

Local Survivable Gateway Deployment Guide

FortiVoice 6.4.4



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/training-certification>

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



December 16, 2021

FortiVoice 6.4.4 Local Survivable Gateway Deployment Guide

26-644-586627-20211216

TABLE OF CONTENTS

Change log	4
Overview	5
Supported models	5
Topology	7
Call flows	8
Inbound call flow	9
Inbound call flow with a network impairment or failure	10
Outbound call flow	11
Outbound call flow when the branch office is down	12
Outbound call flow when the main office trunk is down	13
Outbound call flow for a 911 or emergency medical services call	14
Outbound call flow with a PSTN failover	15
Deployment	16
Connecting to the FortiVoice LSG unit	17
Configuring administrator and network settings	19
Upgrading the FortiVoice LSG firmware	21
Configuring the deployment mode	22
Configuring high availability	22
Adding or importing branch extensions	23
Adding a survivability branch	24
Applying the branch configuration	28
Verifying the heartbeat status	28
Connecting the phones to the network	29
Branch paging	30
Configuring branch paging settings of a survivability branch	30
Configuring an account code and user privilege for branch paging	31
Configuring a speed dial pattern and rule for branch paging	34
Applying the branch paging configuration	37

Change log

Date	Change description
2021-12-16	Initial release of the FortiVoice 6.4.4 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 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 the following benefits:

- Centralized management
 - The main office handles all inbound 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 on page 5](#)
- [Topology on page 7](#)

Supported models

The FortiVoice LSG models are:

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



The FortiVoice phone system continues to support FVE-1000E as a FortiVoice LSG model. However, this FortiVoice LSG model 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.

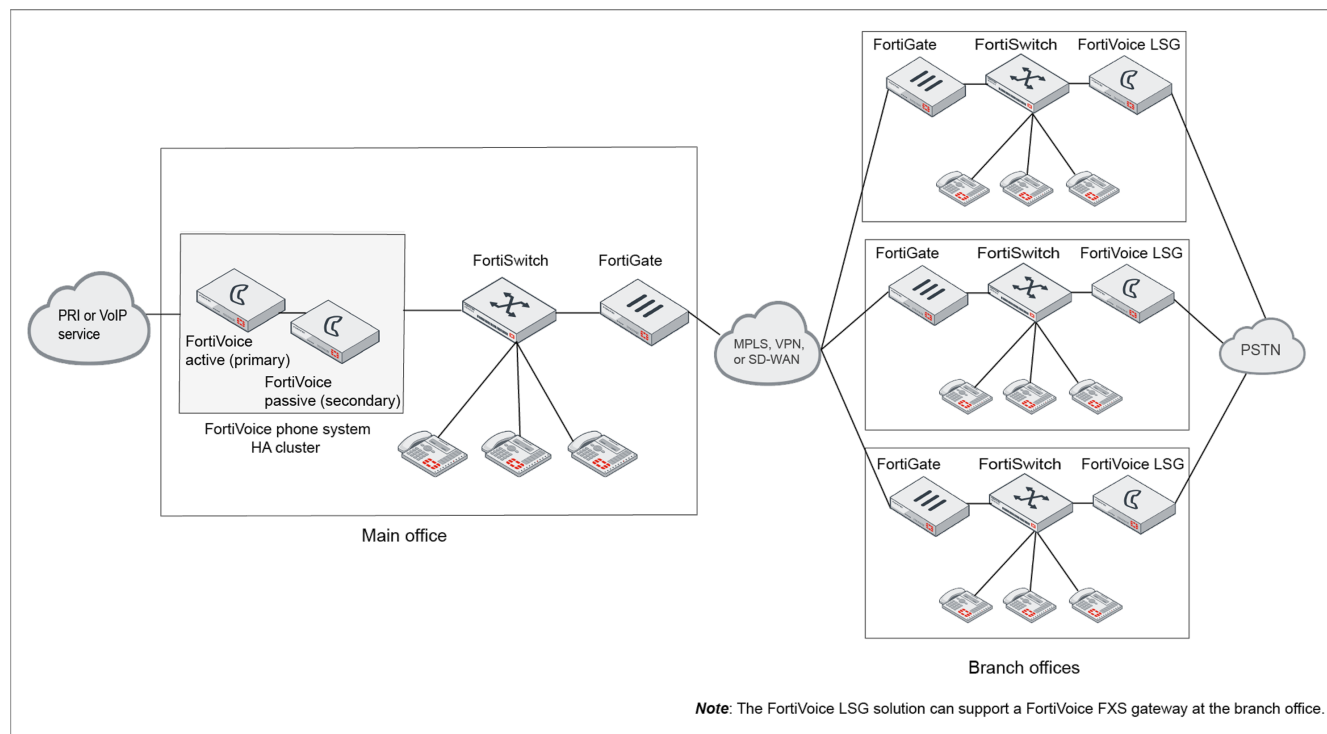
The main office manages configuration information for the branch phones and offices. The main office has the following management functions:

- 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 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:

