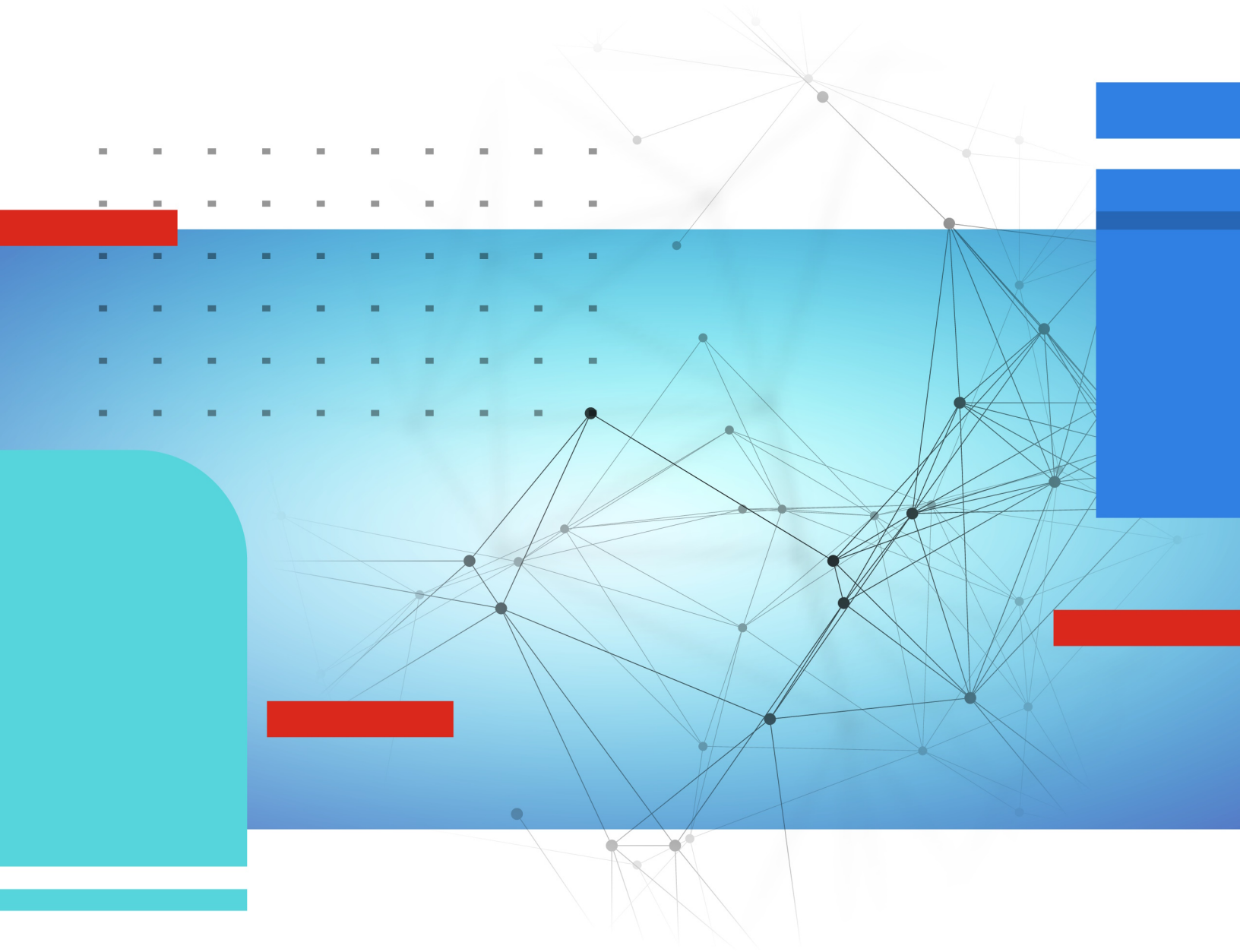
Local Survivable Gateway Deployment Guide

FortiVoice 7.0.7



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

FORTINET VIDEO LIBRARY
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/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

April 23, 2025
FortiVoice 7.0.7 Local Survivable Gateway Deployment Guide
26-707-882578-20250423

TABLE OF CONTENTS

Change log

Date	Change description
2025-04-23	Initial release of the FortiVoice 7.0.7 Local Survivable Gateway Deployment Guide.

Overview

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

Local survivability provides the following benefits:

- Centralized management
  - The main office handles all inbound and outbound calls thereby consolidating the number of lines required for an organization. The FortiVoice phone system at the main office sends consolidated configuration files and extensions to FortiVoice LSG units (survivability branches). Under normal operating conditions, a FortiVoice LSG unit in a branch office operates as a proxy server.
  - With the FortiVoice local survivability solution, you have one place to look for routing rules, logs, call records, and call recordings. If an extension is added, it is operational immediately. Any user at any location is able to call that new extension right away without waiting for configuration synchronization or new policies setup to be completed at each location.
- Branch office resiliency
  - A FortiVoice LSG unit provides branch office resiliency for a centralized multi-site network deployment.
  - If the main office becomes unavailable or the communication between the main office and branch office is interrupted, the FortiVoice LSG unit at the branch office operates as an IP PBX to provide the phone service until the main office is available or the communication between the main office and branch office is restored.

This section includes the following topics:

Supported models

The FortiVoice LSG models are:

- FVE-20E2
- FVE-20E4
- FVE-50E6
- FVE-50G2
- FVE-100E
- FVE-100F
- FVE-200F8
- FVE-1000E
- FVE-500F

The FortiVoice phone system continues to support FVE-100E as a FortiVoice LSG model. However, it has reached its end-of-order (EOO) date.

The following FortiVoice phone system models can manage one or more survivability branches (FortiVoice LSG):

- FVE-300E-T and larger
- FVE-VM-500 and larger

For details about the capacity of FortiVoice phone systems for managed branches, see the FortiVoice Phone System Capacities Data Sheet.

For more details about the FortiVoice phone systems, see the FortiVoice Phone Systems Data Sheet.

Topology

You can create a FortiVoice LSG topology by using Multiprotocol Label Switching (MPLS), a virtual private network (VPN), or software-defined networking in a wide area network (SD-WAN). When using a VPN, you can set up VPN tunnels between the branch office and the main office to avoid configuring rules and policies for various traffic types. Calls between extensions are always routed through the main office system, so a VPN tunnel setup between branch offices is not required.

An office peer configuration between the central office and a branch office must be set up if you want to transfer an incoming call through a FXO or PRI gateway from a branch office extension to a central office extension. For more details on office peer, see the FortiVoice Phone System Administration Guide.

The main office manages configuration information for the branch phones and offices. The main office has the following management functions:

- Creation of all branch office extensions: The main office pushes all branch office extensions to each branch office.
- Storage of all voicemail messages: The main office, not the branch office, stores all voicemail messages.
- Phone registration: Phones register with the FortiVoice phone system at the main office and with the FortiVoice LSG unit at the branch office.

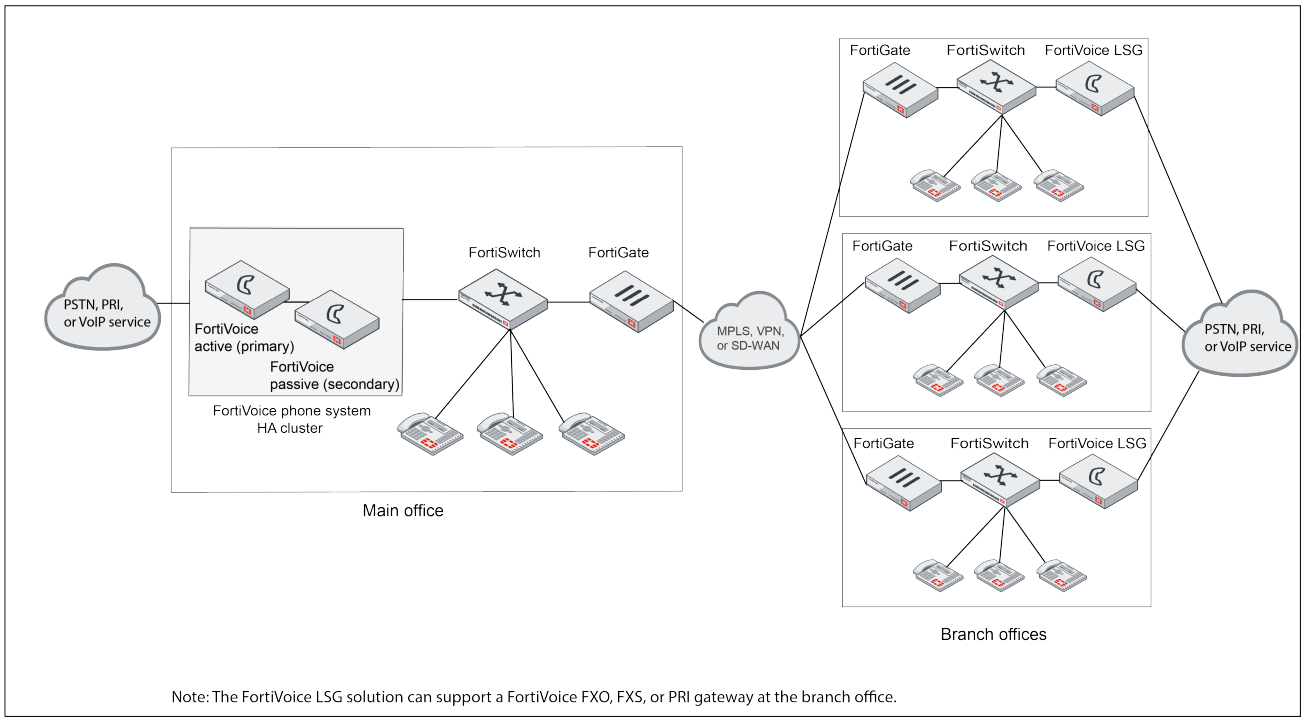
Configuration changes required at each branch office are limited to the following settings:

- Administrator accounts
- Network configuration settings
- Outbound call routing for failover scenarios
- Branch SIP port setting. If the branch office is using a non-default SIP port, then you must make sure to include that branch SIP port setting when configuring the survivability branch management on the FortiVoice phone system at the main office.

The FortiVoice LSG solution can support the following gateways at the branch office:

- FortiVoice Gateway GO04 and GO08, a foreign exchange office (FXO) gateway. For deployment details, see the FortiVoice FXO Gateway Deployment Guide.
- FortiVoice Gateway GS04, GS16, and GS24, a foreign exchange subscriber (FXS) gateway. For deployment details, see the FortiVoice FXS Gateway Deployment Guide.
- FortiVoice Gateway GT01 and GT02, primary rate interface (PRI) gateways. For deployment details, see the FortiVoice PRI Gateway Deployment Guide.

The following image shows a FortiVoice LSG topology example:



Call flows

This section describes inbound and outbound call flows and explains roles taken by the FortiVoice phone system at the main office and the FortiVoice LSG unit at the branch office.

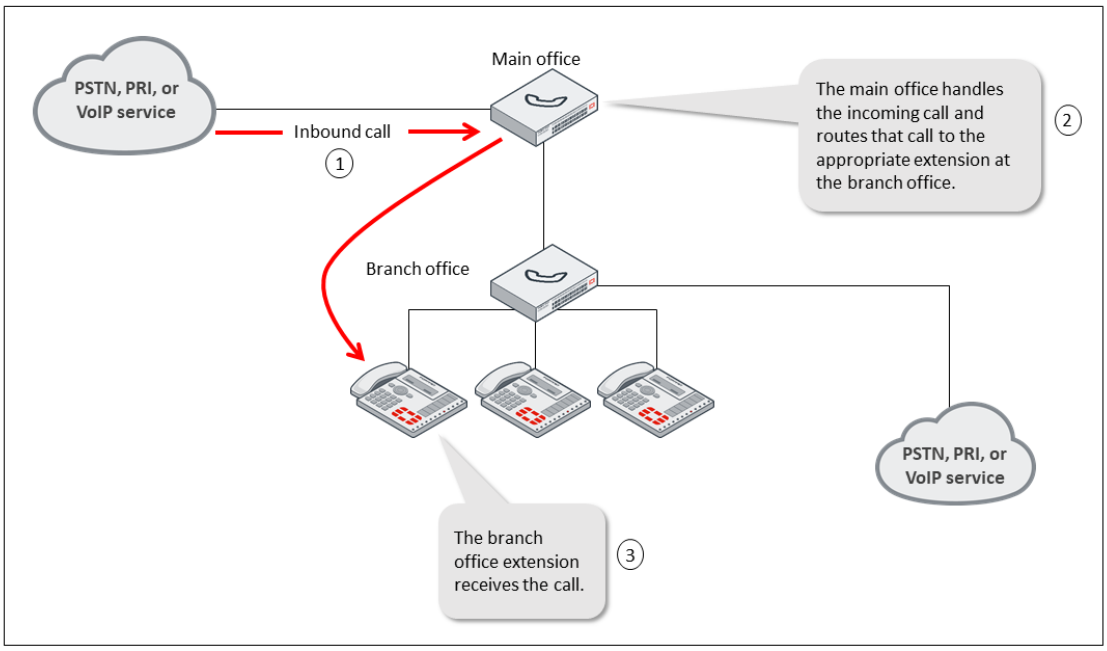
This section includes the following topics:

Inbound call flow

Inbound calls come into the system through the primary rate interface (PRI) or voice over IP (VoIP) service. The main office handles all inbound calls and routes them to the right extension at the branch office.

