FortiVoice - Local Survivable Gateway Deployment Guide

Version 5.3.0

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

February 7, 2020
FortiVoice 5.3.0 Local Survivable Gateway Deployment Guide
26-530-586627-20200207

TABLE OF CONTENTS

Change log **4**
Overview **5**
Supported models 5
Topology **6**
Call flows **7**
Inbound call flow 8
Inbound call flow with a network impairment or failure 9
Outbound call flow 10
Outbound call flow when the branch office is down 11
Outbound call flow when the main office trunk is down 12
Outbound call flow for a 911 or emergency medical services call 13
Outbound call flow with a PSTN failover 14
Workflow **15**
Deployment **17**
Connecting to the FortiVoice LSG unit 17
Configuring administrator and network settings 19
Upgrading the FortiVoice LSG firmware 20
Configuring the deployment mode 22
Configuring high availability 22
Adding or importing branch extensions 23
Configuring an account code and user privilege for branch paging 24
Configuring a speed dial pattern for branch paging 26
Adding a survivability branch 27
Applying the branch configuration 31
Verifying the heartbeat status 32
Connecting the phones to the network 32

Change log

Date	Change description
2019-12-03	Initial release of the FortiVoice 5.3.0 Local Survivable Gateway Deployment Guide.
2020-01-09	Updated the description in Outbound call flow when the branch office is down on page 11.
2020-02-07	Updated the management mode list (fully managed - without branch paging) in Adding a survivability branch on page 27.

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.

Supported models

The FortiVoice LSG models are:

- FVE-20E2
- FVE-20E4
- FVE-50E6
- FVE-200F8

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 and larger
- FVE-VM-500 and larger

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.

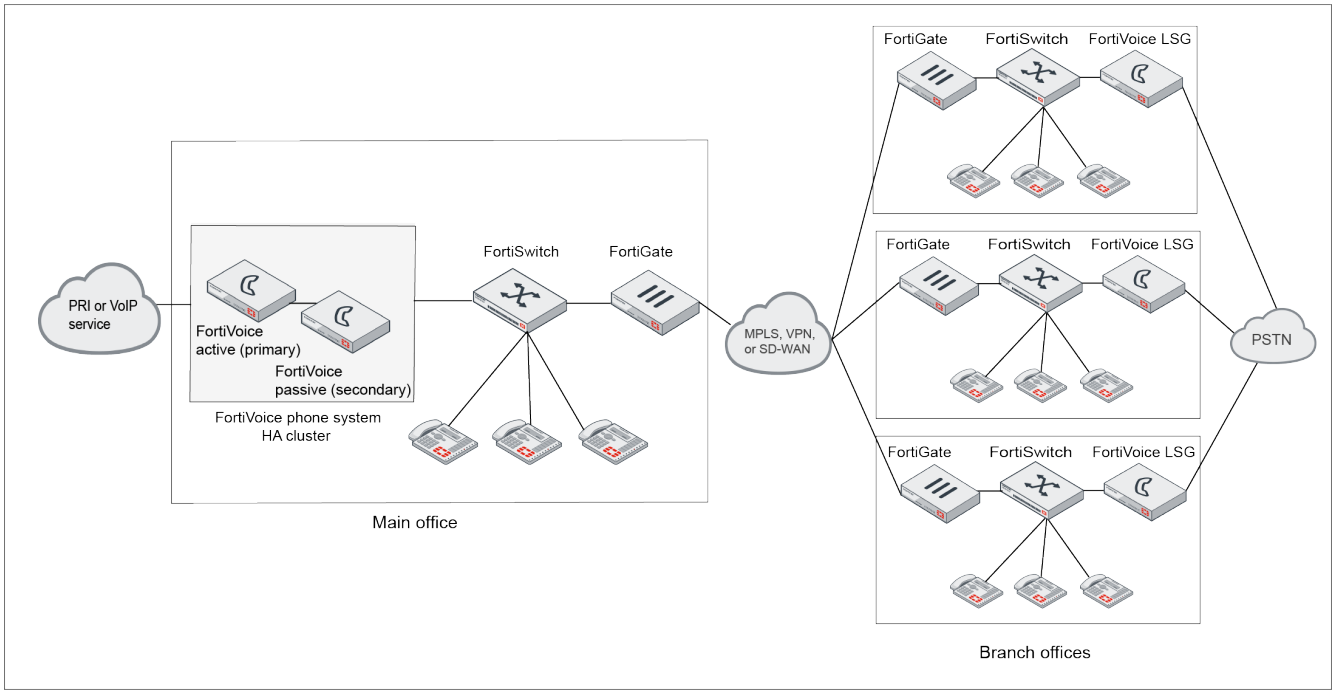
The main office manages configuration information for the branch phones and offices. The main office has the following management functions:

- 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.