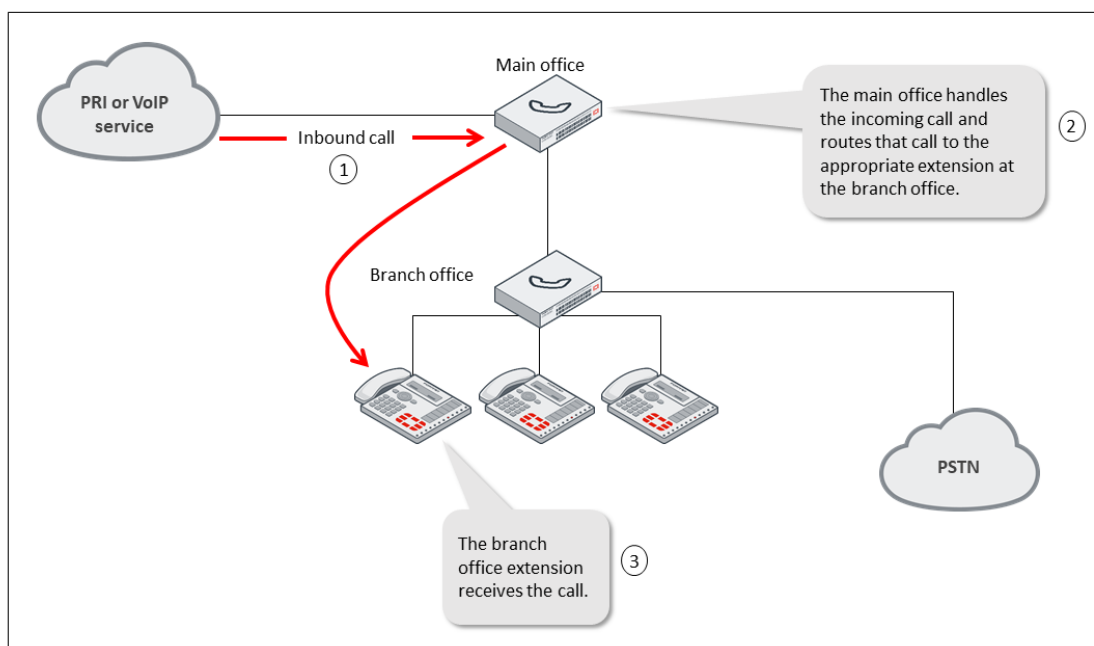
- [Inbound call flow on page 9](#)
- [Inbound call flow with a network impairment or failure on page 10](#)
- [Outbound call flow on page 11](#)
- [Outbound call flow when the branch office is down on page 12](#)
- [Outbound call flow when the main office trunk is down on page 13](#)
- [Outbound call flow for a 911 or emergency medical services call on page 14](#)
- [Outbound call flow with a PSTN failover on page 15](#)

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.

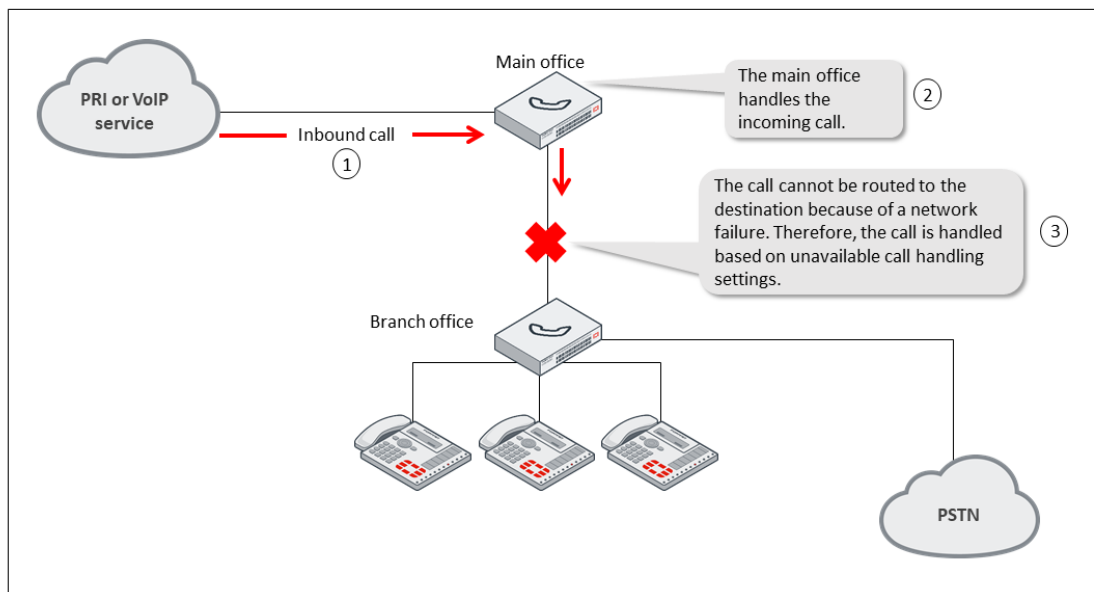


The main office sends Session Initiation Protocol (SIP) and Real Transport Protocol (RTP) traffic directly to the phone, not to the branch office.



