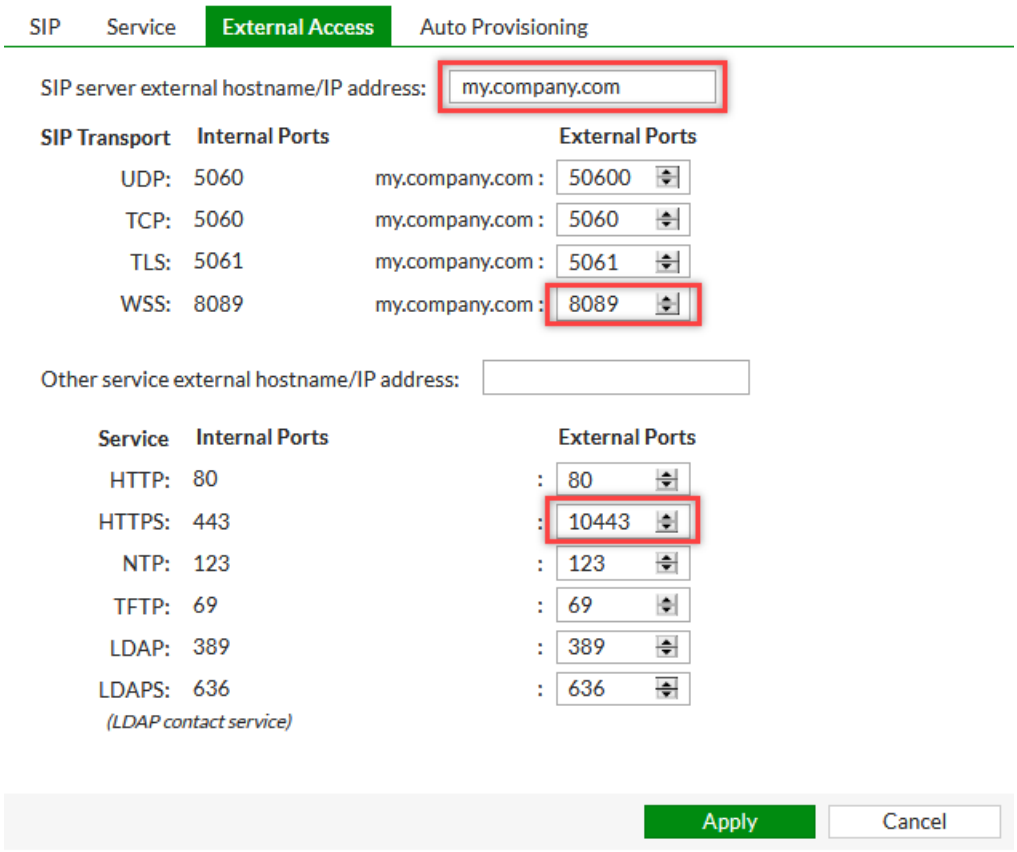
Procedure steps

1. On FortiVoice, go to **Dashboard > Status**.
2. In the **License Information** widget, load the FortiVoice softclient license file to allow activation and registration of softclients on the system.

Configure external access settings

1. On FortiVoice, go to **System > Advanced > External Access**.
2. Set **SIP server external hostname/IP address** to the IP address or FQDN of the FortiVoice unit.