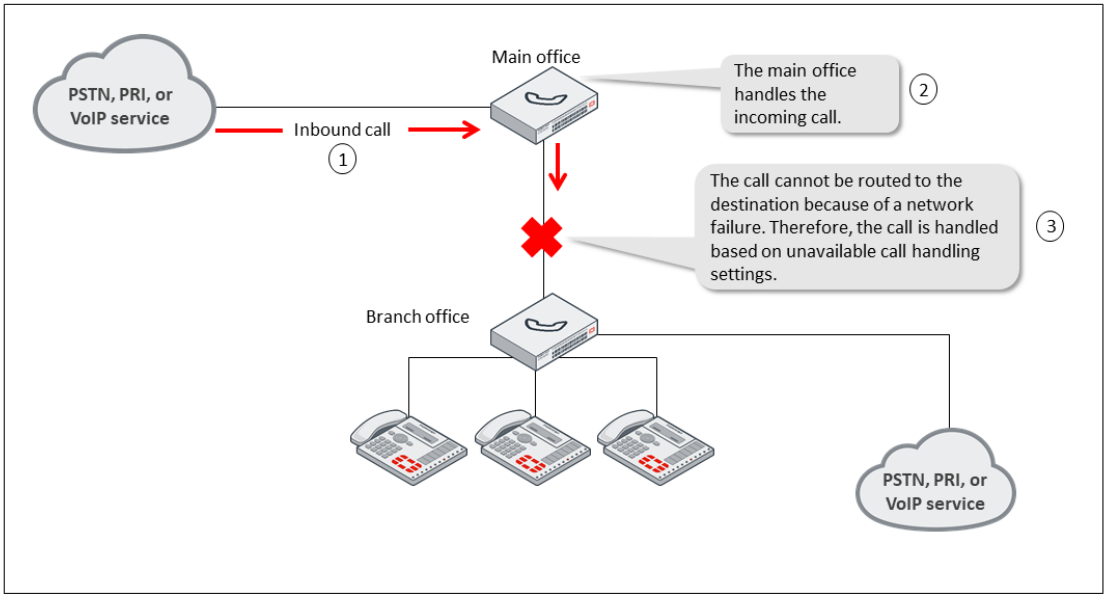
The main office sends Session Initiation Protocol (SIP) and Real Transport Protocol (RTP) traffic directly to the phone, not to the branch office.

An office peer configuration between the central office and a branch office must be set up if you want to transfer an incoming call through a FXO or PRI gateway from a branch office extension to a central office extension. For more details on office peer, see the FortiVoice Phone System Administration Guide.



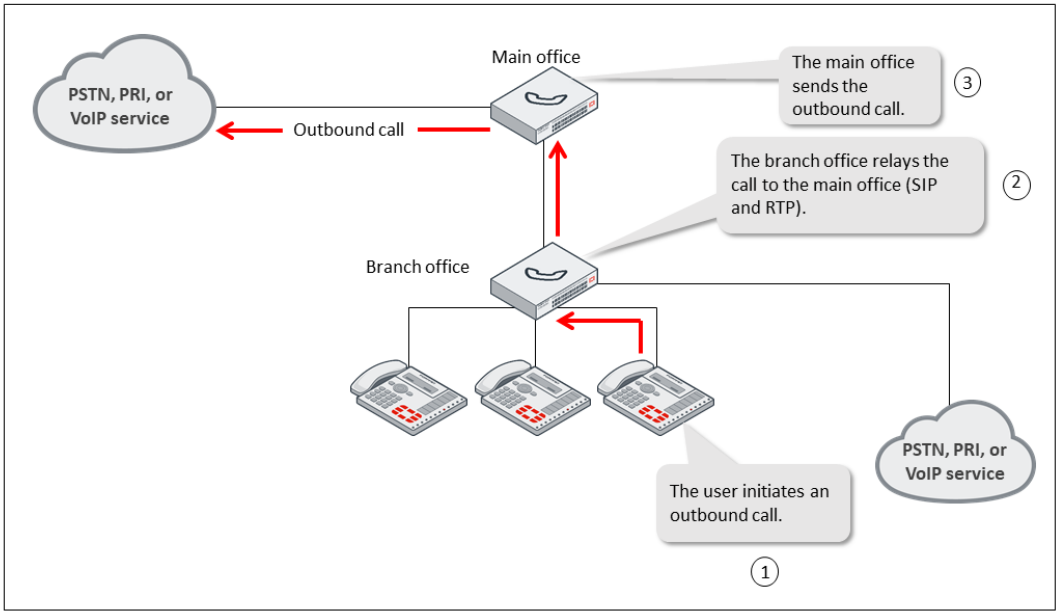
Inbound call flow with a network impairment or failure

If there is a network impairment or failure, a call may not reach the extension at the branch office. The main office routes the call according to the unavailable call handling settings which is typically to send the call to the voicemail.



Outbound call flow

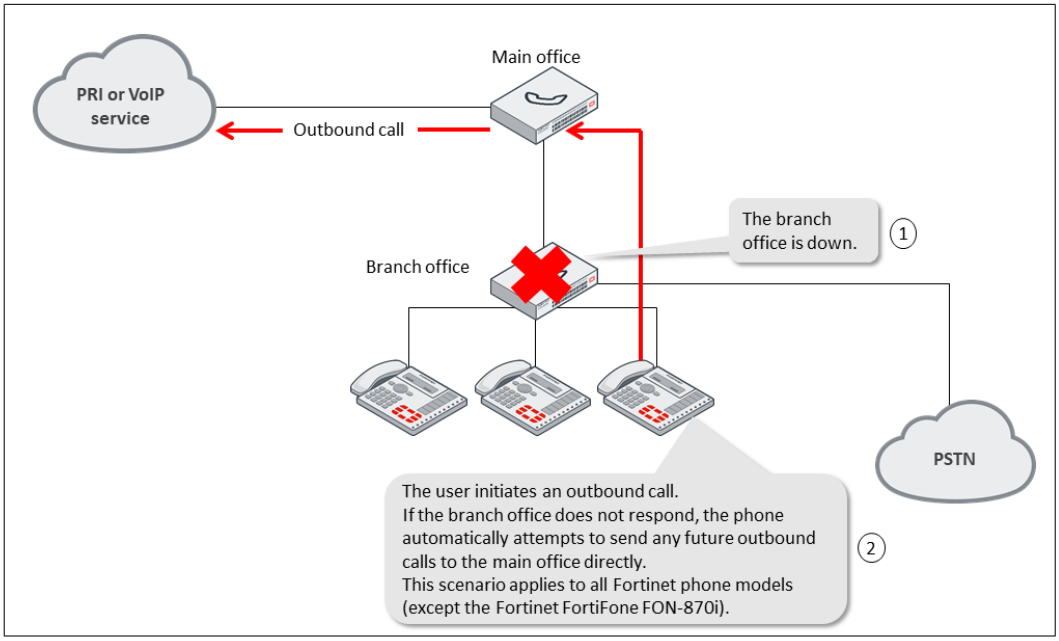
In an outbound call flow, the phone sends calls to the branch office. The branch office relays SIP traffic directly to the main office. The main office processes outbound calls.



Outbound call flow when the branch office is down

If the branch office does not respond, the outbound call flow changes depending on the phone model as explained in the following two scenarios:

- The phone automatically attempts to send any future outbound calls to the main office directly. This scenario applies to all Fortinet phone models (except the Fortinet FortiFone FON-870i).
- The phone does not automatically attempt to send any future outbound calls to the main office directly. This scenario applies to the Fortinet FortiFone FON-870i.



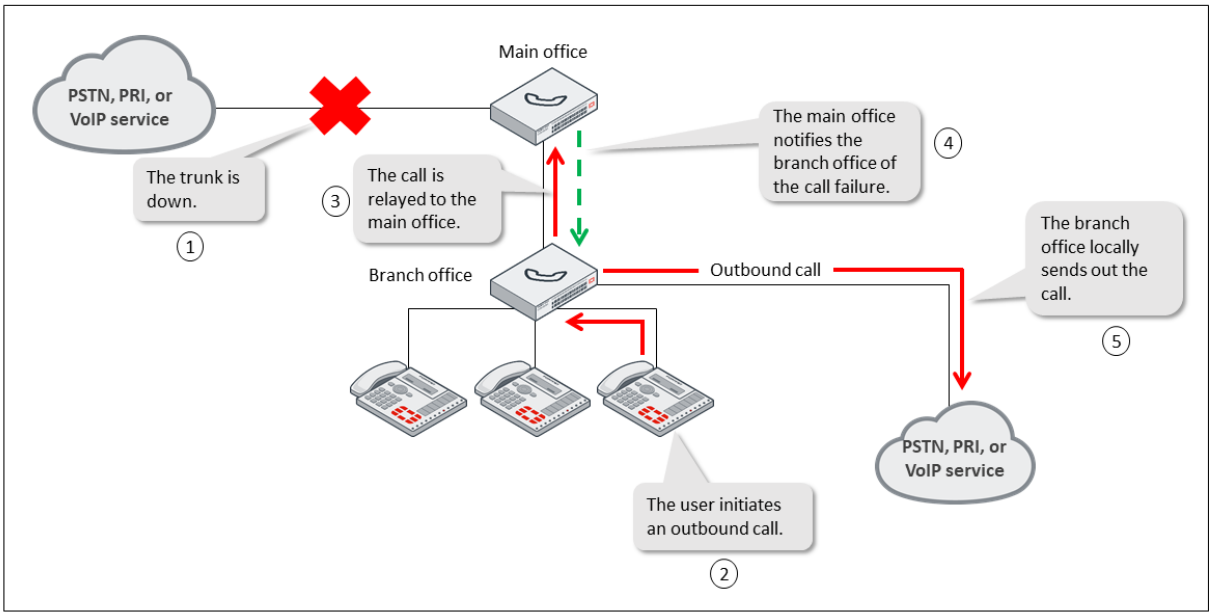
Outbound call flow when the main office trunk is down

If the main office trunk stops working, the branch office system can handle calls.

If you enable the *Central trunk fallback to branch* feature on the main office unit, the main office sends an error code to the branch office when the main office trunk is down. The branch office can then locally handle calls. You may also need to set up an outbound call route on the branch office unit to handle this failover scenario.

Details about enabling the *Central trunk fallback to branch* feature are included in Adding a survivability branch on page 25.

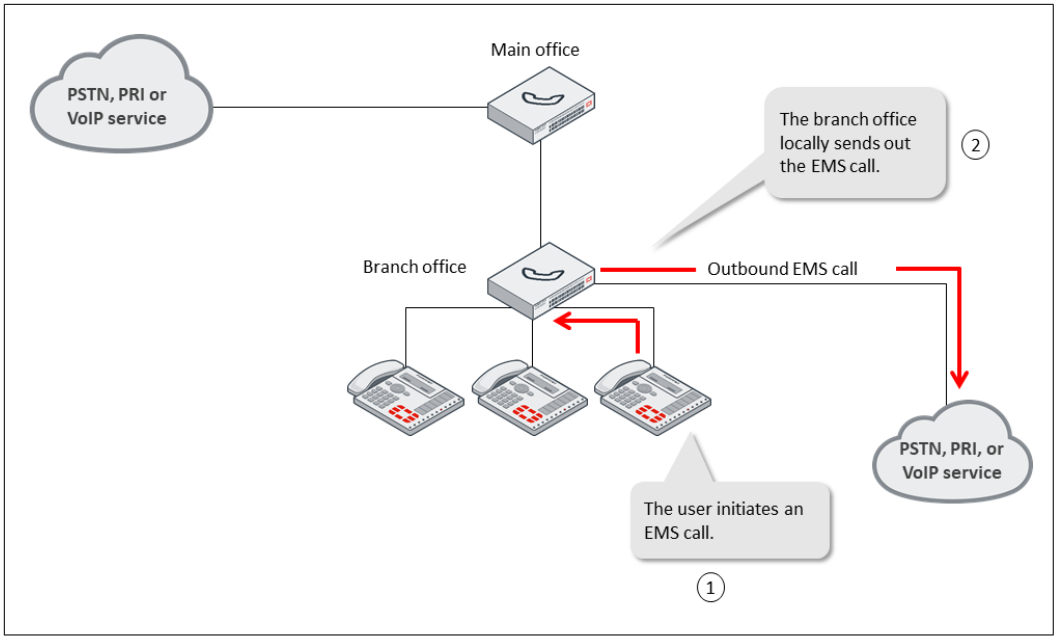
Details about creating an outbound call route are included in Creating an outbound call route for failover scenarios on page 22.