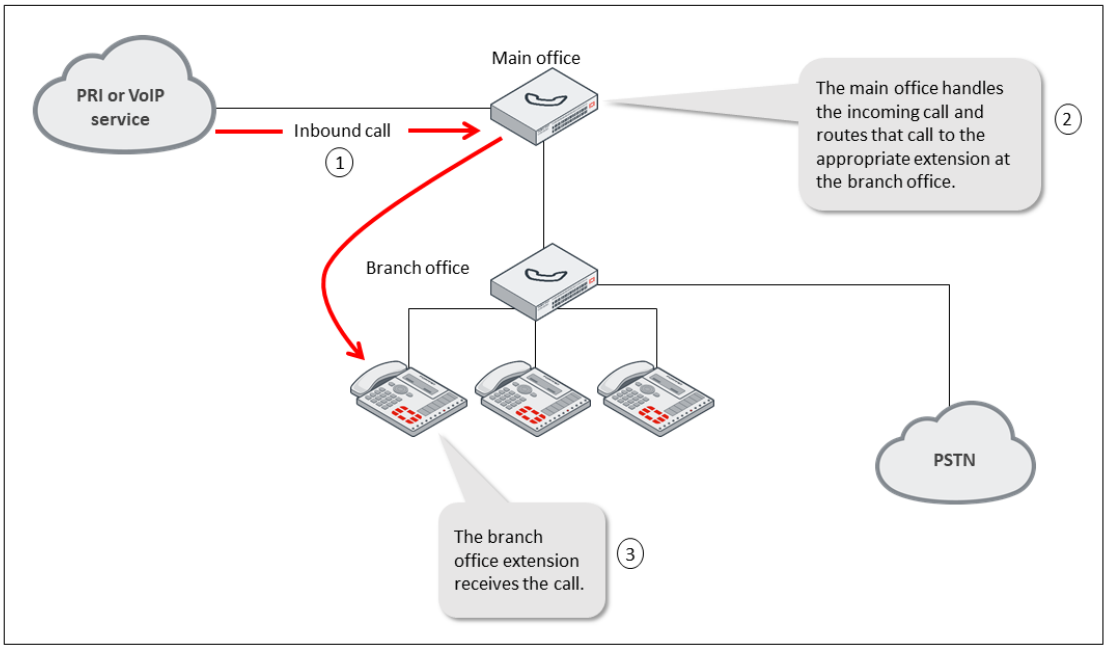
This section includes the following topics:

- Inbound call flow on page 8
- Inbound call flow with a network impairment or failure on page 9
- Outbound call flow on page 10
- Outbound call flow when the branch office is down on page 11
- Outbound call flow when the main office trunk is down on page 12
- Outbound call flow for a 911 or emergency medical services call on page 13
- Outbound call flow with a PSTN failover on page 14

Inbound call flow

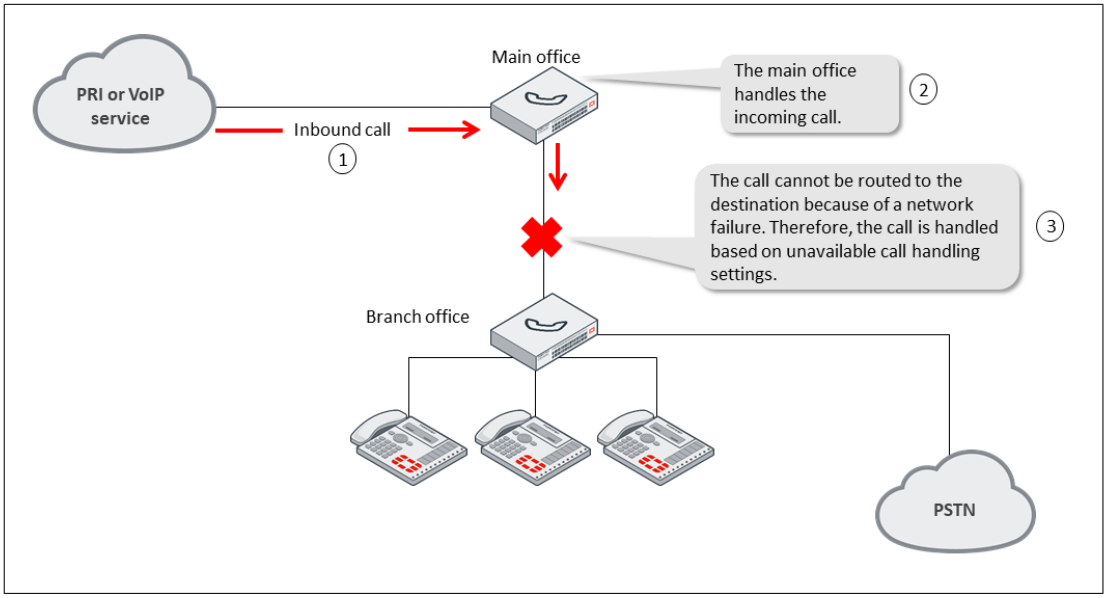
Inbound calls come into the system through the primary rate interface (PRI) or voice-over-IP (VoIP) service. The main office handles all inbound calls. The main office routes an inbound call to the right extension at the branch office.