3. Configure the WSS and HTTPS external access ports.



4. Click **Apply**.

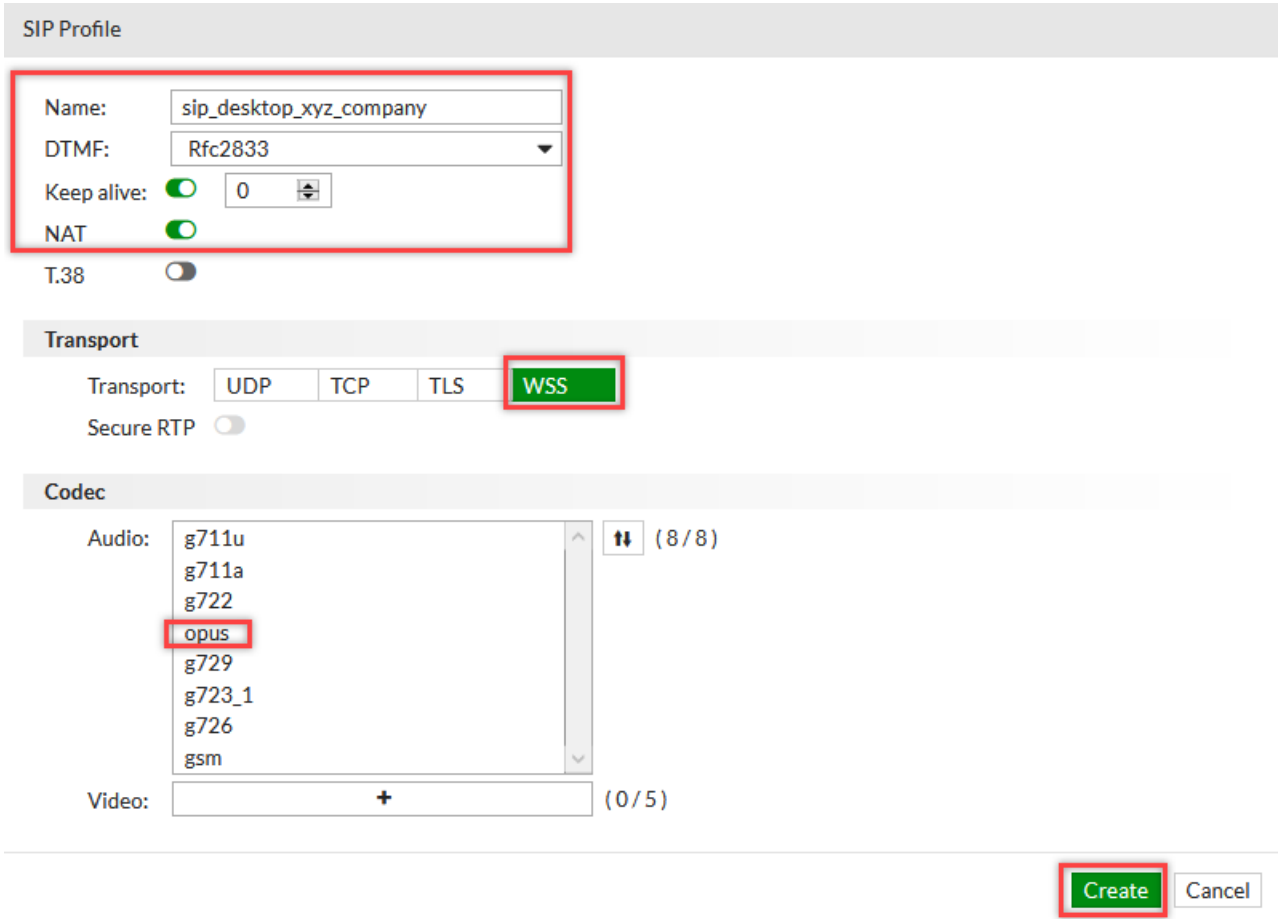
Configure a SIP profile

Fortinet recommends that you use the default SIP profile (sip_desktop_default).

However, if you want to create your own SIP profile, then perform the following steps to set the parameters for your deployment:

1. On FortiVoice, go to **Phone System > Profile > SIP**.
2. Click **New > Desktop**.
3. In **Name**, enter a name for this SIP profile.
4. In **DTMF**, select **RFC2833**.
5. In **Keep alive**, select 0.
6. Enable **NAT**.
7. Set **Transport** to **WSS**.