Outbound call flow for a 911 or emergency medical services call

For routing 911 or emergency medical services (EMS) calls, administrators have the following two options:

- The branch office routes emergency calls to branch lines and then to PSTN lines: This is the preferred routing method because PSTN lines always have the correct civic address setup with the public safety answering point (PSAP) service. For this scenario, administrators must make sure that the survivability branch setup on the FortiVoice phone system at the main office has the *Emergency call* option set to *handled by branch*, not to the default *(handled by central*).
- The main office routes emergency calls: The administrator at the main office manages emergency calls initiated from different extensions to route them to a line that has an address mapped to that location. The carrier providing the phone service, PRI, or VoIP handles the civic address mapping. However, the administrator works with the carrier to make sure that phone numbers map to the correct civic addresses. To configure a profile to manage emergency calls and extensions, access the GUI of the FortiVoice phone system at the main office and go to *Phone System* > *Profile* > *Emergency Zone*.

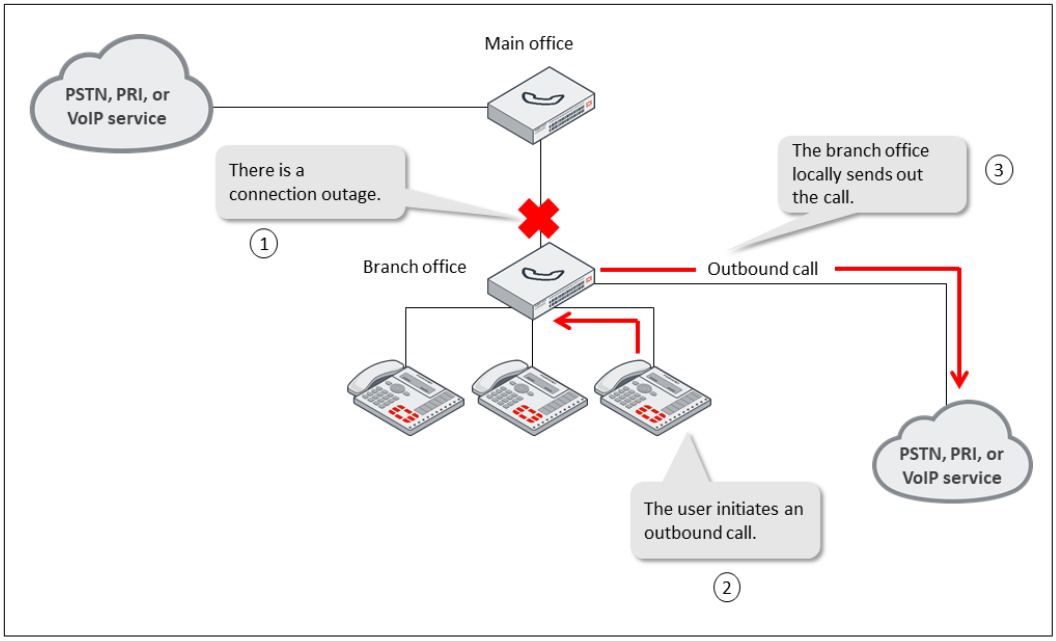


Outbound call flow with a PSTN, PRI, or VoIP failover

If the connection between the branch office system and the main office stops working, the branch office routes the call out through its local lines. The phone is unaware of any problems in the network because the call still goes through. You may also need to set up an outbound call route on the branch office unit to handle this failover scenario. Details about creating an outbound call route are included in Creating an outbound call route for failover scenarios on page 22.

During a connection outage, the following call behaviors apply:

- Calls from the main office cannot reach the branch office.
- Calls from the branch office cannot reach the main office.
- Calls from one branch office cannot reach another branch office. However, calls from one extension can reach another extension at the same branch.
- The branch office voicemail responds to a login. However, recorded messages are unavailable because the branch office voicemail cannot synchronize with the main office voicemail which stores all call recordings.



Deployment

To deploy a FortiVoice LSG unit in a branch office, review the tasks and perform the procedures in the following workflow:

If you connect the phones too early in the workflow, you will need to restore the phones to their factory default settings to remove the unassigned phone configuration that was retrieved from the branch office system.

To connect the phones to the network, make sure to follow the workflow in this section. With this workflow, the phones are assigned the correct configuration from the main office system.

Before starting procedures in this guide, make sure to complete the basic setup of the primary and secondary FortiVoice phone systems and connect to the GUI of both systems. For more details, see the FortiVoice Phone System Administration Guide.

Task sequence	Description	Procedure
Perform tasks 1 to 5 on the FortiVoice LSG unit at the branch office.		
Task 1	Perform the following actions to complete the initial setup of the FortiVoice LSG unit: • Physically install the FortiVoice LSG unit. • Connect the Ethernet port to your network. • Connect an FXO port to the PSTN network. This action does not apply to the FVE-100F and FVE-500F (and FVE-100E which is still supported but have reached the end-of-order [EOO] date).	
Task 2	Connect to the GUI of the FortiVoice LSG unit.	Connecting to the FortiVoice LSG unit on page 18
Task 3	Configure administrator and network settings on the FortiVoice LSG unit.	Configuring administrator and network settings on page 20
Task 4	Upgrade the firmware of the FortiVoice LSG unit.	Upgrading the FortiVoice LSG firmware on page 22

Task sequence	Description	Procedure
Task 5	Change the deployment mode from *PBX* to *survivability branch* on the FortiVoice LSG unit.	Configuring the deployment mode on page 23
Perform tasks 6 to 9 on the FortiVoice phone system at the main office, as applicable.		
Task 6	Optionally, configure high availability (HA) on the primary and secondary FortiVoice units at the main office.	Optional - Configuring high availability on page 24
Task 7	Add or import branch extensions to the primary FortiVoice phone system at the main office.	Adding or importing branch extensions on page 24
Task 8	Add a survivability branch to the FortiVoice phone system at the main office.	Adding a survivability branch on page 25
Task 9	Apply the branch configuration from the main office FortiVoice phone system to the FortiVoice LSG unit at the branch office.	Applying the branch configuration on page 29
Perform tasks 10 and 11 on the FortiVoice LSG unit at the branch office.		
Task 10	Verify that there is a healthy heartbeat between the FortiVoice LSG unit and the FortiVoice phone system.	Verifying the heartbeat status on page 30
Task 11	Connect the phones to the network at the branch office.	Connecting the phones to the network on page 31
Configuring FortiVoice Gateways (optional)		
If you want to configure a FortiVoice Gateway to add analog or PRI phone lines to your FortiVoice LSG unit at the branch office, go to FortiVoice Gateway configuration on page 32.		
Branch paging (optional)		
If you want your FortiVoice LSG deployment to use paging, go to Branch paging on page 46.		

Connecting to the FortiVoice LSG unit

After physically installing the FortiVoice LSG unit and completing its initial setup, connect to the FortiVoice LSG GUI by reviewing the following table and performing the procedure that applies to your scenario:

Scenario	Then
You are connecting to the unit for the first time.	Perform the steps in Connecting to the GUI of the FortiVoice LSG unit on page 19.
You have reset the configuration to its default state.	Perform the steps in Connecting to the GUI of the FortiVoice LSG unit on page 19.
You are a returning user that has completed the basic configuration of the unit.	Access the GUI using the IP address, administrative access protocol, administrator account, and password already configured, instead of the default settings. 1. Start a web browser and enter the URL: `https://<IP_address>/admin` Where <IP_address> is the IP address of the FortiVoice LSG unit that you want to connect to. If the FortiVoice LSG unit configuration is using a non-default HTTPS port, then add :<port_number> after the IP address. For example: `https://<IP_address>:446/admin`. 2. Enter the name and password associated with your account. 3. Click **Login**. You have completed this procedure. 4. Go to Configuring administrator and network settings on page 20 to make sure that you configure the required settings.

Connecting to the GUI of the FortiVoice LSG unit

Prerequisites

To connect to the GUI of the FortiVoice LSG unit using its default settings, you must have the following hardware and software:

- A computer with an RJ-45 Ethernet network port
- One of the recommended web browsers:
  - Google Chrome version 132
  - Microsoft Edge version 132
  - Mozilla Firefox Standard Release version 134
  - Apple Safari version 18.2
- An Ethernet cable

Procedure steps

1. On your management computer, configure the Ethernet port with the static IP address 192.168.1.2 and a subnet mask of 255.255.255.0.
2. Using the Ethernet cable, connect the Ethernet port of the management computer to port1 of the FortiVoice LSG unit.
3. Start your browser and enter the default URL https://192.168.1.99/admin.

4. To support HTTPS authentication, the FortiVoice LSG unit ships with a self-signed security certificate, which it presents to users whenever they initiate an HTTPS connection to the FortiVoice LSG unit. When you connect, depending on your web browser and prior access of the FortiVoice LSG unit, your browser may display two security warnings related to this certificate:
   - The certificate is not automatically trusted because it is self-signed, rather than being signed by a valid certificate authority (CA). Self-signed certificates cannot be verified with a proper CA, and therefore might be fraudulent. You must manually indicate whether or not to trust the certificate.
   - The certificate may belong to another website. The common name (CN) field in the certificate, which usually contains the host name of the website, does not exactly match the URL you requested. This could indicate a server identity theft, but could also simply indicate that the certificate contains a domain name while you have entered an IP address. You must manually indicate whether this mismatch is normal or not.

     Both warnings are normal for the default certificate.
5. Verify and accept the certificate, either permanently (the web browser will not display the self-signing warning again) or temporarily. You cannot log in until you accept the certificate. For details on accepting the certificate, see the documentation for your web browser.
6. In **Name**, enter `admin`.
7. Leave the **Password** field empty. In its default state, there is no password for this account.
8. Click **Login**.

   With a successful login, the GUI appears.
9. Set the password for this account:
   a. In the right corner of the GUI, click **Admin**.
   b. Click **Change Password**.

   Enter a FortiVoice LSG administrator password that is six characters or more. For better security, enter a longer password with a complex combination of characters and numbers, and change the password regularly. Failure to provide a strong password could compromise the security of your FortiVoice LSG.

   c. Enter a password in **New password** and **Confirm password**.

      The password can contain any character except spaces.
   d. Click **OK**.

   You have completed this procedure.
10. Go to Configuring administrator and network settings on page 20.

Configuring administrator and network settings

Configure administrator and network settings on the FortiVoice LSG unit by completing the following procedures:

- Editing a network interface on page 21
- Creating a static route on page 21
- Configuring DNS servers on page 21
- Creating an additional administrator account on page 21, optional
- Creating an outbound call route for failover scenarios on page 22

Editing a network interface

Use this procedure to edit a physical network interface of a FortiVoice LSG unit to change their IP addresses, netmasks, administrative access protocols, and other settings.

1. In the FortiVoice LSG GUI, go to **System > Network**.
   The **Network** tab displays the following default ports:
   Port 1 has a default IP address and netmask set to 192.168.1.99/24.
   Port 2 has a default IP address set to 192.168.2.99/24.
2. Double-click a network interface that you want to use to set the IP address of the FortiVoice LSG unit.
3. In **IP/Netmask**, edit the IP address and netmask of the interface.
4. In **Advanced Setting**, update the **Access** list. Make sure to enable the protocols that you want the network interface to use to accept connections to the FortiVoice LSG unit.
5. In **Administrative status**, make sure that **Up** is selected for the network interface to be available to receive traffic.
6. Click **OK**.

Creating a static route

Use this procedure to create a static route.

1. In the FortiVoice LSG GUI, go to **System > Network** and click the **Routing** tab.
2. Click **New**.
3. In **Destination IP/Netmask**, enter the destination IP address and netmask of packets subject to this static route. To create a default route that matched all destination IP address, enter 0.0.0.0/0.
4. In **Interface**, enter the interface that this route applies to.
5. In **Gateway**, enter the IP address of the router.
6. Click **OK**.

Configuring DNS servers

A FortiVoice LSG unit requires domain name system (DNS) servers for features such as reverse DNS lookups. In this procedure, you can use IP addresses supplied by your internet service provider (ISP) or from your own DNS servers.