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



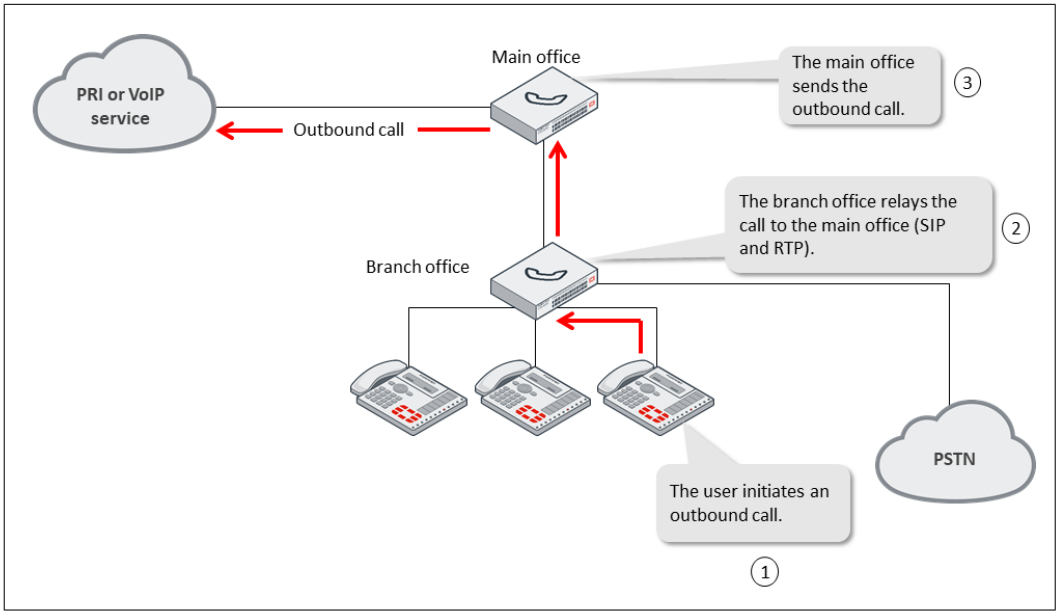
Inbound call flow with a network impairment or failure

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

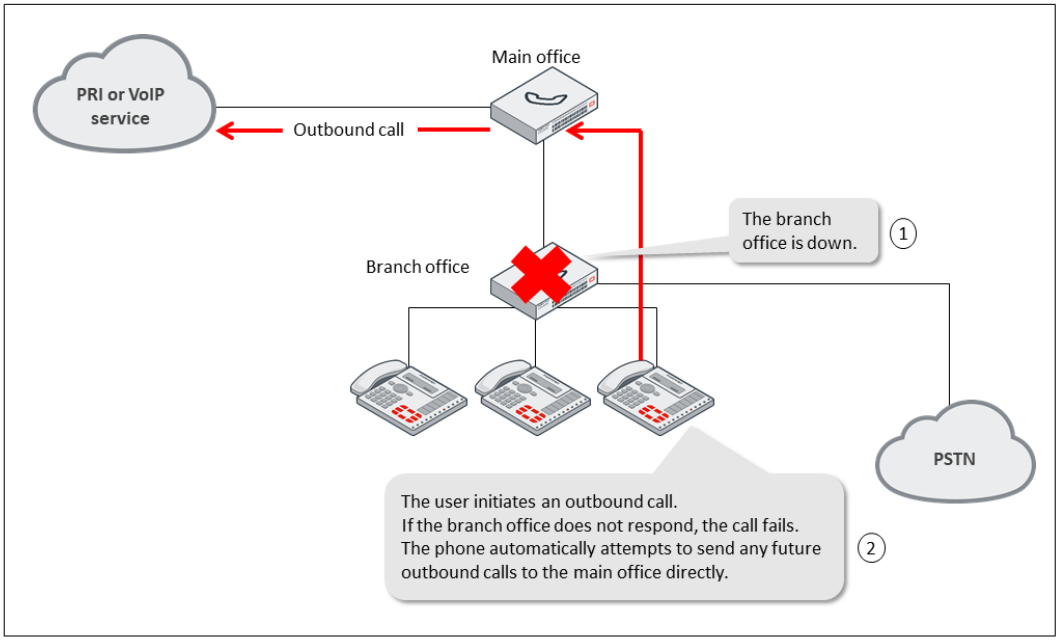
In an outbound call flow, the phone sends calls to the branch office. The branch office relays SIP traffic directly to the main office. The main office processes outbound calls.



Outbound call flow when the branch office is down

If the branch office is down, the outbound call flow changes depending on the phone model as explained in the following two scenarios:

- If the branch office does not respond, the call fails. 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).
- If the branch office does not respond, the call fails. 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.