8. In **Codec**, make sure that **opus** is in the list.



9. Click **Create**.

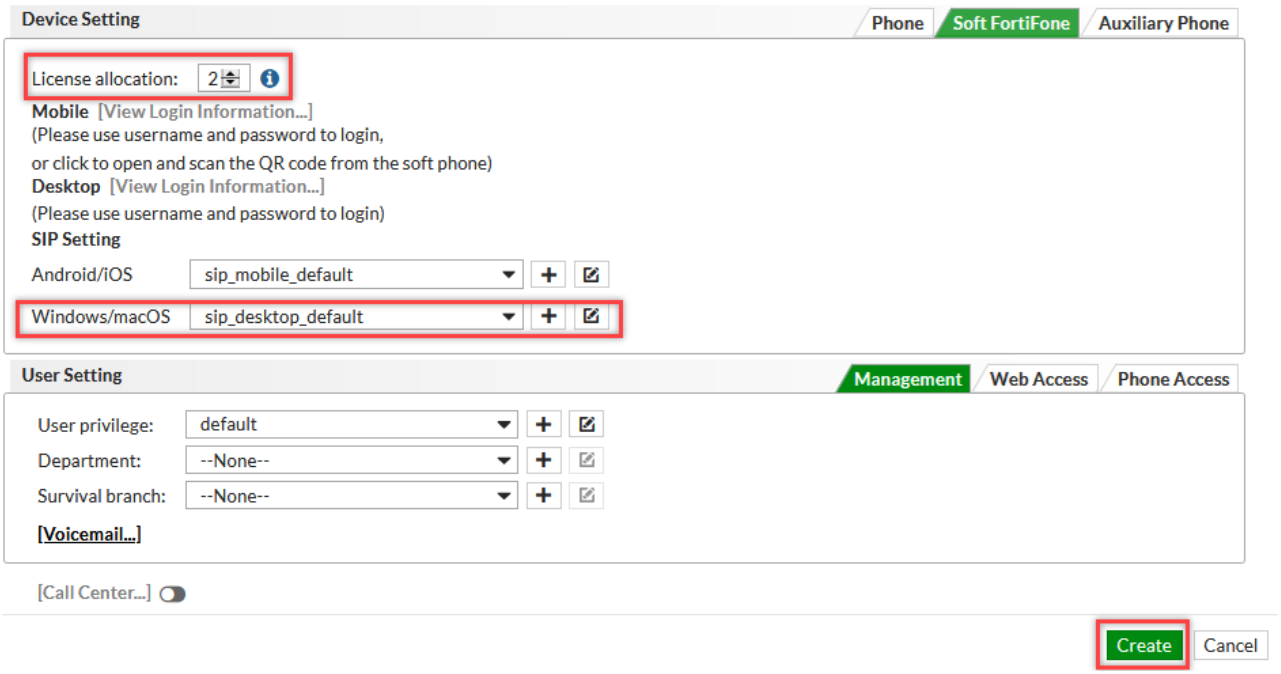
Assign the FortiFone softclient for desktop to a FortiVoice extension

1. On FortiVoice, go to **Extension > Extension > IP Extension** and click **New**.
2. Enter a **Number** for the extension.
3. Under **Device Setting**, click the **Soft FortiFone** tab.

4. In **License allocation**, specify the value to configure. In this example, the value is 2. One license allocation is for the desktop (Windows/macOS) and the other is for the mobile (Android/iOS) that you can deploy later.

After you complete the installation of the FortiFone softclient, the **Soft FortiFone** tab lists the device. From this tab, you can also revoke a license occupied by an inactive or unused device, if applicable.

5. In **Windows/macOS**, keep the default profile or select the profile that you configured in Configure a SIP profile on page 131.



6. Click **Create**.

Configuring the ICE support

When the FortiFone softclient is located behind a Network Address Translator (NAT) or FortiFone softclients are on different networks (without internetwork routing), configure the interactive connectivity establishment (ICE) support to allow the FortiVoice phone system to establish a valid audio path with the FortiFone softclient.

To configure the ICE support, you have the following two options:

- **Static mapping**: Uses the internal and external IP addresses of the FortiVoice phone system.
- **STUN server**: Uses the IP address of a Session Traversal Utilities for NAT (STUN) server.