1. In the FortiVoice LSG GUI, go to **System > Network** and click the **DNS** tab.
2. In **Primary DNS server**, enter the IP address of the primary DNS server.
3. In **Secondary DNS server**, enter the IP address of the secondary DNS server.
4. Click **Apply**.

Creating an additional administrator account

Optionally, perform this procedure to create an additional administrator account with restricted permissions. By default, a FortiVoice LSG unit has a single administrator account called *admin*.

1. In the FortiVoice LSG unit GUI, go to **System > Administrator**, and click the **Administrator** tab.
2. To add an account, click **New**.
3. For details about the GUI fields, see the Configuring administrator accounts section in the FortiVoice Phone System Administration Guide.

Creating an outbound call route for failover scenarios

If you enable the *Central trunk fallback to branch* feature on the main office unit, the main office sends an error code to the branch office when the main office trunk is down. The branch office can then locally handle calls. If you need to create an outbound call route on the branch office unit to handle this failover scenario, make sure that this route matches the route configured at the main office as defined in the **Dialed Number Match** section (**Call Routing > Outbound**).

To create an outbound call route on the branch office unit to handle this failover scenario, perform the following steps:

1. In the FortiVoice LSG GUI, go to **Call Routing > Outbound**.
2. Click **New**.
3. For details about the GUI fields, see the Configuring outbound dial plans section in the FortiVoice Phone System Administration Guide.

You have completed the procedures for configuring administrator and network settings. Go to Upgrading the FortiVoice LSG firmware on page 22.

Upgrading the FortiVoice LSG firmware

Use this procedure to upgrade the FortiVoice LSG firmware.

Procedure steps

1. Identify the firmware version that is running on the FortiVoice LSG unit:
   a. In the FortiVoice LSG GUI, go to **Dashboard** and the **Status** tab.
   b. In the **System Information** widget, review the **Firmware version** row.
   c. Take note of the firmware version and build number.
2. Identify the latest software release that is available for the FortiVoice LSG firmware:
   a. Go to the Fortinet Support website.
   b. Log in to your existing account or register for an account.
   c. Select **Support > Firmware Download**.
   d. In **Select Product**, select **FortiVoice**.
   e. On the **Release Notes** tab, review the list to identify the latest 7.0 firmware build.
   f. Compare the build number with the firmware version that is running on the FortiVoice LSG unit.
   g. If the firmware version running on the FortiVoice LSG unit matches the one on the Fortinet Support website, then you do not need to perform an upgrade. You have completed this procedure. Go to Configuring the deployment mode on page 23.
   h. If the firmware version running on the FortiVoice LSG unit is an earlier build, then you need to prepare for an upgrade:
      i. Review the FortiVoice Phone System 7.0.7 Release Notes. This document includes the most current upgrade information such as supported upgrade paths and may contain details that were unavailable at the time this procedure was created.
      ii. In the **Download** tab, navigate through the v7.00 directories to locate the firmware image file. For example, FVE_200F-v70-build0113-FORTINET.out.
      iii. To download the firmware image file to your management computer, go to the end of the row and click **HTTPS**.
      iv. Save the file on your management computer and take note of the location where you save the file.

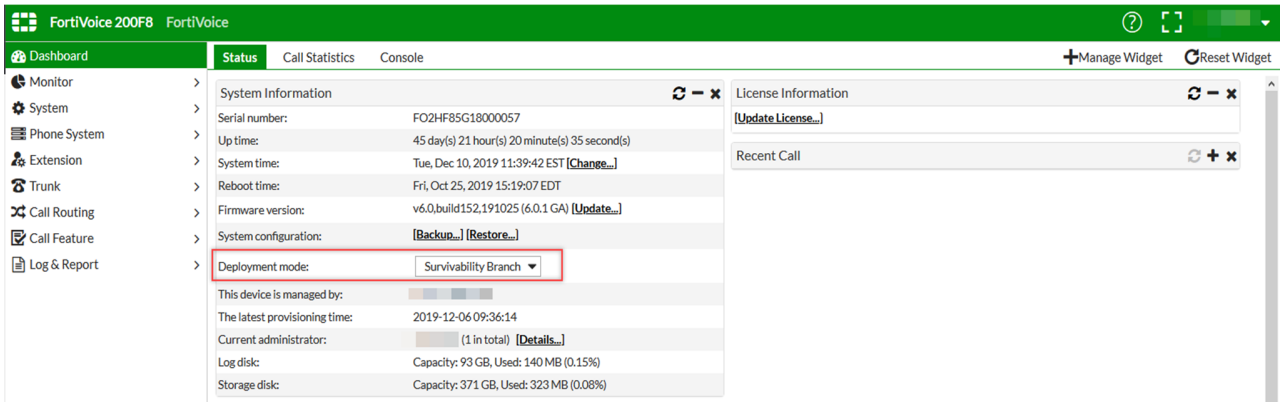
3. Backup the configuration file:
   a. In the FortiVoice LSG GUI, go to **Dashboard** and the **Status** tab.
   b. In the **System Information** widget, go to the **System configuration** row.
   c. Click **Backup**.
   d. Save the file on your management computer and take note of the location where you save the file.
4. Upgrade the firmware:
   a. In the FortiVoice LSG GUI, go to **Dashboard** and the **Status** tab.
   b. In the **System Information** widget, go to the **Firmware version** row.
   c. Click **Update**.
   d. Locate the firmware file and then upload that file.
   Your web browser uploads the firmware file to the FortiVoice LSG unit.
   e. To confirm the upgrade, click **Yes**.
   The FortiVoice LSG unit installs the firmware and restarts.
   f. To make sure that the FortiVoice LSG GUI reloads correctly and displays all changes, clear the cache of your web browser and restart it.
5. Verify that the firmware is successfully installed:
   a. In the FortiVoice LSG GUI, go to **Dashboard** and the **Status** tab.
   b. In the **System Information** widget, go to the **Firmware version** row.
   c. Make sure that the firmware version is the one that you upgraded to.
   You have completed this procedure.
6. Go to Configuring the deployment mode on page 23.

Configuring the deployment mode

Use this procedure to configure the deployment mode on the FortiVoice LSG unit at the branch office.

Procedure steps

1. In the FortiVoice LSG GUI, go to **Dashboard** and the **Status** tab.
2. In the **System Information** widget, go to the **Deployment mode** drop-down list.
3. Select **Survivability Branch**.



4. To confirm, click **Yes**.
   You have completed this procedure.

5. To configure high availability (HA) on the primary and secondary FortiVoice units at the main office, go to Configuring high availability on page 24.
   If you do not want to configure HA, go to Adding or importing branch extensions on page 24.

Configuring high availability

Optionally, configure high availability (HA) on the primary and secondary FortiVoice phone systems at the main office. Make sure to set the correct virtual IP address because this IP address is used throughout the local survivability setup.

Procedure steps

1. Physically connect the primary and secondary FortiVoice phone systems that will be members of the HA group. You must connect at least one of their network interfaces for heartbeat and synchronization traffic between members of the group. For reliability reasons, Fortinet recommends that you connect both a primary and a secondary heartbeat interface, and that they be connected directly or through a dedicated switch that is not connected to your overall network.
2. Connect to the GUI of the primary FortiVoice phone system at the main office.
3. Go to **System > High Availability**, and click the **Configuration** tab.
4. Configure the HA options, as applicable.
   - HA configuration
   - Advanced options
   - Interfaces
   - Service monitoring
5. For more details about configuring HA, see the Configuring the HA mode and group section in the FortiVoice Phone System Administration Guide.
6. HA settings, with the exception of virtual IP Address settings, are not synchronized and must be configured separately on each primary and secondary FortiVoice phone system.
7. Connect to the GUI of the secondary FortiVoice phone system at the main office.
8. Go to **System > High Availability**, and click the **Configuration** tab.
9. Configure the HA options, as applicable.
   - HA configuration
   - Advanced options
   - Interfaces
   - Service monitoring
10. For more details about configuring HA, see the Configuring the HA mode and group section in the FortiVoice Phone System Administration Guide.
    You have completed this procedure.
11. Go to Adding or importing branch extensions on page 24.

Adding or importing branch extensions

Use this procedure to add or import branch extensions to the primary FortiVoice phone system at the main office.

Adding a branch extension

1. Connect to the GUI of the primary FortiVoice phone system at the main office.
2. Go to **Extension > Extension**.
3. On the **IP Extension** tab, click **New**.
4. For details about the fields, see the Configuring IP extensions section in the FortiVoice Phone System Administration Guide.
   You have completed this procedure.
5. Go to Adding a survivability branch on page 25.

Importing a list of branch extensions

Use the import feature to add a list of branch extensions in one operation using a CSV file with columns that match the FortiVoice format.

Make sure that your CSV file includes the following column headings:

- User ID
- Extension
- Display name
- Phone type
- Mac address
- Phone profile

If the CSV does not include those column headings, the import will fail.

1. Connect to the GUI of the primary FortiVoice phone system at the main office.
2. Go to **Extension > Extension**.
3. On the **IP Extension** tab, click **Actions > Import**.
4. Locate and upload the CSV file.
   You have completed this procedure.
5. Go to Adding a survivability branch on page 25.

Adding a survivability branch

Use this procedure to add a survivability branch to the FortiVoice phone system at the main office. You may apply the configurations to the FortiVoice LSG unit. For details, see Applying the branch configuration on page 29.

Procedure steps

1. Connect to the GUI of the primary FortiVoice phone system at the main office.
2. Go to **Managed System > Survivability**.
3. On the **Survivability Branch** tab, click **New** and configure the following parameters:

GUI field	Description
Enabled	Select to enable the configuration of the branch unit (FortiVoice LSG).
Name	Enter a unique name for this survivability branch.

GUI field	Description
Display name	Not required. You can leave this field empty.
Host name/IP address	Enter the hostname or IP address of the branch unit (FortiVoice LSG). If the FortiVoice LSG unit is configured to use a non-default HTTPS port, then add `:<port number>` after the IP address. For example, `172.16.5.11:4430`. **Get Device Information**: • Before you click this button, make sure to enter the required information in the **Admin user name** and **Admin password** fields below. • Click this button to poll the provisioned branch unit and get the serial number, type, and MAC address of the branch unit. This action can confirm that the systems can communicate and that the password is valid. **Connect Device**: This procedure does not use this button.
Admin user name	Enter the user name of the administrator account used for logging in to the branch unit. The default is admin.
Admin password	Enter the password associated with the Admin user name. To show the password, click the eye icon  .
Serial number	The serial number of the FortiVoice LSG unit that you are adding to this survivability branch. If you are configuring the survivability branch before deploying the FortiVoice LSG unit, then manually update the serial number, type, and MAC address.
Type	Select the model of the FortiVoice LSG unit that you are adding to this survivability branch. If you select FVE-20E2, FVE-50E6, or FVE-50G2, these models will each support 2 FXS ports for analog phones and fax. When the configuration is applied to the FortiVoice LSG unit, 2 analog extensions associated with the FXS ports and 2 SIP trunks mapped to the extensions are automatically generated by the system. To view the analog extensions, on the FortiVoice LSG unit, go to **Extension > Extension > Analog Extension**. To view the SIP trunks, on the FortiVoice LSG unit, go to **Trunk > VoIP > SIP**.
MAC address	The MAC address of the FortiVoice LSG unit that you are adding to this survivability branch. If you are configuring the survivability branch before deploying the FortiVoice LSG unit, then manually update the MAC address.
Description	Optionally, add any applicable notes for this survivability branch.
Survivability Setting	This section includes settings related to how the branch unit operates.
Management mode	Make sure to select **Fully managed**. **Fully managed - without branch paging**

GUI field	Description
	With the fully managed mode and without branch paging configured, the main office pushes the following configurations to the branch unit. • Extension user • Extension preferences • Global system settings • PBX setting • Profile location • Survivability branch • System auto-provisioning • System PSTN channels • Trunk PSTN **Fully managed - with branch paging** With the fully managed mode and branch paging configured, the main office pushes the following configurations to the branch unit. • Call handling • Dialplan FXO gateway mapping • Dialplan outbound • Extension user • Extension preferences • Global system settings • PBX account code • PBX setting • Profile location • Survivability branch • System auto-provisioning • System PSTN channels • Trunk PSTN • Trunk SIP peer
Heartbeat server address	Select the heartbeat server on the main office unit that is used to monitor the status of each branch unit in the network and enable communications between the main office unit and the branch unit. • **Internal Provisioning Address**: The SIP server IP address of the main office unit which the branch unit sends OPTIONS SIP message to. • **External Host IP**: The external static IP address of the main office unit which the branch unit sends OPTIONS SIP messages to.
Branch SIP server	Enter the SIP hostname or local IP address of the branch unit which local extensions (phones) can reach.
Branch SIP port	Enter the SIP server port number of the branch unit which local extensions (phones) can reach. The range is from 1 to 65535. The default is 5060.