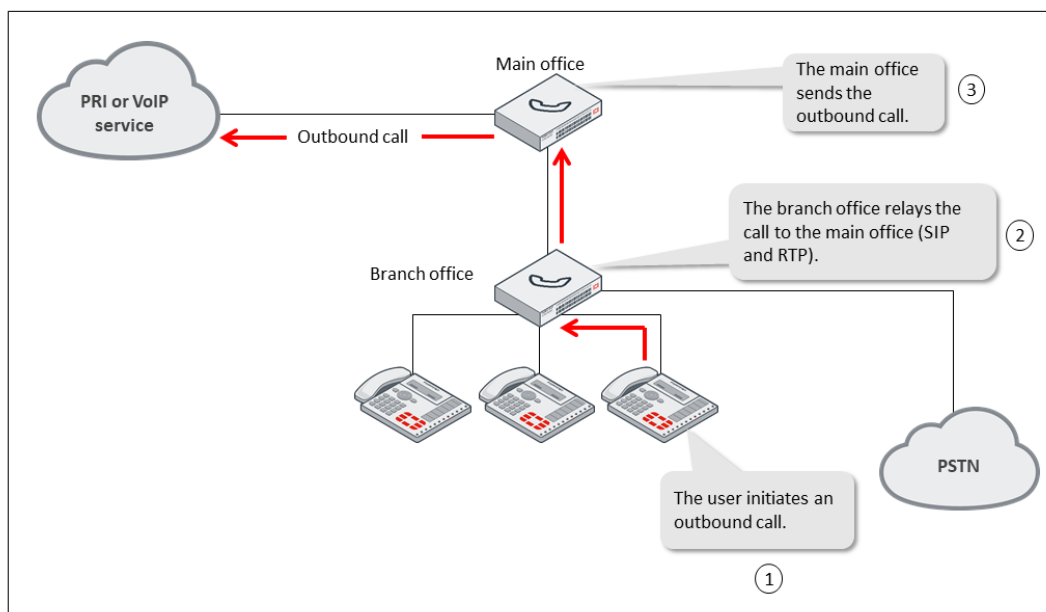
Inbound call flow with a network impairment or failure

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

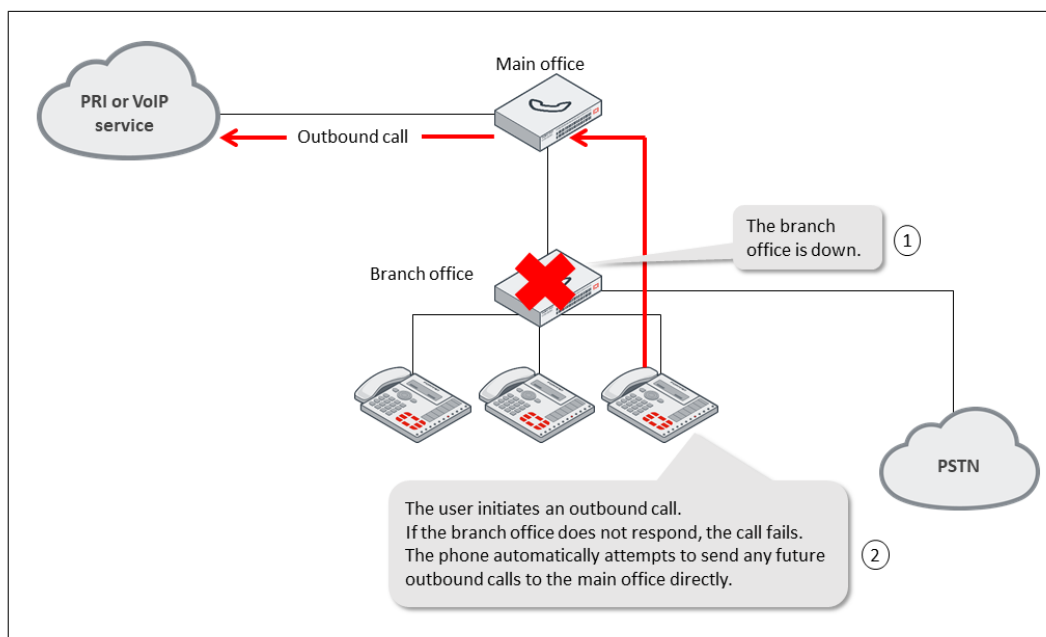
In an outbound call flow, the phone sends calls to the branch office. The branch office relays SIP traffic directly to the main office. The main office processes outbound calls.



Outbound call flow when the branch office is down

If the branch office does not respond, the call fails. If FXS gateway analog extensions are connected to the FortiVoice LSG unit, those extensions are also out of service. 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.