Decide which option you want to configure for ICE support.

To configure the static mapping for ICE support

1. To connect to the FortiVoice CLI, go to **Dashboard > Console** and click inside the window.
2. Enter the following commands and replace xxx.xxx.xxx.xxx with the internal and external FortiVoice IP addresses used in your deployment:
```
config system sip-setting
set ice-support static-mapping
   config ice-ip-mapping
      edit 1
         set status enable
         set internal-ipaddr xxx.xxx.xxx.xxx
         set external-ipaddr xxx.xxx.xxx.xxx
      next
   end
```
3. Reload the configuration by entering the following command:
```
execute reload voiced
```

To configure the STUN server for ICE support

1. To connect to the FortiVoice CLI, go to **Dashboard > Console** and click inside the window.
2. Enter the following commands and replace xxx.xxx.xxx.xxx with the IP address or host name of a Fortinet or third-party STUN server:
```
config system sip-setting
   set ice-support stun-server
   set stun-server xxx.xxx.xxx.xxx
end
```
3. Reload the configuration by entering the following command:
```
execute reload voiced
```

Creating virtual IP addresses on FortiGate

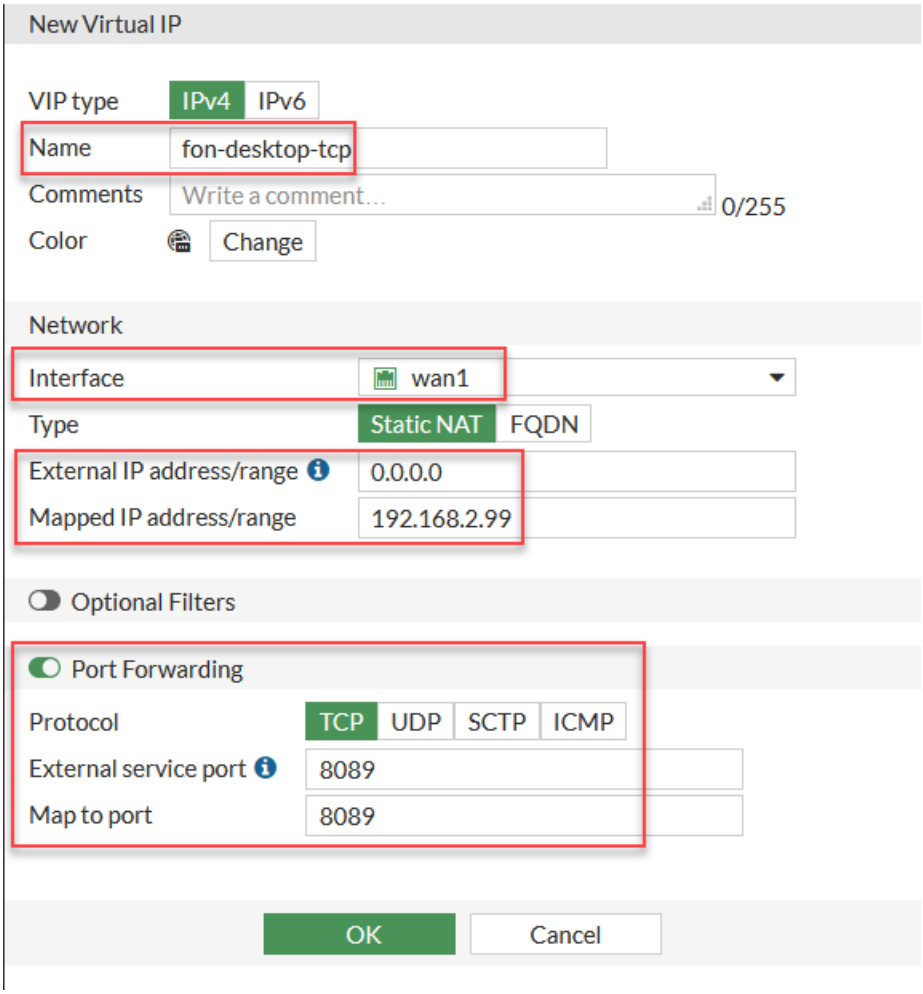
Create virtual IP addresses to be used for the following port forwarding:

- WSS port
- RTP port
- HTTPS port

To create a virtual IP address for the WSS port (using the TCP protocol)

1. On FortiGate, go to **Policy & Objects > Virtual IPs**.
2. Click **Create New > Virtual IP**.
3. Enter a **Name** to identify this virtual IP address.
4. Configure the settings.
   Here are example settings:
   - **Interface**: wan1
   - **External IP address/range**: 0.0.0.0
   - **Mapped IP address/range**: IP address of the FortiVoice unit
   - Enable **Port Forwarding**.
     - **Protocol**: TCP
     - **External port service**: 8089

- **Map to port**: 8089

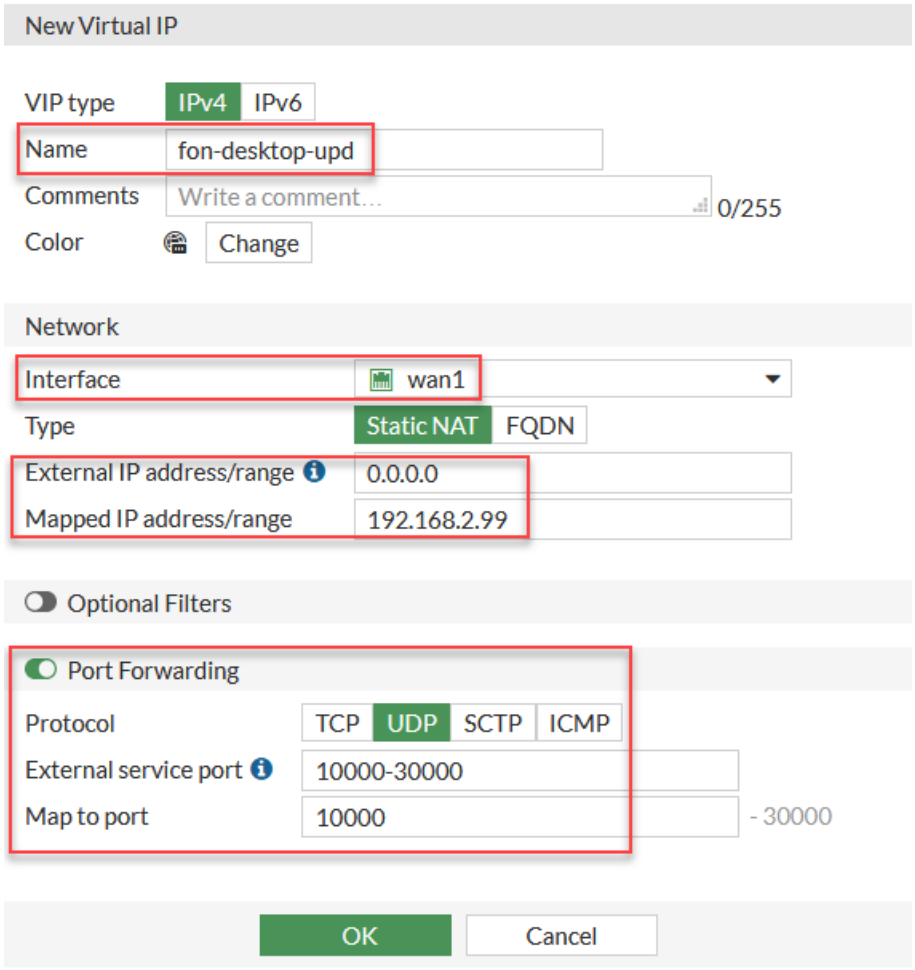


5. To save the changes, click **OK**.

To create a virtual IP address for the RTP port (encrypted using DTLS and running over UDP)

7. Click **Create New > Virtual IP**.
8. Enter a **Name** to identify this virtual IP address.
9. Configure the settings.
   Here are example settings:
   - **Interface**: wan1
   - **External IP address/range**: 0.0.0.0
   - **Mapped IP address/range**: IP address of the FortiVoice unit
   - Enable **Port Forwarding**.
     - **Protocol**: UDP
     - **External port service**: 10000 - 30000
       - **Note**: For the range of the **External port service**, make sure to use the same values as the **RTP Setting** available in **System > Advanced > SIP**.