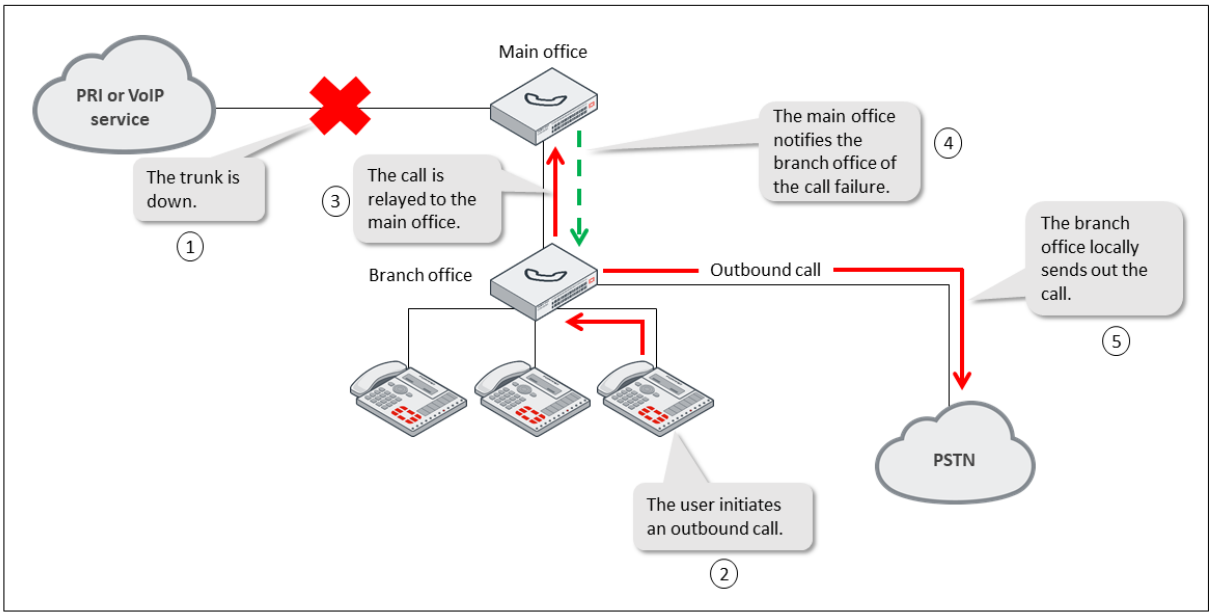
Outbound call flow when the main office trunk is down

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 27.

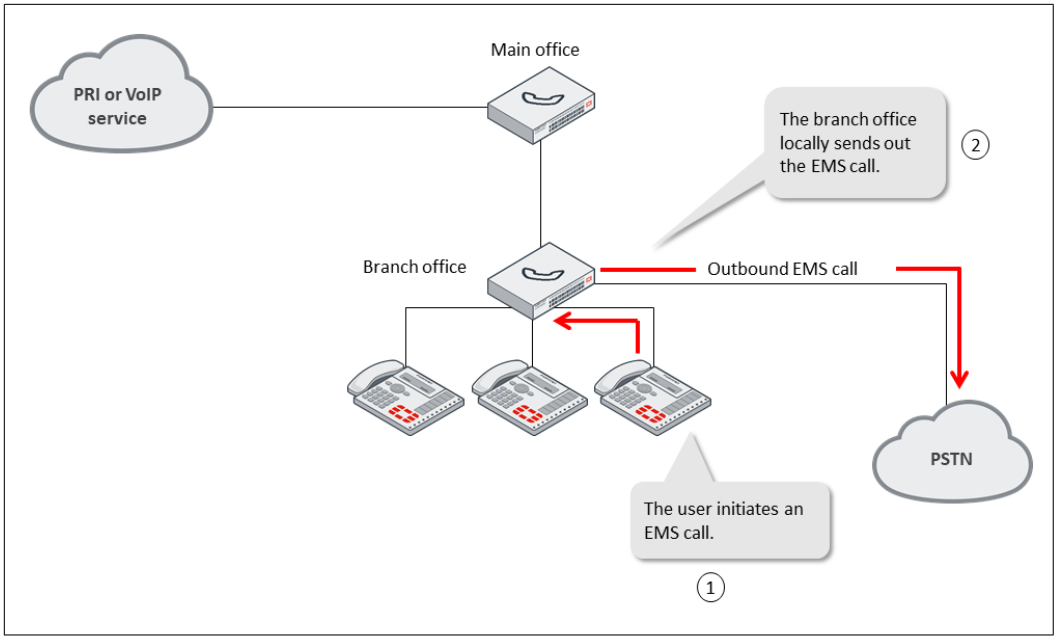
Details about creating an outbound call route are included in Creating an outbound call route for failover scenarios on page 20.



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* > *Profiles* > *Location*.