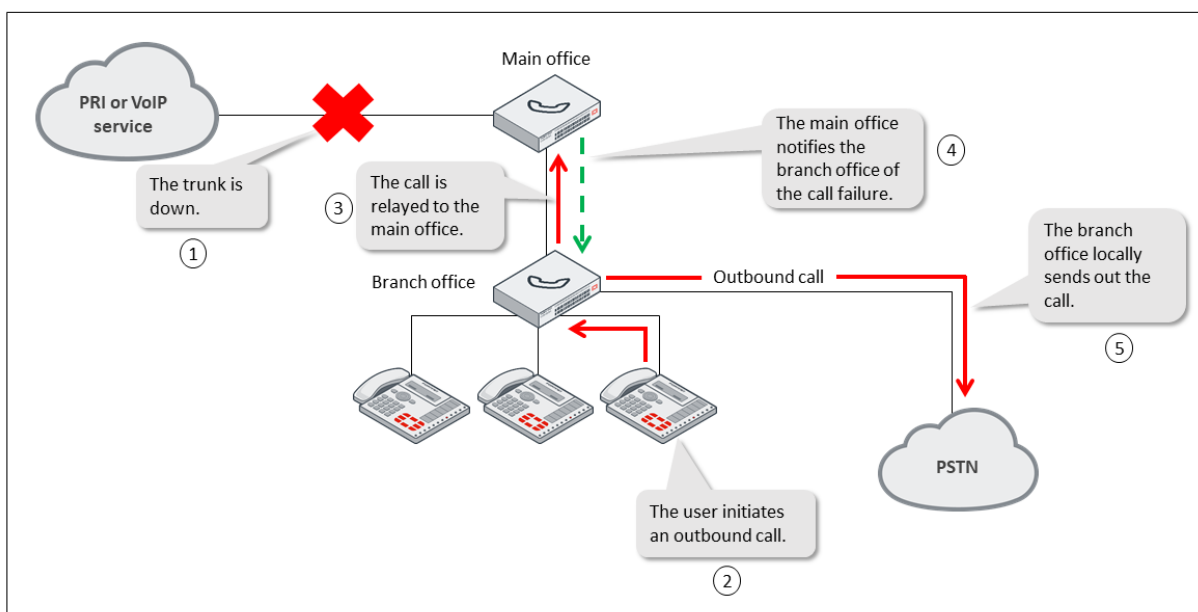
Outbound call flow when the main office trunk is down

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 24](#).

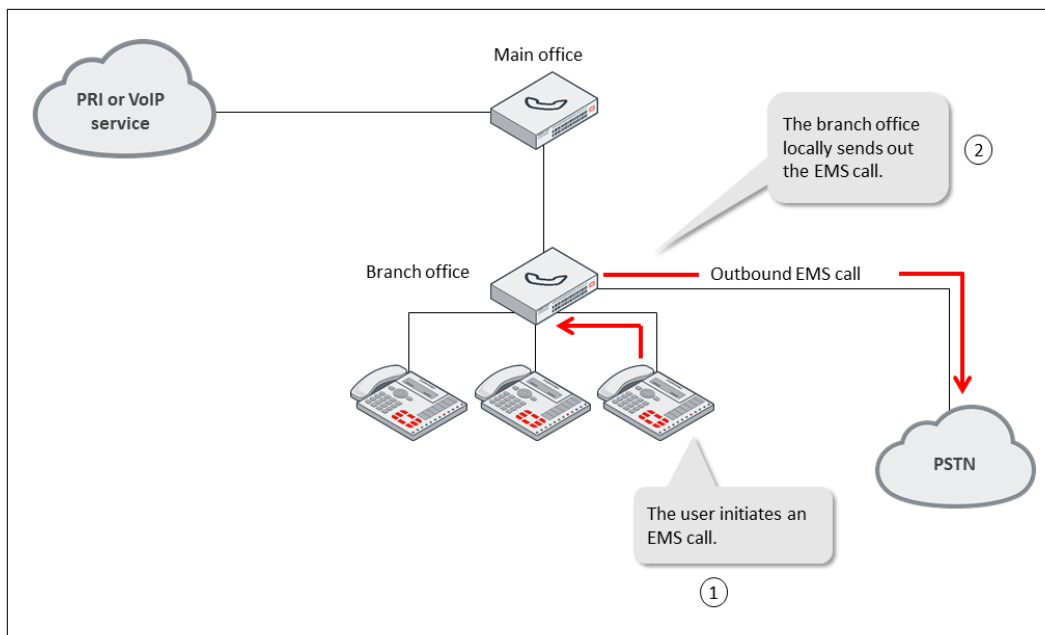
Details about creating an outbound call route are included in [Creating an outbound call route for failover scenarios on page 20](#).



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 web-based manager of the FortiVoice phone system at the main office and go to *Phone System > Profile > Emergency Zone*.