- **Map to port**: 10000



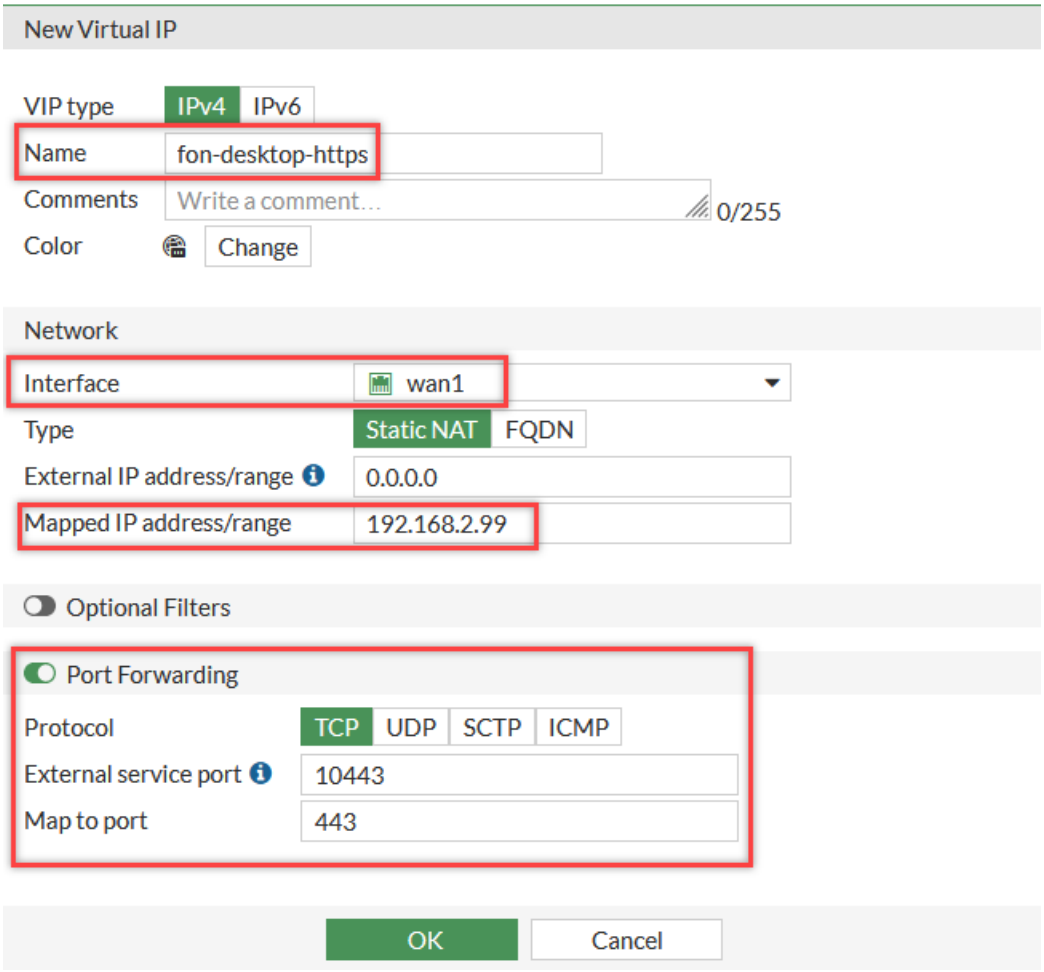
10. To save the changes, click **OK**.