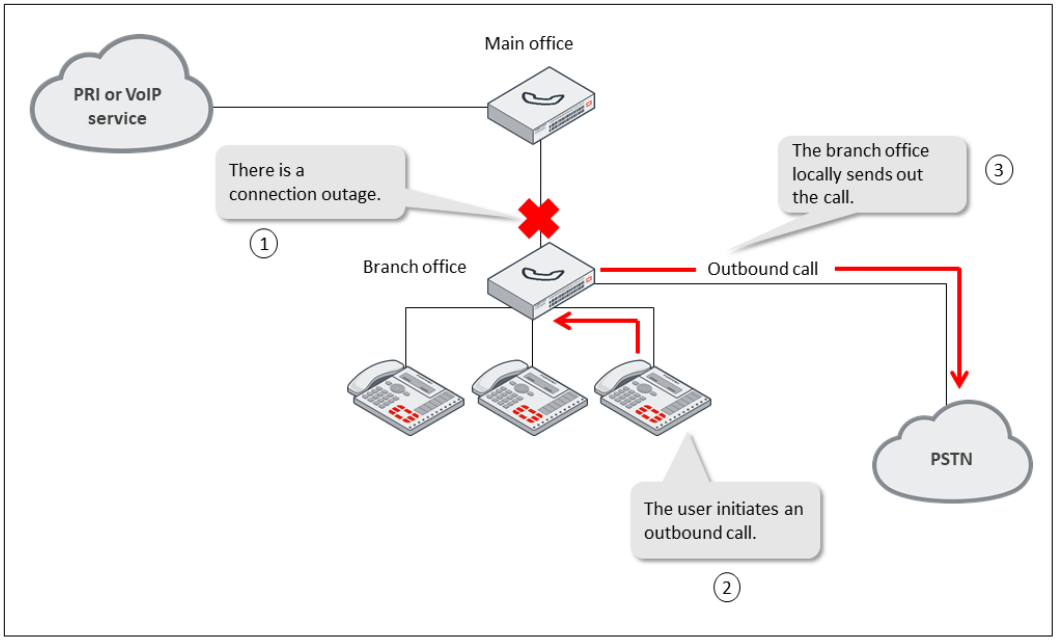


Outbound call flow with a PSTN failover

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.



Workflow

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 4 on the FortiVoice LSG unit at the branch office.		
Task 1	Connect to the web-based manager of the FortiVoice LSG unit.	Connecting to the FortiVoice LSG unit on page 17
Task 2	Configure administrator and network settings on the FortiVoice LSG unit.	Configuring administrator and network settings on page 19
Task 3	Upgrade the firmware of the FortiVoice LSG unit.	Upgrading the FortiVoice LSG firmware on page 20
Task 4	Change the deployment mode from *PBX* to *survivability branch* on the FortiVoice LSG unit.	Configuring the deployment mode on page 22
Perform tasks 5 to 10 on the FortiVoice phone system at the main office, as applicable.		
Task 5	Optionally, configure high availability (HA) on the primary and secondary FortiVoice units at the main office.	Optional - Configuring high availability on page 22
Task 6	Add or import branch extensions to the primary FortiVoice phone system at the main office.	Adding or importing branch extensions on page 23
Task 7	Allow extension users at the same branch to connect to the paging system using a user privilege and account code.	Optional - Configuring an account code and user privilege for branch paging on page 24

Task sequence	Description	Procedure
Task 8	Use speed dials for branch paging.	Optional - Configuring a speed dial pattern for branch paging on page 26
Task 9	Add a survivability branch to the FortiVoice phone system at the main office.	Adding a survivability branch on page 27
Task 10	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 31
Perform tasks 11 and 12 on the FortiVoice LSG unit at the branch office.		
Task 11	Verify that there is a healthy heartbeat between the FortiVoice LSG unit and the FortiVoice phone system.	Verifying the heartbeat status on page 32
Task 12	Connect the phones to the network at the branch office.	Connecting the phones to the network on page 32

Deployment

Make sure that you can access the FortiVoice Phone System Administration Guide.

Procedures in this section refer to this guide to help you find additional details about graphical user interface (GUI) fields in the FortiVoice phone system web-based manager.

This section includes the following topics:

1. Connecting to the FortiVoice LSG unit on page 17
2. Configuring administrator and network settings on page 19
3. Upgrading the FortiVoice LSG firmware on page 20
4. Configuring the deployment mode on page 22
5. Configuring high availability on page 22
6. Adding or importing branch extensions on page 23
7. Configuring an account code and user privilege for branch paging on page 24
8. Configuring a speed dial pattern for branch paging on page 26
9. Adding a survivability branch on page 27
10. Applying the branch configuration on page 31
11. Verifying the heartbeat status on page 32
12. Connecting the phones to the network on page 32

Connecting to the FortiVoice LSG unit

After physically installing the FortiVoice LSG unit, you need to connect to its web-based manager to perform procedures in this guide.

To connect to the FortiVoice LSG web-based manager, review the following table and perform 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. 1. Start a web browser and enter the URL: `https://<IP_address>/admin`

Scenario	Then
	Where <IP_address> is the IP address of the FortiVoice LSG unit that you want to connect to. 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:
  - Microsoft Edge version 40 or 41
  - Microsoft Internet Explorer version 11
  - Mozilla Firefox version 52.7.2 ESR or 59
  - Google Chrome version 65
  - Apple Safari version 10 or 11
- An Ethernet crossover 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 crossover 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.
   You have completed this procedure.
9. 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 interfaces
- Static routes
- DNS servers
- Administrator account, optional
- Outbound call route for failover scenarios

Editing a network interface

Use this procedure to edit physical network interfaces 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 set to 192.168.1.99.
   Port 2 has a default IP address set to 192.168.2.99.
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 Settings**, 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. Click **OK**.

Creating a static route

Use this procedure to create a static route.

1. 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. 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 > Admin**, 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. 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 20.