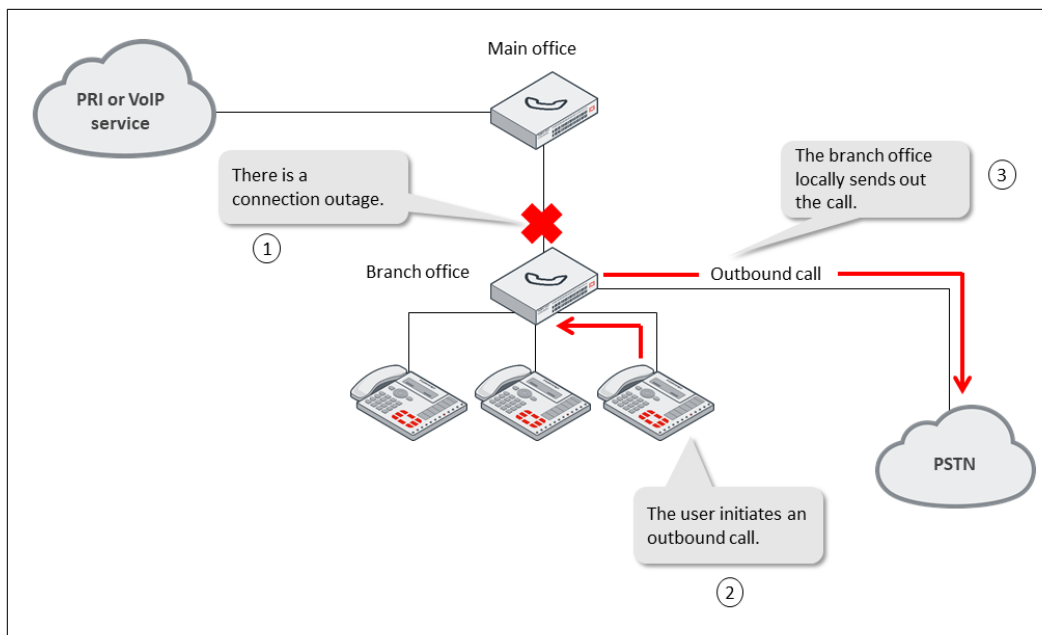


Outbound call flow with a PSTN failover

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 PSTN failover scenario. Details about creating an outbound call route are included in [Creating an outbound call route for failover scenarios on page 20](#).

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:



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. If you connect the phones too early in the workflow, then 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.



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 web-based manager 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: <ul style="list-style-type: none">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-100E, FVE-500F, and FVE-1000E models.	
Task 2	Connect to the web-based manager of the FortiVoice LSG unit.	Connecting to the FortiVoice LSG unit on page 17
Task 3	Configure administrator and network settings on the FortiVoice LSG unit.	Configuring administrator and network settings on page 19
Task 4	Upgrade the firmware of the FortiVoice LSG unit.	Upgrading the FortiVoice LSG firmware on page 21
Task 5	Change the deployment mode from <i>PBX</i> to <i>survivability branch</i> on the FortiVoice LSG unit.	Configuring the deployment mode on page 22

Task sequence	Description	Procedure
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 22
Task 7	Add or import branch extensions to the primary FortiVoice phone system at the main office.	Adding or importing branch extensions on page 23
Task 8	Add a survivability branch to the FortiVoice phone system at the main office.	Adding a survivability branch on page 24
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 28
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 28
Task 11	Connect the phones to the network at the branch office.	Connecting the phones to the network on page 29
Branch paging (optional)		
If you want your FortiVoice LSG deployment to use paging, go to Branch paging on page 30 .		

Connecting to the FortiVoice LSG unit

After physically installing the FortiVoice LSG unit and completing its initial setup, connect to the FortiVoice LSG web-based manager 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 web-based manager of the FortiVoice LSG unit on page 18 .
You have reset the configuration to its default state.	Perform the steps in Connecting to the web-based manager of the FortiVoice LSG unit on page 18 .
You are a returning user that has completed the basic configuration of the unit.	Access the web-based manager using the IP address, administrative access protocol, administrator account, and password already configured, instead of the default settings.

Scenario	Then
	<ol style="list-style-type: none"> 1. Start a web browser and enter the URL: <code>https://<IP_address>/admin</code> 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: <code>https://<IP_address>:446/admin</code>. 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 19 to make sure that you configure the required settings.

Connecting to the web-based manager of the FortiVoice LSG unit

Prerequisites

To connect to the web-based manager 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 95
 - Mozilla FireFox version 94
 - Microsoft Edge version 95
 - Apple Safari version 15
- 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 web-based manager appears.
9. Set the password for this account:
 - a. In the right corner of the web-based manager, 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 19](#).

Configuring administrator and network settings

This section includes the configuration of the following settings on the FortiVoice LSG unit at the branch office:

- [Network interface](#)
- [Static route](#)
- [DNS servers](#)
- [Administrator account](#), optional
- [Outbound call route for failover scenarios](#)

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 web-based manager, 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 web-based manager, 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 web-based manager, 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 web-based manager, 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 web-based manager, 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 21](#).

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 web-based manager, 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 **FortiVoiceEnterprise**.
 - e. On the **Release Notes** tab, review the list to identify the latest 6.4 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 22](#).
 - 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 Enterprise 6.4.4 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 v6.00 directories to locate the firmware image file. For example, FVE_200F-v64-build0394-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 web-based manager, 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 web-based manager, go to **Dashboard** and the **Status** tab.
 - b. In the **System Information** widget, go to the **Firmware version** row.
 - c. Click **Update**.