To create a virtual IP address for the HTTPS port

The HTTPS port is used for logging in and downloading call detail records and voicemail messages.

11. Click **Create New > Virtual IP**.
12. Enter a **Name** to identify this virtual IP address.
13. Configure the settings.
    Here are example settings:
    - **Interface**: wan1
    - **External IP address/range**: 0.0.0.0
    - **Mapped IP address/range**: IP address of the FortiVoice unit
    - Enable **Port Forwarding**.
      - **Protocol**: TCP
      - **External port service**: 10443

- **Map to port**: 443



14. To save the changes, click **OK**.

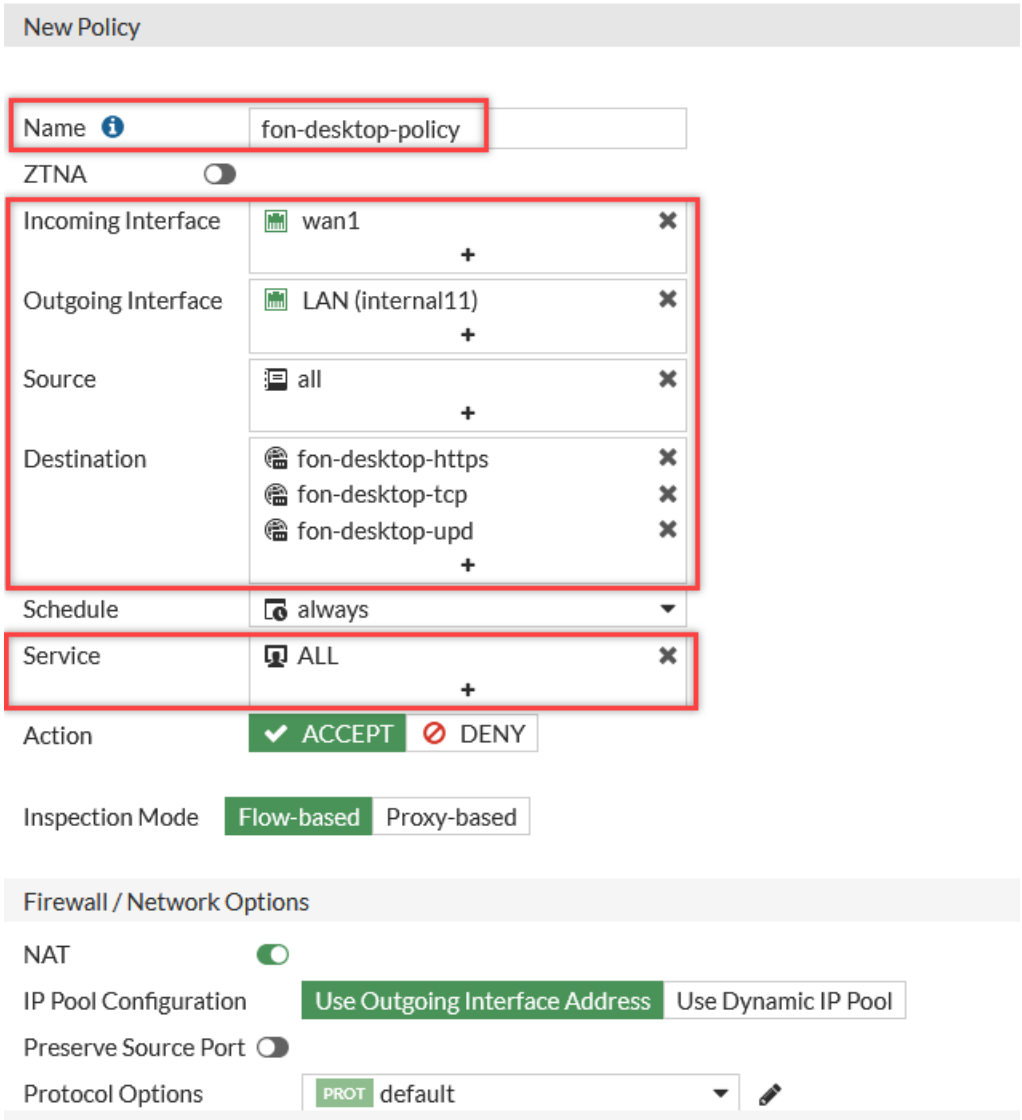
Configuring a FortiGate firewall policy for port forwarding