Upgrading the FortiVoice LSG firmware

Use this procedure to upgrade the FortiVoice LSG firmware.

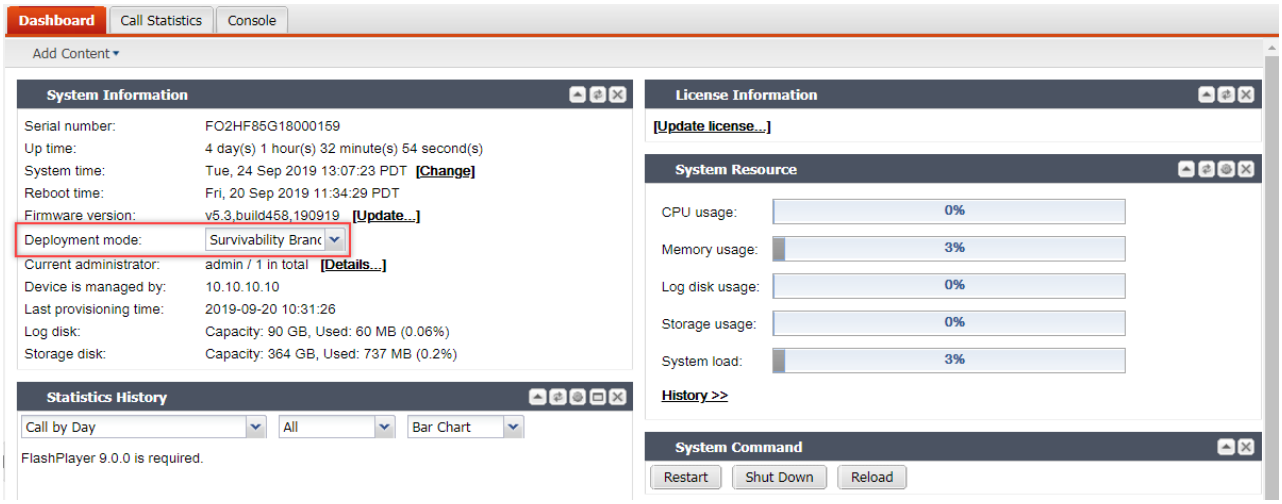
1. Identify the firmware version that is running on the FortiVoice LSG unit:
   a. In the FortiVoice LSG web-based manager, go to **Status > Dashboard**, and click the **Dashboard** tab.
   b. In the **System Information** area, review the **Firmware version** row.
   c. Take note of the firmware version 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 **Download > Firmware Images**.
   d. In **Select Product**, select **FortiVoiceEnterprise**.
   e. On the **Release Notes** tab, review the list to identify the latest 5.3 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 is an earlier build, then you need to perform an upgrade. Download the firmware image file and Release Notes to your management computer and go to step 3.
      If you do not need to perform an upgrade, you have completed this procedure. Go to Configuring the deployment mode on page 22.
3. Backup the configuration file:
   a. Go to **System > Maintenance > Configuration**.
   b. In the **Backup Configuration** area, select **System configuration**.
   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. Review the FortiVoice Enterprise 5.3 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.
   b. In the FortiVoice LSG web-based manager, go to **Status > Dashboard**, and click the **Dashboard** tab.
   c. In the Dashboard tab, go to the **System Information** area and the **Firmware version** row.
   d. Click **Update**.
   e. Locate the firmware file and then upload that file.
      Your web browser uploads the firmware file to the FortiVoice LSG unit.
   f. To confirm the upgrade, click **Yes**.
      The FortiVoice LSG unit installs the firmware and restarts.
   g. 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. Go to **Status > Dashboard**.
   b. In the **Dashboard** tab, go to the **System Information** area and review 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.

1. Connect to the web-based manager of the FortiVoice LSG unit at the branch office.
2. Go to **Dashboard > Status**.
3. In the Deployment mode drop-down list, select **Survivability Branch**.



You have completed this procedure.

4. Go to Configuring high availability on page 22.

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.

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.
   - Configuration
   - Advanced options
   - Interface monitoring
   - 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. Repeat steps 4 and 5.
   You have completed this procedure.
10. 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 **Extensions > Extensions**.
3. On the **IP Extensions** 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 one of the following procedures, as applicable:
   - Configuring an account code and user privilege for branch paging on page 24
   - Adding a survivability branch on page 27

Importing a list of branch extensions

1. Connect to the web-based manager of the primary FortiVoice phone system at the main office.
2. Go to **Extensions > Extensions**.
3. On the **IP Extensions** tab, click **Import**.
   The Import SIP extension from CSV file page opens.
4. If you want to overwrite the existing extensions with the matching imported records, select **Update existing extensions**. If you do not select this option, the import process skips the uploaded extensions if they already exist on the FortiVoice phone system.
5. If you want to import extension records with the User ID column, select **The import CSV file contains 'User ID' field**.
6. To locate the CSV file to import, click **Browse**.
7. Select the CSV file and click **Open**.
8. To access the sample CSV file, click **Download sample**. You can open or save the file and then review the sample extension entries.
9. Click **OK**.
   A progress bar shows the percentage of import completion.
   A dialog shows a summary of the extensions to be imported.