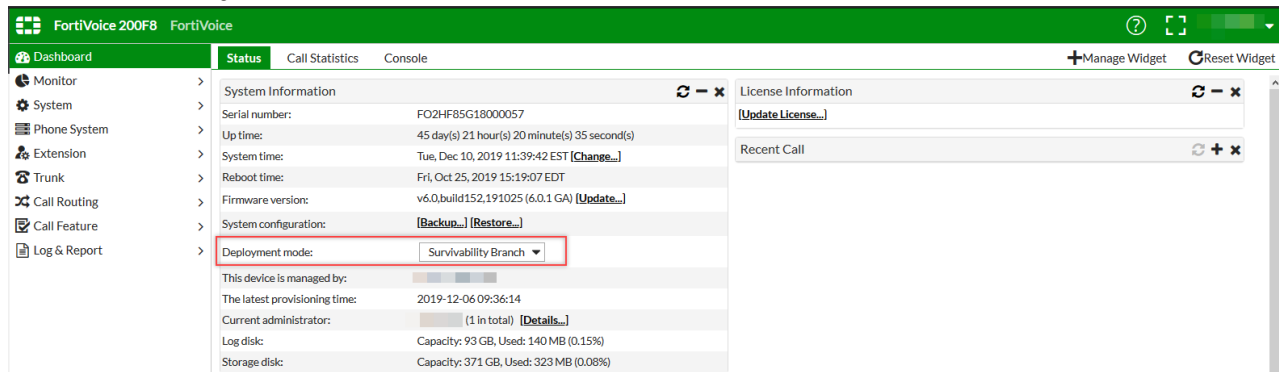
- d. Locate the firmware file and then upload that file.
Your web browser uploads the firmware file to the FortiVoice LSG unit.
- e. To confirm the upgrade, click **Yes**.
The FortiVoice LSG unit installs the firmware and restarts.
- f. To make sure that the FortiVoice LSG web-based manager reloads correctly 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 web-based manager, 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 22](#).

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 web-based manager, 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**.



You have completed this procedure.

4. To configure high availability (HA) on the primary and secondary FortiVoice units at the main office, go to [Configuring high availability on page 22](#).
If you do not want to configure HA, go to [Adding or importing branch extensions on page 23](#).

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 web-based manager 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 web-based manager 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 23](#).

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 web-based manager 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 24](#).

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 web-based manager 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 24](#).


Adding a survivability branch

Use this procedure to add a survivability branch to the FortiVoice phone system at the main office.



Procedure steps

1. Connect to the web-based manager 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
Name	Enter a unique name for this survivability branch.
Enable	Select to enable the configuration of the branch unit (FortiVoice LSG).
Display name	Not required. You can leave this field empty.
Host name/IP address	<p>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 <code>:<port number></code> after the IP address. For example, <code>172.16.5.11:4430</code>.</p> <p>Get Device Information:</p> <ul style="list-style-type: none"> • 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

GUI field	Description
	<p>number, type, and MAC address of the branch unit. This action can confirm that the systems can communicate and that the password is valid.</p> <p>Connect Device: This procedure does not use this button.</p>
Admin user name	<p>Enter the user name of the administrator account used for logging in to the branch unit.</p> <p>The default is admin.</p>
Admin password	<p>Enter the password associated with the Admin user name.</p> <p>To show the password, click the eye icon .</p>
Serial number	<p>The serial number of the FortiVoice LSG unit that you are adding to this survivability branch.</p> <p>If you are configuring the survivability branch before deploying the FortiVoice LSG unit, then manually update the serial number, type, and MAC address.</p>
Type	<p>Select the model of the FortiVoice LSG unit that you are adding to this survivability branch.</p>
MAC address	<p>The MAC address of the FortiVoice LSG unit that you are adding to this survivability branch.</p> <p>If you are configuring the survivability branch before deploying the FortiVoice LSG unit, then manually update the MAC address.</p>
Description	<p>Optionally, add any applicable notes for this survivability branch.</p>
Survivability	<p>This section includes settings related to how the branch unit operates.</p>
Management mode	<p>Make sure to select Fully managed.</p> <p>Fully managed - without branch paging</p> <p>With the fully managed mode and without branch paging configured, the main office pushes the following configurations to the branch unit.</p> <ul style="list-style-type: none"> • Extension user • Extension preferences • Global system settings • PBX setting • Profile location • Survivability branch • System auto-provisioning • System PSTN channels • Trunk PSTN <p>Fully managed - with branch paging</p> <p>With the fully managed mode and branch paging configured, the main office pushes the following configurations to the branch unit.</p> <ul style="list-style-type: none"> • Call handling • Dialplan FXO gateway mapping • Dialplan outbound • Extension user

GUI field	Description
	<ul style="list-style-type: none"> • 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	<p>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.</p> <ul style="list-style-type: none"> • 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	<p>Enter the SIP hostname or local IP address of the branch unit which local extensions (phones) can reach.</p>
Branch SIP port	<p>Enter the SIP server port number of the branch unit which local extensions (phones) can reach.</p> <p>The range is from 1 to 65535.</p> <p>The default is 5060.</p>
SIP phone registration interval	<p>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.</p> <p>The range is from 1 to 120 minutes.</p> <p>The default is 5 minutes.</p>
Emergency call	<p>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.</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p>
External caller ID option	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Use Default Caller ID: This is the caller ID associated with the extension.