GUI field	Description
SIP phone registration interval	To keep the extension registration status with the main office unit, enter the extension registration time interval (in minutes) as required by the FortiVoice phone system. The range is from 1 to 120 minutes. The default is 30 minutes.
SIP phone subscription interval	To keep the extension subscription status with the main office unit, enter the extension subscription time interval (in minutes) as required by the FortiVoice phone system. The range is from 1 to 120 minutes. The default is 60 minutes.
Emergency call	Choose how to handle EMS calls. The recommendation is to choose the branch unit to make sure calls are routed to the correct locations due to regional or international boundaries. • **Handled by Branch**: The branch office intercepts the EMS call and sends it out on one of the local lines. • **Handled by Central**: The main office handles the EMS call based on its configuration.
Central trunk fallback to branch	If the main office fails to process a call (for example, all lines busy or trunk down) and you want the branch office unit to locally handle the call, then select this option. To create an outbound call route for the branch office unit to handle this failover scenario, see Creating an outbound call route for failover scenarios.
External caller ID option	Select one of the following options: • **Use Default Caller ID**: This is the caller ID associated with the extension. • **Use Branch Caller ID**: If you select this option, you must fill in the next field (**External caller ID**).
External caller ID	If you select the **Use Branch Caller ID** option, then enter the external caller ID. Use the `name<phone_number>` format, such as `HR<222134>`.
Phone directory option	Select one of the following phone directories: • **Branch directory** • **System directory**
Local call handling	Select how you want local calls to be handled: • **Handled by branch** • **Handled by central**
Branch failover trunk FXO ports	This option only activates when you edit a survivability branch. Enter the trunk FXO ports to be used for outbound calls in the event of a failover scenario. For a port range, enter the starting and ending ports separated by a dash. For separate ports, use a comma. Port list example: 1-4,6.

GUI field	Description
	 **Branch failover trunk FXO ports** is applicable for all FortiVoice LSG models except FVE-100F and FVE-500F (and FVE-100E which is still supported but have reached the end-of-order [EOO] date).
Branch WSS port	Enter a WebSocket Secure (WSS) port to allow the FortiVoice LSG unit to support the FortiFone softclient for desktop application. The default port is 8089.
Branch HTTPs port	Enter an HTTPs port for the endpoint devices at the branch office to use. The default port is 443.
Branch extensions	Select extensions to add to the branch.
Gateway	The FortiVoice LSG solution can support a FortiVoice FXS, FXO, or PRI gateway at the branch office. To select a deployed FortiVoice gateway: 1. Click **+**. 2. Select the gateway. 3. Click **Close**. For details about how to deploy an FXS, FXO, or PRI gateway, see FortiVoice FXS Gateway Deployment Guide, FortiVoice FXO Gateway Deployment Guide, or FortiVoice PRI Gateway Deployment Guide.
Branch Paging	Options in this section are only available when you edit a survivability branch. If you want your deployment to use branch paging, you can complete the configuration later in Branch paging on page 46.  Branch paging using an FXO port is applicable for all FortiVoice LSG models except FVE-100F and FVE-500F (and FVE-100E which is still supported but have reached the end-of-order [EOO] date).
Speed Dial Rule	This option is only available when you edit a survivability branch. You can access details about this option later in Configuring a speed dial pattern and rule for branch paging on page 50.

4. Click **Create**.
   You have completed this procedure.
5. Go to Applying the branch configuration on page 29.

Applying the branch configuration

Use this procedure to apply the branch configuration from the main office FortiVoice phone system to the FortiVoice LSG unit and if present, its associated FortiVoice FXS, FXO, or PRI gateway.

Procedure steps

1. Connect to the GUI of the primary FortiVoice phone system at the main office.
2. Go to **Managed System > Survivability**.
3. On the **Survivability Branch** tab, select the branch to which you want to apply the configuration.
4. Click **Actions** > **Apply Configuration**.
   If a gateway is not linked to a survivability branch, a dialog box displays the following message:
   Do you want to update the selected gateway?
   If a gateway is linked to a survivability branch, a dialog box displays the following message:
   Do you want to apply the configuration to both the selected LSG and associated gateway?
5. To confirm, click **OK**.
   When the configuration changes are complete, a dialog box displays the following message:
   The gateway update is complete.
6. Click **OK**.
   You have completed this procedure.
7. Go to Verifying the heartbeat status on page 30.

Verifying the heartbeat status

Use this procedure to verify that the heartbeat between the FortiVoice LSG unit at the branch office and the FortiVoice phone system at the main office is healthy.

Procedure steps

1. Connect to the GUI of the FortiVoice LSG unit at the branch office
2. Go to **Dashboard**, and click the **Console** tab.
   The Console window opens.
3. To connect, click anywhere in the console window.
   The Console window shows a system prompt.
4. Enter the following command:
   `diagnose debug application proxyd status summary`
5. Review the system output.
   The following system output is an example:

```
System Time: 2019-11-04 10:06:53 EST (Uptime: 3d 19h 5m)
200 OK
Status:: mode: proxy (local survival is enabled), central office status=up, call handle location=central
```

6. If the system output shows **central office status=up**, then you have completed this procedure. To disconnect from the console session, enter `exit`. Go to Connecting the phones to the network on page 31.
   If the system output shows **central office status=down**, you need to troubleshoot the setup. You can start by verifying the IP address and port configuration (see Configuring administrator and network settings on page 20 and Adding a survivability branch on page 25) and the heartbeat status again. Make sure that the heartbeat between the FortiVoice LSG unit at the branch office and the FortiVoice phone system at the main office is healthy before connecting the phones to the network. To disconnect from the console session, enter `exit`.

Connecting the phones to the network

If you connected the phones too early in the FortiVoice LSG workflow, you must restore the phones to their factory default settings. For details about restoring factory default settings, see the documentation for your phone.

Connect the phones to the network at the branch office. For more details, see the documentation for your phone.

The phones automatically detect the branch office and are redirected to the main office FortiVoice phone system to retrieve their configuration files.

FortiVoice Gateway configuration

This section introduces how to configure a FortiVoice Gateway to add analog or PRI phone lines to your FortiVoice LSG unit at the branch office.

The FortiVoice LSG solution supports the following gateways at the branch office:

- FortiVoice Gateway GO08 and GO04, a foreign exchange office (FXO) gateway. For deployment details, see the FortiVoice FXO Gateway Deployment Guide.
- FortiVoice Gateway GS16, GS04, and GS24, a foreign exchange subscriber (FXS) gateway. For deployment details, see the FortiVoice FXS Gateway Deployment Guide.
- FortiVoice Gateway GT01 and GT02, primary rate interface (PRI) gateways. For deployment details, see the FortiVoice PRI Gateway Deployment Guide.

You must complete the following tasks in sequence:

- Associating a gateway to a survivability branch on page 32
- Setting up an office peer trunk on page 34
- Creating a local VoIP trunk on page 36
- Adding dial plans on page 40

Associating a gateway to a survivability branch

Set up a trunk between the gateway and the FortiVoice LSG unit at the branch office to directly route calls between the gateway and the extensions on the FortiVoice LSG unit. A gateway in a local survivability branch is managed by the primary FortiVoice phone system at the main office.

Prerequisite

- In the Deployment on page 17, complete tasks 1 to 11.
- Disable your gateway's cloud mode by going to Dashboard > Managed Device > Cloud Mode on the GUI of your gateway.

For details on gateway deployment, see the following guides:

- FortiVoice FXO Gateway Deployment Guide
- FortiVoice FXS Gateway Deployment Guide
- FortiVoice PRI Gateway Deployment Guide

Procedure steps

1. Connect to GUI of the primary FortiVoice phone system at the main office.
2. Go to **Managed System > Gateway**.
3. Select the type of gateway (FXO, FXS, or PRI) that you want to associate with the local survivability branch.

4. Click **New**, then configure the following settings:

GUI field	Description
Enabled	Select to activate the configuration of the gateway.
Name	Enter a unique name to identify the gateway.
Display name	Not required. You can leave this field empty.
Host name/IP address	Enter the hostname or IP address of the gateway. If the gateway is configured to use a non-default HTTPS port, then add :<port number> after the IP address. For example, 192.168.1.21:4430. **Get Device Information**: • Before you click this button, make sure to enter the required information in the **Admin user name** and **Admin password** fields below. • When clicking this button, both the serial number and MAC address are fetched and populated in the corresponding fields. **Connect Device**: This procedure does not use this button. With this button, you would access the FortiVoice Gateway GUI in a separate tab in your web browser.
Admin user name	Enter the user name of the administrator account used for logging in to the gateway. The default is admin.
Admin password	Enter the password associated with the Admin user name. To show the password, click the eye icon  . The default is no password.
Serial number	The serial number of the gateway that you are adding to the local survivability branch.
Type	Choose the type of gateway (FVG-GO04, GO08, GS04, GS16, GS24, GT01, or GT02) that you are adding to the local survivability branch.
MAC address	Enter the MAC address of the gateway that you are adding to the FortiVoice LSG unit.
Survivability branch	Select the current FortiVoice LSG unit to be linked to this gateway.
Physical location	Select **Internal** if the gateway and the local survivability branch are on the same LAN. The gateway connects to the internal IP address of the local survivability branch. Select **External** if the gateway connects to the local survivability branch with an external IP.
Description	Optionally, add any applicable notes for this gateway.

5. Click **Create**.
6. You have completed this procedure. You can now go to Setting up an office peer trunk on page 34.

Setting up an office peer trunk

Set up an office peer trunk between the central office and your branch office to transfer calls from your branch office to a central office or another branch office through a gateway. For details on office peers, see the FortiVoice Phone System Administration Guide.

The office peer trunk setup is only required if you use the following gateways in the branch office:

- GO04, GO08
- GT01, GT02

To set up an office peer trunk, you must meet the following requirements:

- Complete Associating a gateway to a survivability branch on page 32.
- Select **Partially managed** for **Management Mode** when adding a survivability branch. For details, see Adding a survivability branch on page 25.
- Select **Handled by branch** for **Local call handling**. For details, see Adding a survivability branch on page 25.

Procedure steps

1. Connect to the GUI of the primary FortiVoice phone system at the main office.
2. Go to **Trunk > Office Peer**.
3. Click **New**.
4. For **Office peer type**, select **Remote Access**.
5. Select **Satellite** for the role of the office peer.
6. If you want to change your local number pattern, click the **Edit** icon beside **Local/incoming digit pattern** to modify it.
7. Review the basic **New office peer information**, click **Next**.
8. Configure the following:

GUI field	Description
Enabled	Select to activate the trunk.
Name	Enter a name for the trunk.
Display name	Enter the trunk name displaying on the extension.
Peer Configuration	
Central Host/IP	Enter the domain name or IP address of the primary FortiVoice unit at the main office.
Port	Enter the port number for VoIP network on the primary FortiVoice unit.
User name	To authenticate the FortiVoice units forming the office peer trunk, enter the **User name**. This name must be the same on both units. The FortiVoice unit on each end will use this user name to authenticate each other.
Password	To authenticate the FortiVoice units forming the office peer trunk, enter the **Password**. This password must be the same on both units. The FortiVoice unit on each end will use this password to authenticate each other.

GUI field	Description
Outgoing digit pattern	Click the **Edit** icon if you want to modify the digit pattern of the outgoing dial plan for the main and branch offices.
Advanced	
Local/incoming digit pattern	Click the **Edit** icon if you want to modify the digit pattern of the local/incoming dial plan for the main and branch offices.
Call routing	Select the call routing plan as required.
Directory	Select this option and click **Fetch now** to obtain the phone directory from the branch office peer. This option only works if the same option is selected on the branch office peer's FortiVoice unit. You can view the directory by going to **Monitor > Directory** and selecting this office in the **Location** field.
Share metric	Enter the hop count value for this FortiVoice unit to share the phone directory with the branch office peer. Example 1: You have configured the following deployment: • A and B are office peers. • A and C are office peers. If you want A, B, and C FortiVoice systems to share their phone directories, enter 2 on all three FortiVoice systems. Example 2: If your enter 1, the directory can only be shared with the first peer office site designated on the routing table of this FortiVoice unit.
SIP settings	Select the SIP profile for the trunk. You can edit the existing profile or click **New** to add a new one.
Max channel	Enter the maximum voice channels for the trunk. This field accepts a value in the range of 1 to 450 inclusive.
More	This feature is used for remote access office peer connection through a proxy server.
DNS SRV record	The DNS service (SRV) record provides host and port information for specific services such as voice over IP (VoIP). SIP needs to connect to a specific port on a specific server. Enable this option to allow the FortiVoice unit to query the DNS SRV record for the IP address and port number of the central FortiVoice unit (office peer) to register.
Proxy	To connect to the central office peer through a proxy server, do the following: • If you have enabled **DNS SRV record**, enable **Proxy** and enter the unique hostname of the central office peer in the **(Host/IP)** field. The DNS SRV record will use the information to look for and provide the IP address and port number of the central office peer. • If you do not want to use the **DNS SRV record** service and therefore did not enable it, enable **Proxy** and enter the unique hostname of the central office peer in the **(Host/IP)** field. Also select the port number and communication protocol for the central office peer. The DNS server will use the information to look for and provide the IP address of the central office peer.