10. To complete the import, click **Import**.
    When the import is complete, a dialog shows the total of imported extensions and a status summary (succeeded, skipped, failed).
11. Click **OK**.
    You have completed this procedure.
12. Go to one of the following procedures, as applicable:
    - Configuring an account code and user privilege for branch paging on page 24
    - Adding a survivability branch on page 27

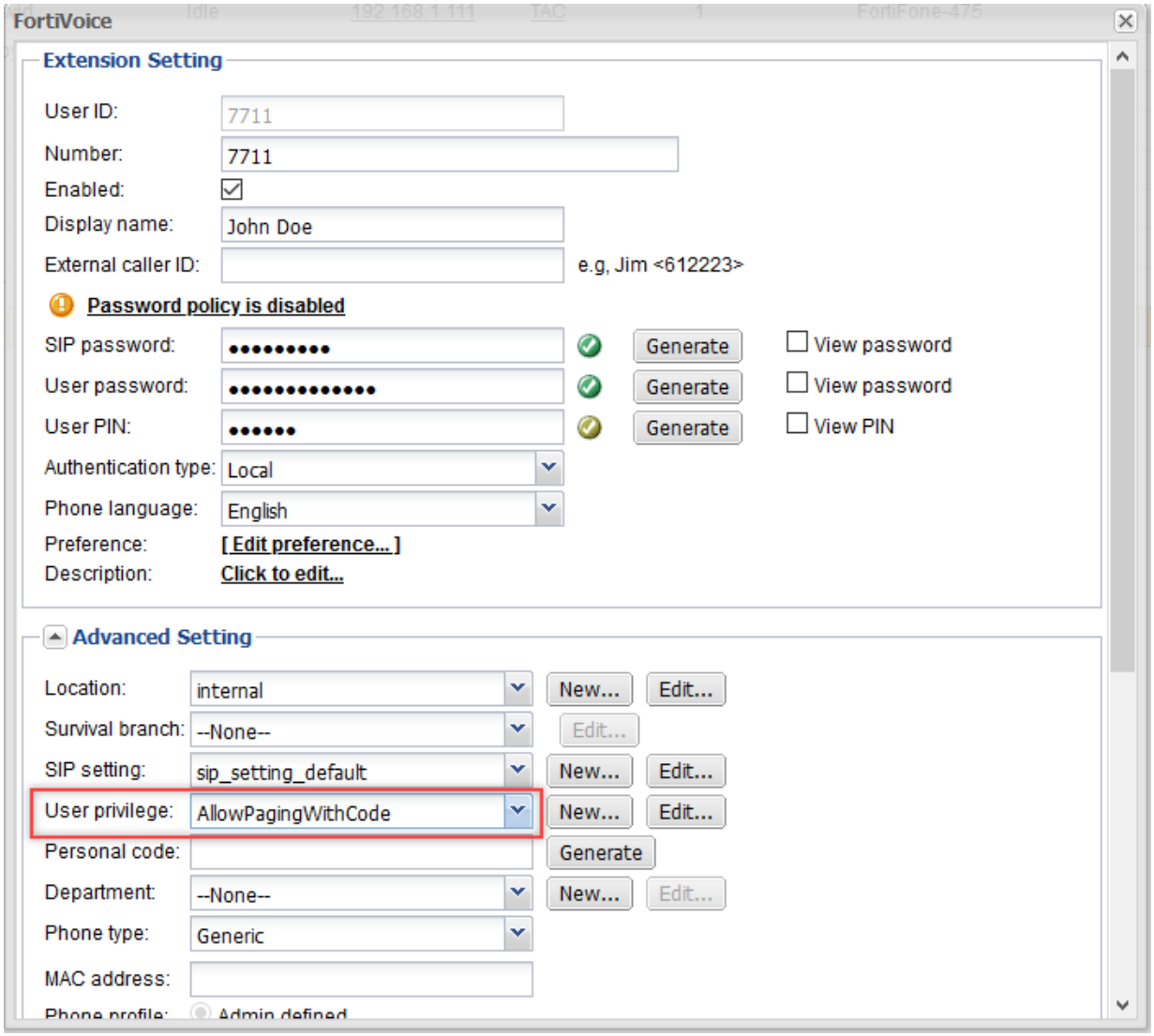
Configuring an account code and user privilege for branch paging

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 assigned to the user privilege and then validate their access to the paging system by entering the access code (PIN) when prompted.