GUI field	Description
	<ul style="list-style-type: none"> • 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 <code>name<phone_number></code> format, such as <code>HR<222134></code> .
Phone directory option	Select one of the following phone directories: <ul style="list-style-type: none"> • Branch directory • System directory
Branch failover trunk FXO ports	<p>This option only activates when you edit a survivability branch.</p> <p>Enter the trunk FXO ports to be used for outbound calls in the event of a failover scenario.</p> <p>For a port range, enter the starting and ending ports separated by a dash. For separate ports, use a comma.</p> <p>Port list example: 1-4,6.</p> <hr/> <div>  <p>Branch failover trunk FXO ports is applicable for all FortiVoice LSG models except FVE-100E and FVE-500F (and FVE 1000E which is still supported but has reached its end-of-order [EOO] date).</p> </div> <hr/>
Branch WSS port	<p>Enter a WebSocket Secure (WSS) port to allow the FortiVoice LSG unit to support the FortiFone softclient for desktop application.</p> <p>The default port is 8089.</p>
Branch extensions	Select extensions from the Available list and use the right arrow to move them to the Selected list.
Gateway	<p>The FortiVoice LSG solution can support a FortiVoice FXS gateway at the branch office.</p> <p>To link the FortiVoice LSG unit with a deployed FortiVoice FXS gateway, select the FortiVoice FXS gateway from the Available list and use the right arrow to move it to the Selected list.</p>
Branch Paging	<p>Options in this section are only available when you edit a survivability branch.</p> <p>If you want your deployment to use branch paging, you can complete the configuration later in Branch paging on page 30.</p> <hr/> <div>  <p>Branch paging using an FXO port is applicable for all FortiVoice LSG models except FVE-100E and FVE-500F (and FVE 1000E which is still supported but has reached its EOO date).</p> </div> <hr/>
Speed Dial Rule	<p>This option is only available when you edit a survivability branch.</p> <p>You can access details about this option later in Configuring a speed dial pattern and rule for branch paging on page 34.</p>

4. Click **Create**.
You have completed this procedure.
5. Go to [Applying the branch configuration on page 28](#).

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 gateway.

Procedure steps

1. Connect to the web-based manager 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 the FXS gateway is not linked to a survivability branch, a dialog box displays the following message:
Do you really want to update selected gateway?
If the FXS gateway is linked to a survivability branch, a dialog box displays the following message:
The config would be applied to both LSG and GW's. Do you really want to update selected gateway?
5. To confirm, click **OK**.
When the configuration changes are complete, a dialog box displays the following message:
Gateway upgrade finished.
6. Click **OK**.
You have completed this procedure.
7. Go to [Verifying the heartbeat status on page 28](#).

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 web-based manager 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 29](#).
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 19](#) and [Adding a survivability branch on page 24](#)) 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, then 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.

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-100E and FVE-500F (and FVE 1000E which is still supported but has reached its 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 30](#)
2. [Configuring an account code and user privilege for branch paging on page 31](#)
3. [Configuring a speed dial pattern and rule for branch paging on page 34](#), optional
4. [Applying the branch paging configuration on page 37](#)

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 16](#), complete tasks 1 to 11.

Procedure steps

1. Connect to the web-based manager 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
Branch FXO paging 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	<p>To allow all extensions at the same branch to connect to the paging system without a user privilege and complete a paging call, select the following option:</p> <p>Accept same branch paging </p> <p>Reject paging by default </p>
Reject paging by default	<p>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, select the following option:</p> <p>Accept same branch paging </p> <p>Reject paging by default </p>
Accept failover local paging	<p>If the main office is down and you want to do paging from the branch office, select this option.</p> <p>with authentication code: This code is not required.</p>

- Click **OK**.
You have completed this procedure.
- If you selected the **Accept same branch paging** option, then go to [Applying the branch paging configuration on page 37](#).
If you selected the **Reject paging by default** option, then go to [Configuring an account code and user privilege for branch paging on page 31](#).


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 30](#), enable the **Reject paging by default** option.

Procedure steps

- Create a paging account code:
 - Connect to the web-based manager of the primary FortiVoice phone system at the main office.
 - Go to **Security > User Privilege**, and then click the **Account Code** tab.
 - Click **New**.
 - In **Name**, enter a name to identify this account code. For example, PagingAccCode.
 - In **Description**, add any notes for this account code by clicking Edit .
 - 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**.