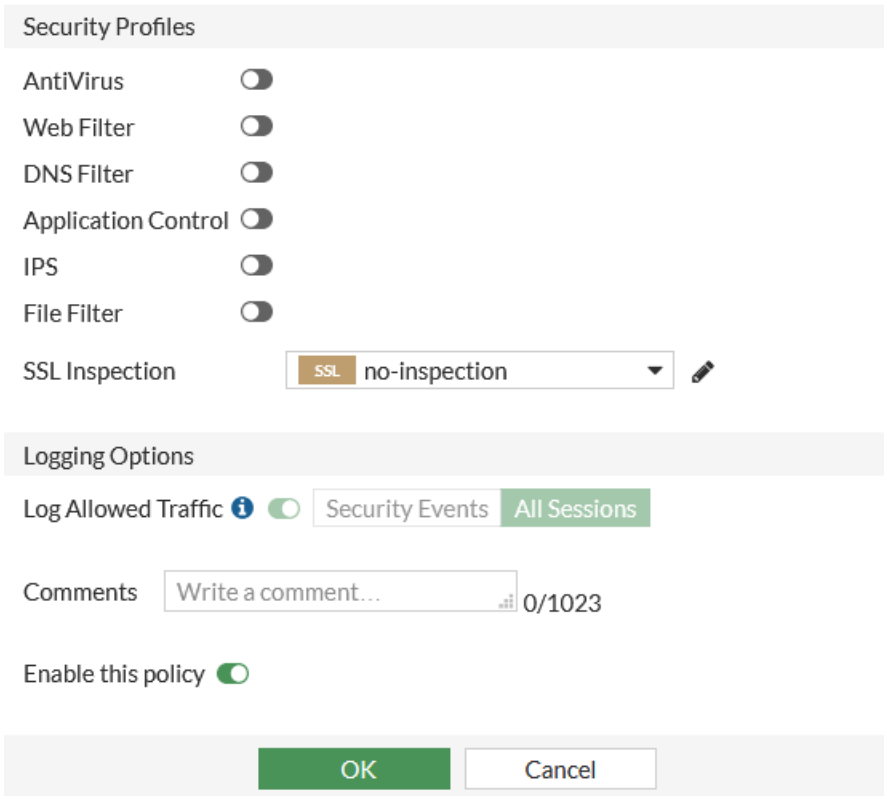
On FortiGate, configure a firewall policy to manage the port forwarding for the FortiFone softclient for desktop on the FortiVoice phone system.

Procedure steps

1. On FortiGate, go to **Policy & Objects > Firewall Policy**.
2. Click **Create New**.
3. Add a **Name** to identify this policy.
4. For a basic setup example, you can configure the following settings:
   - **Incoming interface**: wan1
   - **Outgoing interface**: LAN
   - **Source**: All
   - **Destination**: Select the virtual IP addresses that you created in Creating virtual IP addresses on FortiGate on page 134.

- **Service**: All


New Policy
Name
fon-desktop-policy
ZTNA
Incoming Interface
wan1
Outgoing Interface
LAN (internal11)
Source
all
Destination
fon-desktop-https
fon-desktop-tcp
fon-desktop-upd
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool
Preserve Source Port
Protocol Options
PROT
default



5. To save the new firewall policy, click **OK**.

Installing and configuring the FortiFone softclient for desktop

For details about installing, configuring, troubleshooting, and using the FortiFone softclient for desktop, see the FortiFone Softclient for Desktop User Guide.

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.