GUI field	Description
	• If you know the IP address of the central office peer, enter it in the **(Host/IP)** field. In this case, you do not need to enable **DNS SRV record**.
Registration interval	Select the time (in seconds) needed for your FortiVoice unit to register to the central office peer until it receives a response.

9. Click *Create*
10. You have completed this procedure. You can now go to Creating a local VoIP trunk on page 36.

Creating a local VoIP trunk

Create a VoIP trunk for inbound and outbound calls at the branch office.

The office peer trunk setup is only required if you use the following gateways in the branch office:

- GO04, GO08
- GT01, GT02

To create a VoIP trunk, you must meet the following requirements:

Prerequisite

- In the Deployment on page 17, complete tasks 1 to 11.
- Select **Partially managed** for **Management Mode** when adding a survivability branch. For details, see Adding a survivability branch on page 25.
- Select **Handled by branch** for **Local call handling**. For details, see Adding a survivability branch on page 25.

Procedure steps

1. Connect to the GUI of the FortiVoice LSG unit.
2. Go to **Trunk > VoIP > SIP.**
3. Click **New**.
4. Configure the following:

GUI field	Description
Enabled	Select to activate the SIP trunk.
Name	Enter a name for this trunk such as the name of the VoIP service provider.
Display name	Enter your caller ID that will appear on the called phone, such as Example Company. For details about the caller ID hierarchy, see the Caller ID modification section in the FortiVoice Cookbook.
Main number	Enter the phone number provided by the VoIP service provider.
SIP Setting	
SIP server	Enter the VoIP provider's IP address or domain name. For example, `172.20.120.11` or `voip.example.com`.

GUI field	Description
SIP port	Most SIP configurations use TCP or UDP port 5060 for SIP sessions. If your VoIP service provider uses a different port for SIP sessions, enter the port number. If you select the **Using SRV record** option, this field is greyed out.
Using SRV record	If you entered the VoIP provider's domain name in the **SIP server** field, select this option to translate the domain name and obtain the SIP port. You can only select this option if your VoIP provider uses the same setting.
User name	Enter the user name provided by the VoIP service provider for the FortiVoice LSG unit to register with the SIP server.
Password	Enter the password provided by the VoIP service provider for the FortiVoice LSG unit to register with the SIP server.
Auth. user name	Some VoIP providers may provide you with an authentication user name that is different from your user name for the FortiVoice LSG unit to register with the SIP server. If that is the case, enter the authentication user name here.
Realm/Domain	Some VoIP service providers' SIP servers authenticate the PBXes that register with them by requesting the name of the host performing the authentication. If this is the case with your VoIP service provider, enter the name of the host performing the authentication provided by your VoIP service provider.
SIP settings	Select the SIP profile to apply the supported phone features and codecs for the trunk. To match the information of the VoIP service provider, you can edit the existing profile or click + to add a new one.
Max channel	Each trunk contains multiple channels. The number of channels you can have in a trunk is controlled by your VoIP service provider. This number displays under line appearance option when you configure programmable phone keys for phone profiles. Consult your VoIP service provider for the maximum of channels that you can set to limit the number of concurrent calls. For example, if you want to allow six calls at a time, enter 6. The value range is from 1 to 450.
Overflow check	If selected, the phone calls exceeding the **Max channel** limit will be handled according to the call handling actions set in the dialplan applied to this trunk. If unselected, the phone calls exceeding the **Max channel** limit will be disconnected.
Max outgoing channel	With known max channels, if you need to reserve incoming channels, you may enter the number of outgoing channels allowed and the remaining channels are for incoming calls. For example, if the max channel number is 10 and you want to reserve 4 channels for incoming calls, then you can enter 6 for **Max outgoing channel**. The value range is from 0 to 2000.
User=Phone in SIP URI	Select if your service provider requires this option to make the FortiVoice LSG unit to be compatible with the VoIP service provider's configurations.
Inband ringtone (Early media)	Select to enable the FortiVoice LSG unit to send ring tone to the caller of an incoming call before the establishment of a call connection.

GUI field	Description
Caller ID Option	Configure how to display your caller ID to meet the different requirements and scenarios of the service providers. Caller ID information is contained in the From header and P-Asserted-Identity header of SIP packets sent to the called phone's PBX. **From header**: The From header field indicates the identity of the initiator of the call request from the point of view of the PBX server. • SIP user name: Select if you want the user name provided by the VoIP service provider for the FortiVoice LSG unit to register with the SIP server to appear on the called phone. See User name on page 37. • Caller ID priority rule: Select if you want to configure your FortiVoice caller ID according to the FortiVoice caller ID priority hierarchy. For more information, see the FortiVoice Phone System Administration Guide. • Main number: Select if you want the trunk main number to appear on the called phone. See Main number on page 36. • Specified: Enter the ID you want to display on the called phone in the format of `display name <number>`. **P-Asserted-Identity header**: This header contains the caller ID information for the call on the INVITE SIP packet. • No PAI header: Select if you want to disable PAI header. • Caller ID priority rule: Select if you want to configure your FortiVoice LSG unit's caller ID according to the FortiVoice caller ID priority hierarchy. For more information, see the FortiVoice Phone System Administration Guide. • Main number: Select if you want the trunk main number to appear on the called phone. See Main number on page 36. • Specified: Enter the ID you want to display on the called phone in the format of `display name <number>`. **Diversion Header Use**: Allows you to set the use of the diversion header for call twinning, call forwarding, or normal outbound calls. • On Redirect: Use the diversion header during call twinning and call forwarding. • No Diversion Header: Disable the use of the diversion header for all calls. • Always: Allow the diversion header to be applied to all calls. **Diversion Header Source**: • DID Mapping: Use the mapped DID if available, then use the caller ID (CID) of the main trunk. • Trunk Caller ID: Use the caller ID of the main trunk.
Registration	
Type	Enter the SIP registration information from the VoIP service provider by selecting a registration method in **Type**. You can receive calls after registering with the SIP server of the VoIP service provider. • **Disable**: Select to deactivate the registration with the VoIP service provider. • **Standard**: Select to use the standard registration method which automatically registers with the SIP server of the VoIP service provider. Enter the registration interval in minutes. • **Registration URI**: Enter the registration string provided by the VoIP service provider. The string in Registration URI has the following format:

GUI field	Description

	`<user>@<host><:port>`
	where `<user>` is the user name.
	`<host>` is a hostname, domain name, FQDN, or IP address.
	`<:port>` is the port number. If you omit to specify a port, the default port (5060) is used.
	Examples:
	`support@mycompany.com`
	`support@mycompany.com:6000`
	`bob@168.176.248.255`
	• **Registrar**: Select to enter the registration information from the VoIP service provider:
	  • **Registrarhost/IP**: Enter the VoIP service provider's SIP registration server domain name or IP address. For example, `172.20.120.11` or `voip.example.com`.
	  • **Registrar port:** Most SIP configurations use TCP or UDP port 5060 for SIP sessions. If your VoIP service provider uses a different port for SIP sessions, enter the port number.
	  • **Transport protocol**: Select the transport protocol used for the registration.
	  • **Registration interval**: Enter the registration interval with the SIP server in minutes.

Outbound Proxy	Some VoIP service providers use proxy servers to direct its traffic. If this is the case, your registration request will go to the proxy server first before reaching the registration server. Configure the following: • Select to activate the proxy server setting. • **Proxy (Host/IP)**: Enter the proxy server's domain name or IP address. For example, `172.20.120.11` or `voip.example.com`. • **Proxy port**: Enter the port number of the proxy server. • **Transport protocol**: Select the transport protocol used for the registration.
Fax	
Automatic fax detection	 Selecting this option may cause the following behaviors: • Delay the call response time on this trunk by automatically adding two ring tones to detect incoming fax signals. • Affect toll charges on incoming lines. Select for the FortiVoice LSG unit to detect incoming fax signal on this trunk automatically.
Forward to DID mapping extension	This option is available when you select **Automatic fax detection**. Select this option if a DID number is mapped directly to an extension to receive voice and fax calls. Faxes will be sent to the extension's personal fax account, accessible through the FortiVoice User Portal. In **Forward to eFax account** (next field), select an eFax account. Should a fax fail to be received by the DID mapping extension, the FortiVoice unit will use this eFax account as a fallback.

GUI field	Description
Forward to eFax account	This option is available when you select **Automatic fax detection**. Select or edit an eFax account to receive faxes. To add a new eFax account, click +.
Phone Number	Adding a phone number in this field is optional and for information purposes only. The phone number supports digits from 0 to 9 and a maximum of 63 digits. Click **New** to add a phone number provided by your VoIP service provider. Click **Create** when done. You can add multiple phone numbers.

5. Click **Create**.
6. You have completed this procedure. You can now go to Adding dial plans on page 40.

Adding dial plans

Add dial plans to define how to route calls between the branch office and the main office.

Dial plans are required if you use the following gateways in the branch office:

- GO04, GO08
- GT01, GT02

Prerequisite

- In the Deployment on page 17, complete tasks 1 to 11.

This section includes:

Adding an inbound dial plan for calls from the branch to the main office

1. Connect to the GUI of the FortiVoice phone system at the main office.
2. Go to **Call Routing > Inbound > Inbound**.
3. Click **New** and configure the following:

GUI field	Description
Enabled	Select to activate this dial plan.
Name	Enter a name for this plan.
From Trunk	Select the FortiVoice LSG trunk for the incoming calls that are subject to this dial plan. Click + and select the trunk. Click **Close**.

GUI field	Description
Dialed Number Match	 If you configure **Dial Local Number on page 42**, FortiVoice ignores this **Dialed Number Match** setting. With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers. When a called number matches this pattern, FortiVoice follows the dial plan rule that you configure in **Call Handling on page 41** (**Endpoint Action** or **Call Routing**). Create the number match by following the pattern-matching syntax you have configured. For more information on FortiVoice-supported pattern-matching syntax and examples, see the FortiVoice Phone System Administration Guide.
Caller ID Match	Click **New** to set the caller ID pattern following the pattern-matching syntax you have configured for this dial plan, and click **Create**. For more information on FortiVoice-supported pattern-matching syntax and examples, see the FortiVoice Phone System Administration Guide. You can enter an incoming call's display name string or the caller's phone number string as the pattern. Click **Export** to open or save the caller ID match file and **Import** to browse for a caller ID match file. Caller IDs under this pattern are subject to this plan.
Caller ID Modification	Click + and select one or more caller ID modification configurations. Click **Close**. You can associate multiple caller ID modification configurations with a dial plan.
Call Handling	Select the actions to process the incoming calls with matched dialed numbers and/or caller IDs.
Action type	Select the type of action for the plan and configure the actions accordingly.
Endpoint Action	Select if you want to send incoming calls to the main office according to operation schedules. For example, send calls to the voicemail after business hours. To configure this action type: 1. In **Action type**, select **Endpoint Action**. 2. Click **New**. 3. Select the **Schedule** for the action. 4. Select an **Action** for the incoming calls under this plan. For some actions, you need to enter the extension (such as **Go voicemail**) or select a profile (such as **Play announcement**). 5. Click **Create**. 6. If you need more actions for this action type, repeat this procedure. To avoid schedule conflicts, do not use the same schedule for more than one action.

GUI field	Description
Dial Local Number	 When you configure this **Dial Local Number** setting, FortiVoice ignores the **Dialed Number Match on page 41**. Select this action type if you want to send incoming calls to the main office at any time. For example, you can enter 222XXXX as a pattern and strip 222. The FortiVoice unit will only dial the last four digits for all called numbers matching the pattern. To configure this action type: 1. In **Action type**, select **Dial Local Number**. 2. Click **New**. 3. Add a number pattern in **Match Pattern** following the pattern-matching syntax you have configured for this dial plan. Repeat to add more patterns. 4. For **Strip**, enter a number to omit dialing the starting part of a pattern. 0 means no action. For example, if your **Match Pattern** is 222XXXX and **Strip** is 3, the FortiVoice unit will only dial the last four digits for all called numbers matching the pattern. 5. For **Prefix**, add a number before a pattern. For example, if your **Match Pattern** is 9XXX and the numbers under this pattern have been upgraded to have an additional digit 5 at the beginning, you can enter 5 for the **Prefix**. When an incoming call matches the pattern, the FortiVoice unit will add a 5 before the number. 6. For **Postfix**, add a number after a pattern. For example, if your **Match Pattern** is 9XXX and the numbers under this pattern have been upgraded to have an additional digit 5 at the end, you can enter 5 for the **Postfix**. When an incoming call matches the pattern, the FortiVoice unit will add a 5 after the number. 7. Click *Create*.