User Privilege

Name:

Basic Settings

- ☒ Auto provisioning
- ☒ List in directory
- ☒ Configure programmable phone key/PFK
- ☒ Softclient API login
- ☒ Lookup directory
- ☒ Lookup directory in remote office(s)
- ☐ Twinning

Operator Role ☐

Voicemail ☒

Music

Fax ☒

Call Restriction

Allow international call:

Allow long distance call:

Local:

Internal:

Other Restricted Area Code

Name	Status	Area Code	Permission	Account 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 30](#)).

- 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`.

The screenshot shows the 'IP Extension' configuration window. The 'Enabled' toggle is on. Fields for 'Number' (8601), 'User ID' (8601), 'Display name' (John Coleman), and 'Description' are visible. The 'Device Setting' section has tabs for 'Phone', 'Soft FortiFone', and 'Auxiliary Phone'. The 'Phone' tab is selected, showing fields for 'Type' (FortiFone), 'Device', 'Phone model' (FortiFone-380), 'SIP settings' (sip_phone_setting_default), 'Emergency zone' (default), and 'Programmable keys' (Default-FortiFone-380). A status box on the right shows 'Status' (green dot), 'IP', 'Phone info' (Fortinet FON-380 3.0.11.196), and 'Phone profile' (Default-FortiFone-380). The 'User Setting' section at the bottom has tabs for 'Management', 'Web Access', and 'Phone Access'. The 'Management' tab is selected, and the 'User privilege' dropdown is highlighted with a red box, showing 'AllowPagingWithCode' selected. Other fields in 'User Setting' include 'Department' (--None--) and 'Survival branch' (--None--).

- 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 34](#).
If your deployment does not require paging zones, go to [Applying the branch paging configuration on page 37](#).

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

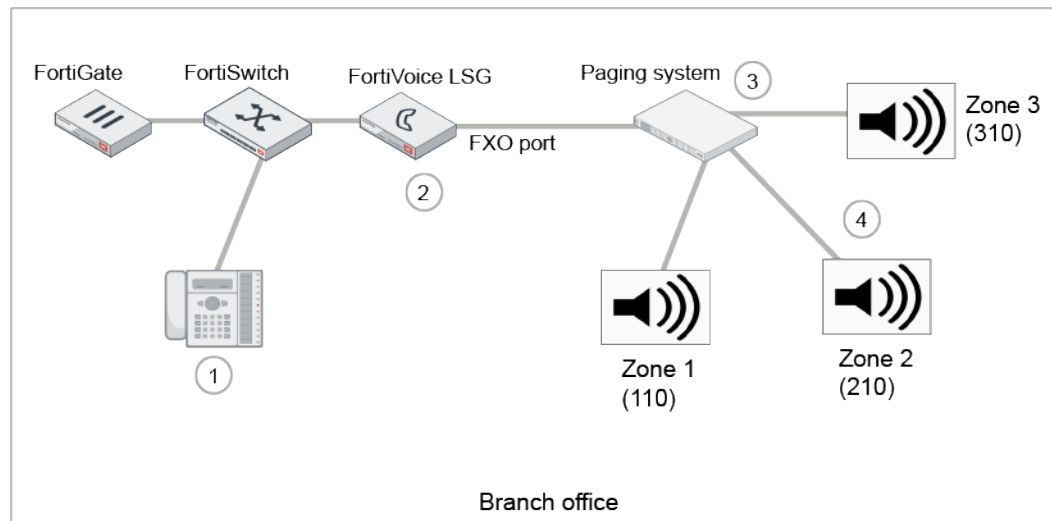
Complete [Configuring an account code and user privilege for branch paging on page 31](#).

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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • The FortiVoice LSG unit (2) communicates with the paging system (3). • At the prompt, speak to make the paging announcement.
4	<ul style="list-style-type: none"> • 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 web-based manager 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 (#)

The screenshot shows the 'Option' tab in the 'Number Management' section. The 'Speed dial pattern' field is highlighted with a red box, showing two entries: '*3XX' and '*XXX'. The 'System prohibited prefix' is set to '900', and 'System unrestricted prefix' includes '800', '866', '877', and '888'.

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	<p>The speed dial number is comprised of the following:</p> <ul style="list-style-type: none"> • Digits used to engage the paging system. Example, 0110. <div>  <p>Make sure to use the same number as in the Number field (see Configuring branch paging settings of a survivability branch on page 30).</p> </div>

GUI field	Description
	<ul style="list-style-type: none"> 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 37](#).

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 gateway.

Procedure steps

1. Connect to the web-based manager 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 the FXS gateway is not linked to a survivability branch, a dialog box displays the following message:
Do you really want to update selected gateway?
If the FXS gateway is linked to a survivability branch, a dialog box displays the following message:
The config would be applied to both LSG and GW's. Do you really want to update selected gateway?
5. To confirm, click **OK**.
When the configuration changes are complete and successful, a dialog box displays the following message:
Gateway upgrade finished.
Successful:<configured_branch_name>, <configured_FXS_gateway, if applicable>.
6. Click **OK**.
You have completed the configuration changes for branch paging.



www.fortinet.com

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.