4. Click **Create**.
5. You have completed this procedure. You can now go to Adding an inbound dial plan for calls from the gateway to the branch office on page 42.

Adding an inbound dial plan for calls from the gateway to the branch office

1. Connect to the GUI of the FortiVoice ISG unit at the branch office.
2. Go to **Call Routing > Inbound > Inbound**.
3. Click **New** and configure the following:

GUI field	Description
Enabled	Select to activate this dial plan.
Name	Enter a name for this plan.
From Trunk	Select the gateway trunks of the incoming calls that are subject to this dial plan.

GUI field	Description
	Click + and select the trunks. Click **Close**.
Dialed Number Match	 If you configure **Dial Local Number on page 43**, FortiVoice ignores this **Dialed Number Match** setting. With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers. When a called number matches this pattern, FortiVoice follows the dial plan rule that you configure in **Call Handling on page 43** (**Endpoint Action** or **Call Routing**). Create the number match by following the pattern-matching syntax you have configured.
Caller ID Match	Click **New** to set the caller ID pattern following the pattern-matching syntax you have configured for this dial plan, and click **Create**. You can enter an incoming call's display name string or the caller's phone number string as the pattern. Click **Export** to open or save the caller ID match file and **Import** to browse for a caller ID match file. Caller IDs under this pattern are subject to this plan.
Caller ID Modification	Click + and select one or more caller ID modification configurations. Click **Close**. You can associate multiple caller ID modification configurations with a dial plan.
Call Handling	Select the actions to process the incoming calls with matched dialed numbers and/or caller IDs.
Action type	Select the type of action for the plan and configure the actions accordingly.
Endpoint Action	Select if you want to send incoming calls to the branch office according to operation schedules. For example, send calls to the voicemail after business hours. To configure this action type: 1. In **Action type**, select **Endpoint Action**. 2. Click **New**. 3. Select the **Schedule** for the action. 4. Select an **Action** for the incoming calls under this plan. For some actions, you need to enter the extension (such as **Go voicemail**) or select a profile (such as **Play announcement**). 5. Click **Create**. 6. If you need more actions for this action type, repeat this procedure. To avoid schedule conflicts, do not use the same schedule for more than one action.
Dial Local Number	 When you configure this **Dial Local Number** setting, FortiVoice ignores the **Dialed Number Match on page 43**.

GUI field	Description
	Select this action type if you want to send incoming calls to the branch office at any time. For example, you can enter 222XXXX as a pattern and strip 222. The FortiVoice unit will only dial the last four digits for all called numbers matching the pattern. To configure this action type: 1. In **Action type**, select **Dial Local Number**. 2. Click **New**. 3. Add a number pattern in **Match Pattern** following the pattern-matching syntax you have configured for this dial plan. Repeat to add more patterns. 4. For **Strip**, enter a number to omit dialing the starting part of a pattern. 0 means no action. For example, if your **Match Pattern** is 222XXXX and **Strip** is 3, the FortiVoice unit will only dial the last four digits for all called numbers matching the pattern. 5. For **Prefix**, add a number before a pattern. For example, if your **Match Pattern** is 9XXX and the numbers under this pattern have been upgraded to have an additional digit 5 at the beginning, you can enter 5 for the **Prefix**. When an incoming call matches the pattern, the FortiVoice unit will add a 5 before the number. 6. For **Postfix**, add a number after a pattern. For example, if your **Match Pattern**is 9XXX and the numbers under this pattern have been upgraded to have an additional digit 5 at the end, you can enter 5 for the **Postfix**. When an incoming call matches the pattern, the FortiVoice unit will add a 5 after the number. 7. Click *Create*.

4. Click **Create**.
5. You have completed this procedure. You can now go to Adding an outbound dial plan for calls from the branch office to the main office on page 44.

Adding an outbound dial plan for calls from the branch office to the main office

Configure dial plans for outgoing calls from the branch office to the main office.

You can create one extension number pattern in your dial plan that matches many different numbers for outbound calls to the main office.

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

Procedure steps

1. Connect to the GUI of the FortiVoice LSG unit.
2. Go to **Call Routing > Outbound > Outbound.**
3. Click **New**.

4. Configure the following:

GUI field	Description
Enabled	Select to activate this dial plan.
Name	Enter a name for this plan.
Emergency Call	Select to allow emergency call with this plan. By default, this is selected.
Retain original caller ID	Select to keep the original caller ID.
Caller ID Match	Enter the caller ID pattern following the pattern-matching syntax you have configured for this dial plan. For more information on FortiVoice-supported pattern-matching syntax and examples, see the FortiVoice Phone System Administration Guide. Click + if you need to enter more caller ID patterns. You can enter the caller's phone number string as the pattern. Callers with IDs under this pattern are subject to this plan.
Dialed Number Match	With dialed number pattern matching, you can create one phone number pattern in your dial plan that matches many different numbers for outbound calls to the main office. The dialed numbers matching this pattern will follow this dial plan rule.
Call Handling	Click *New* to configure the call handling action for the numbers matching the configured number pattern and the caller IDs matching the caller ID pattern.

5. Click **Create**.

Branch paging

The FortiVoice phone system and FortiVoice LSG solution can work with a paging system to allow you to send an audio announcement (page) to an overhead speaker system located at a branch office.

Branch paging using an FXO port is applicable for all FortiVoice LSG models except FVE-100F and FVE-500F (and FVE-100E / FVE-1-000E which are still supported but have reached the end-of-order [EOO] date).

This section lists procedures to configure branch paging using your FortiVoice phone system:

1. Configuring branch paging settings of a survivability branch on page 46
2. Configuring an account code and user privilege for branch paging on page 47
3. Configuring a speed dial pattern and rule for branch paging on page 50, optional
4. Applying the branch paging configuration on page 53

Configuring branch paging settings of a survivability branch

Use this procedure to edit a survivability branch to configure branch paging settings.

Prerequisite

In the Deployment on page 17, complete tasks 1 to 11.

Procedure steps

1. Connect to the GUI of the primary FortiVoice phone system at the main office.
2. Go to **Managed System > Survivability**.
3. On the **Survivability Branch** tab, double-click the survivability branch that you want to edit.
4. Click **Survivability**.
5. Scroll to the bottom of the page and click **Branch Paging**.
6. Configure the following parameters:

GUI field	Description
FXO port	Enter the FXO port that the paging system is plugged in to at the branch office, if applicable.
Max duration	Enter the maximum duration for the branch paging session. When the maximum duration is reached, the branch paging session automatically ends. The duration range is from 0 to 64800 seconds.
Paging number	Enter the number to engage the paging system.

GUI field	Description
	For example, 0110.
Accept same branch paging	Select this option to allow all extensions at the same branch to connect to the paging system without a user privilege and complete a paging call.
Reject paging by default	Select this option to allow extensions at the same branch to connect to the paging system using a user privilege and account code, and complete a paging call.
Reject paging from other branch	Select this option to refuse paging calls from other branches.
Accept failover local paging	If the main office is down and you want to do paging from the branch office, select this option. **with authentication code**: This code is not required.

7. Click **OK**.
   You have completed this procedure.
8. If you selected the **Accept same branch paging** option, then go to Applying the branch paging configuration on page 53.
   If you selected the **Reject paging by default** option, then go to Configuring an account code and user privilege for branch paging on page 47.

Configuring an account code and user privilege for branch paging

Use this procedure to create an account code to restrict the access to a paging system at the branch office. Assign this account code to a user privilege and then apply this user privilege to a user extension. To engage the paging system, extension users must dial the configured paging number and then validate their access to the paging system by entering the access code (PIN) when prompted.

Prerequisite

In Configuring branch paging settings of a survivability branch on page 46, enable the **Reject paging by default** option.

Procedure steps

1. Create a paging account code:
   a. Connect to the GUI of the primary FortiVoice phone system at the main office.
   b. Go to **Security > User Privilege**, and then click the **Account Code** tab.
   c. Click **New**.
   d. In **Name**, enter a name to identify this account code. For example, PagingAccCode.
   e. In **Description**, add any notes for this account code by clicking Edit .
   f. Do not select **Shared**.
   g. In **Represented in CDR**, decide how you want to display the account code in the call detail record (CDR) by selecting **By Code** or **By Name**.
   h. Under **Access Code Set**, click **New**.

i. In **Code**, enter an access code. When the FortiVoice phone system prompts for a PIN (access code) after a user has engaged the paging system, the user enters this code.

Make sure that the access code has the following format:
- Numbers from 0 to 9. Other characters are not allowed.
- Minimum of 3 digits.
- Maximum of 10 digits.

Example: 8012

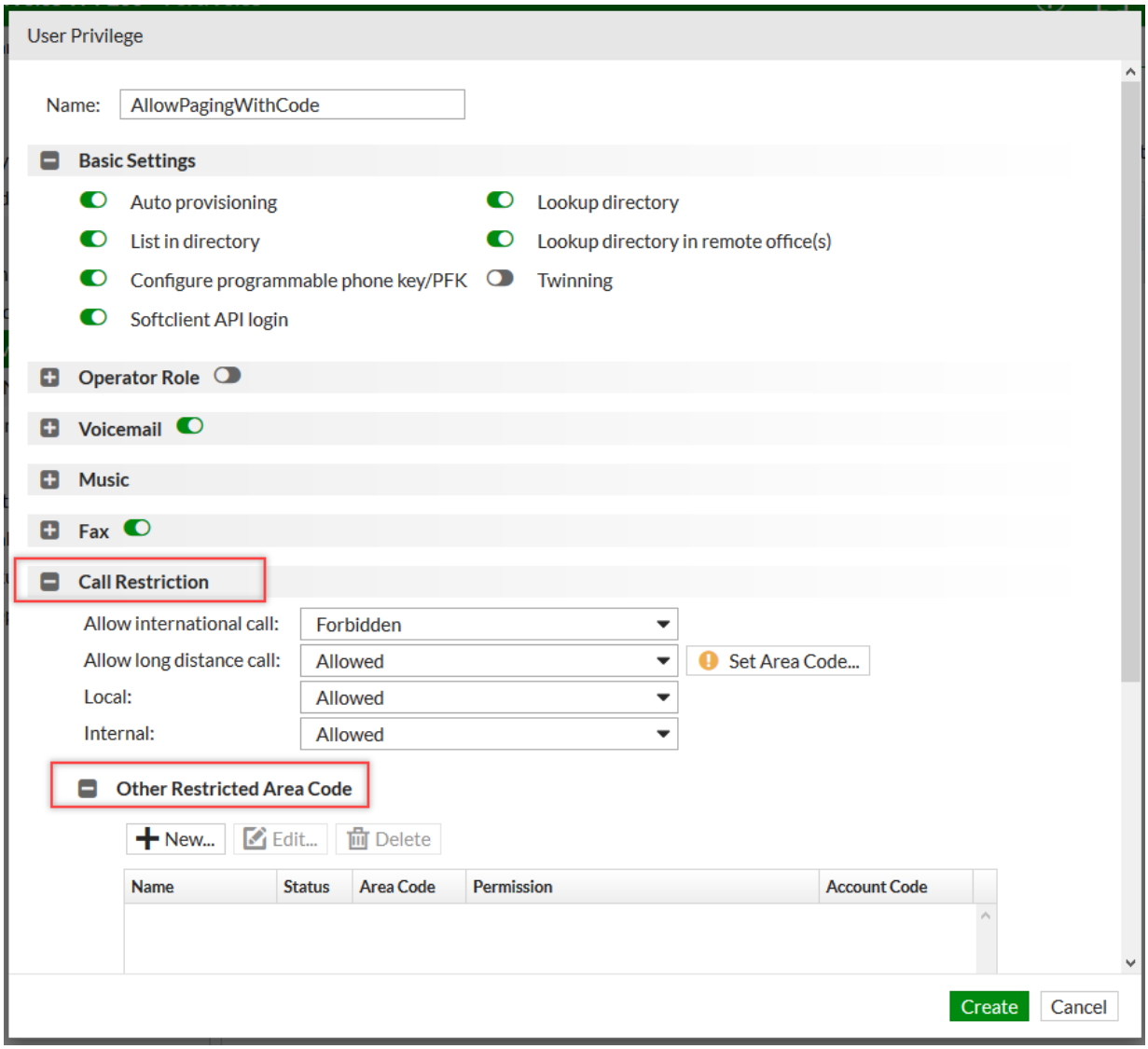
j. In **Display name**, enter a name for the access code. For example, PagingAccessCode.

k. In **Comments**, add any notes for the access code by clicking Edit .

l. To create the access code, click **Create**.

m. To create the account code, click **Create**.

2. Create a paging user privilege:
   a. Go to **Security > User Privilege**, and then click the **User Privilege** tab.
   b. Click **New**.
   c. In **Name**, enter a name to identify this user privilege. For example, AllowPagingWithCode.
   d. Click **Call Restriction** and then click **Other Restricted Area Code**.

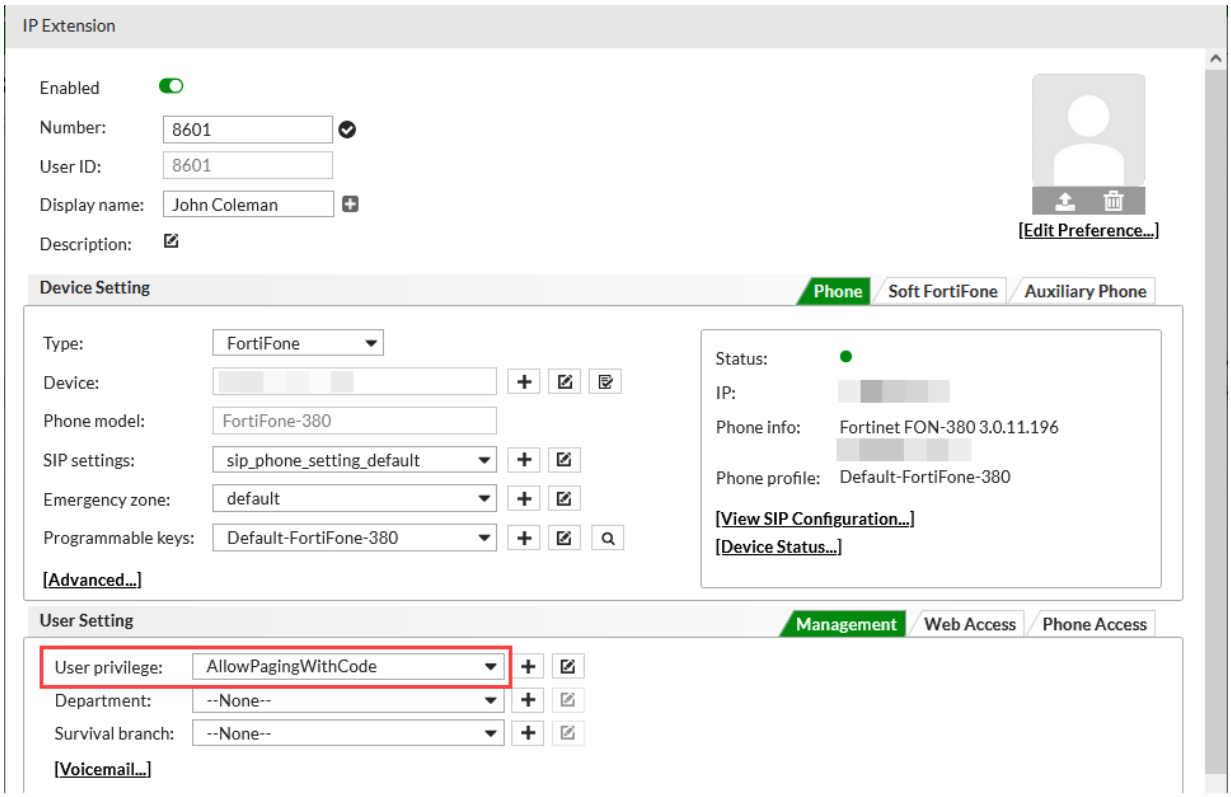


e. Click **New**.
f. To activate this restriction, make sure that **Enabled** is selected.
g. In **Name**, enter a name to identify this paging call restriction. For example, Paging.
h. In **Area code**, enter the paging number to be configured to engage the paging system. For example, 0110.

Make sure to use the same number as in the **Number** field (see Configuring branch paging settings of a survivability branch on page 46).

i. In **Permission**, select **Allowed with Account Code**.
j. In **Account code**, click + and select the account code that you created in step 1.
k. Click **Close**.
l. To create the call restriction, click **Create**.
m. To create the user privilege, click **Create**.

3. Apply the paging user privilege to one or more extensions:
   a. Go to **Extension > Extension**, and then click the **IP Extension** tab.
   b. Double-click the extension that you want to edit.
   c. Go to **User Setting**.
   d. In **User privilege**, select the paging user privilege that you created in step 2. In this example, you would select AllowPagingWithCode.



   e. Click **OK**.
   You have completed this procedure.
4. If you want your deployment to use paging zones, then go to Configuring a speed dial pattern and rule for branch paging on page 50.
   If your deployment does not require paging zones, go to Applying the branch paging configuration on page 53.

Configuring a speed dial pattern and rule for branch paging

By default, a paging announcement reaches users in a general area such as an airport, office building, school, or store. If you want a paging announcement to reach a specific area only, then use paging zones.

Optionally, use this procedure to configure the required speed dial pattern for zone paging and use this pattern in the speed dial rule.

Prerequisite

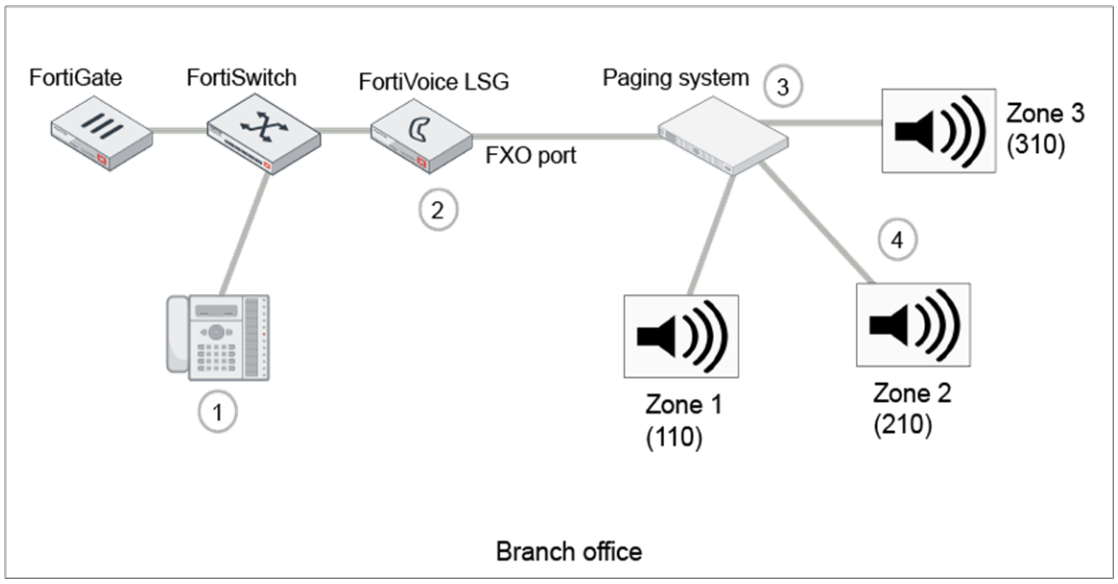
Complete Configuring an account code and user privilege for branch paging on page 47.

Example of paging settings

To illustrate the configuration of a speed dial pattern for branch paging, this procedure uses the following example settings:

- The speed dial pattern is set to *XXX.
- The mapped pattern is set to 0110, XXX.
- The building has three floors and each floor is a paging zone:
  - Paging zone 1 is identified with 110.
  - Paging zone 2 is identified with 210.
  - Paging zone 3 is identified with 310.

Example of a branch paging topology



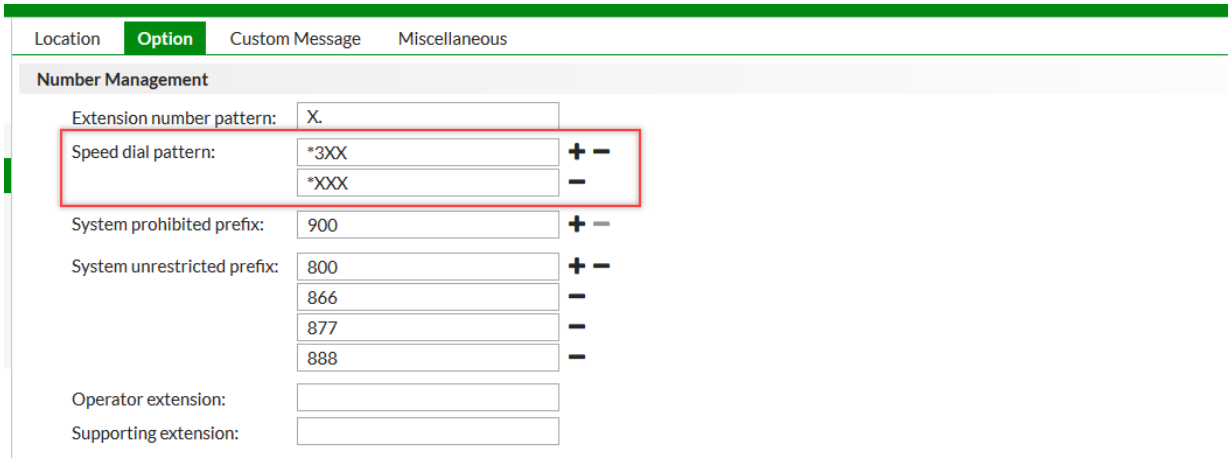
Using the branch paging topology example, the following table describes the sequence of events to deliver a paging announcement to zone 2:

1	• To page zone 2, lift the phone handset and dial *210. • If the FortiVoice phone system prompts you for a PIN (access code), enter the code.
2 and 3	• The FortiVoice LSG unit (2) communicates with the paging system (3). • At the prompt, speak to make the paging announcement.
4	• Users in zone 2 receive the paging announcement through the overhead speaker system. • To end the paging announcement, hang up the phone handset.

Procedure steps

1. Connect to the GUI of the primary FortiVoice phone system at the main office.
2. Set the speed dial pattern:
   a. Go to **Phone System > Setting**, and then click the **Option** tab.
   b. In **Speed dial pattern**, add a code. For example, *XXX.

The speed dial pattern supports the following characters:
- Numbers (0 to 9)
- Asterisk (*)
- Capital letter X
- Number sign (#)



3. Set the speed dial rule:
   a. Go to **Managed System > Survivability**.
   b. On the **Survivability Branch** tab, double-click the survivability branch to edit.
   c. Click **Survivability**.
   d. Scroll to the bottom of the page and click **Speed Dial Rule**.
   e. Click **New**.
   f. Configure the following parameters:

GUI field	Description
Name	Enter a name for the speed dial mapping.
Dialed Pattern	Enter a code for the speed dial pattern. This is the code that you added in step 2 b. Example, *XXX.
Mapped Pattern	The speed dial number is comprised of the following: • Digits used to engage the paging system. Example, 0110.  Make sure to use the same number as in the **Number** field (see Configuring branch paging settings of a survivability branch on page 46).

GUI field	Description
	• Digits for the speed dial pattern. Example, XXX. For example, 0110,XXX.
Description	Optionally, add a description for the speed dial rule.

4. Click **Create**.
5. To close the Speed Dial Rule dialog box, click **Close**.
6. To close the Survivability Settings dialog box, click **OK**.
7. To close the Survivability Branch dialog box, click **OK**.
   You have completed this procedure.
8. Go to Applying the branch paging configuration on page 53.

Applying the branch paging configuration

Use this procedure to apply the branch paging configuration from the main office FortiVoice phone system to the FortiVoice LSG unit and if present, its associated FortiVoice FXS, FXO, or PRI gateway.

Procedure steps

1. Connect to the GUI of the primary FortiVoice phone system at the main office.
2. Go to **Managed System > Survivability**.
3. On the **Survivability Branch** tab, select the branch to which you want to apply the configuration.
4. Click **Apply Configuration**.
   If a gateway is not linked to a survivability branch, a dialog box displays the following message:
   Do you want to update the selected gateway?
   If a gateway is linked to a survivability branch, a dialog box displays the following message:
   Do you want to apply the configuration to both the selected LSG and associated gateway?
5. To confirm, click **Yes**.
   When the configuration changes are complete and successful, a dialog box displays the following message:
   The gateway update is complete.
   Successful:<configured_branch_name>, <configured_FXS, FXO, or PRI_gateway, if applicable>.
6. Click **OK**.
   You have completed the configuration changes for branch paging.

www.fortinet.com