1. Create a paging account code:
   a. Connect to the web-based manager of the primary FortiVoice phone system at the main office.
   b. Go to **Call Features > User Privileges**, 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. Do not select **Shared**.
   f. 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**.
   g. In **Description**, add any notes for this account code.
   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.
   j. In **Display name**, enter a name for the access code. For example, PagingAccessCode.
   k. In **Comments**, select **Click to edit** and add any notes for the access code.
   l. To create the access code set, click **Create**.
   m. To create the account code, click **Create**.
2. Create a paging user privilege:
   a. Go to **Call Features > User Privileges**, and then click the **User Privileges** tab.
   b. Click **New**.
   c. In **Name**, enter a name to identify this user privilege. For example, AllowPagingWithCode.
   d. Click **Call Restriction**.
   e. Click **Other Restricted Area Code/Number**.
   f. Click **New**.
   g. In **Name**, enter a name to identify this paging call restriction. For example, Paging.
   h. Select **Enabled** to activate this restriction.
   i. In **Area code/Number**, enter the paging number to be configured to engage the paging system. For example, 12$. In this example, the $ symbol functions as an explicit character match. Later in this guide, you will configure this paging number in Adding a survivability branch on page 27.

j. In **Permission**, select **Allowed with account code**.
k. In **Account code**, click **>>**.
l. In the **Available** column, select the account code that you created in step 1. In this example, you would select PagingAccCode.
m. Click **->** to move the account code to the **Selected** column.
n. Click **Create**.

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



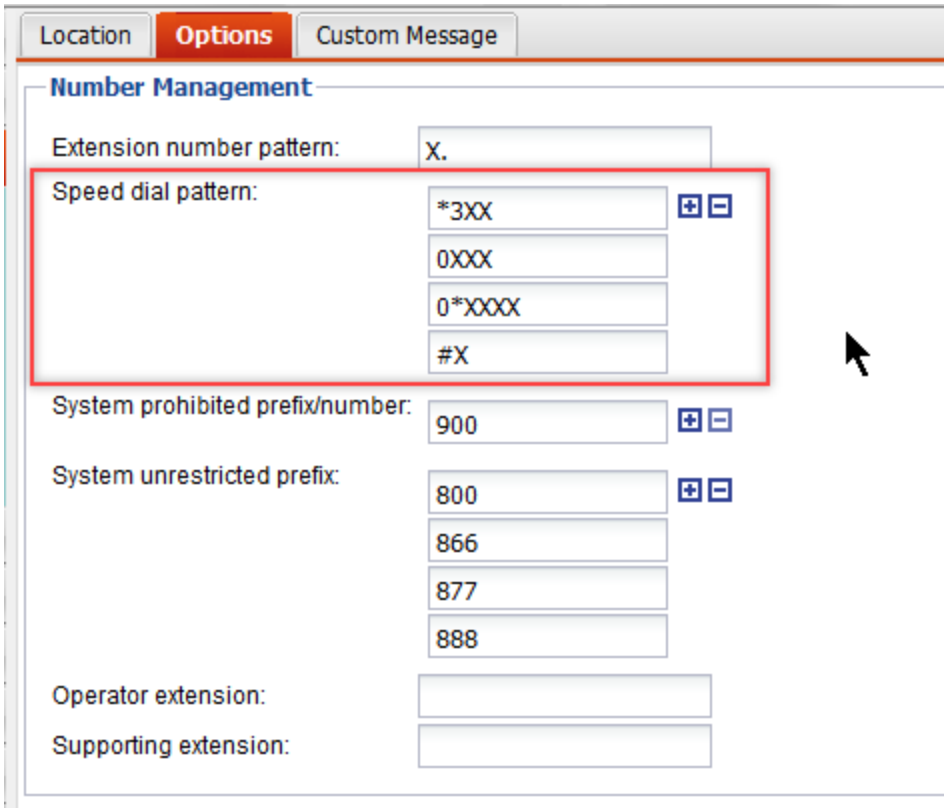
   e. Click **OK**.
   You have completed this procedure.

f. Go to one of the following procedures, as applicable:
- Configuring a speed dial pattern for branch paging on page 26
- Adding a survivability branch on page 27

Configuring a speed dial pattern for branch paging

Use this procedure to configure a speed dial pattern for branch paging. You will use this pattern later in the workflow in Adding a survivability branch on page 27.

1. Connect to the web-based manager of the primary FortiVoice phone system at the main office.
2. Go to **Phone System > Settings**, and then click the **Options** tab.
3. In **Speed dial pattern**, add one or more codes.



The FortiVoice phone system supports the following characters in a speed dial code:

Character	Description
0 to 9	Numbers from zero to nine
X	Capital letter x
*	Asterisk
#	Number sign

The following table lists speed dial code examples for branch paging:

Code	Description
*3XX	To page a three-digit room with a leading start. All rooms starting with the number 3.
0XXX	To page a three-digit room.
0*XXXX	To page a four-digit room with a leading star.
#X	To page all rooms using #0.

4. Click **Apply**.
   You have completed this procedure.
5. Go to Adding a survivability branch on page 27.

Adding a survivability branch

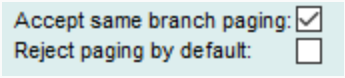
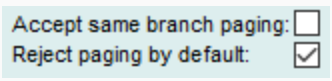
Use this procedure to add a survivability branch to the FortiVoice phone system at the main office.

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.
Enabled	Select to enable the configuration of the branch unit (FortiVoice LSG).
Display name	Not required. You can leave this field empty.
Hostname/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**: Do not click this button at this time.
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 view the password, select **View password**.

GUI field	Description
Change password	You can use the FortiVoice phone system at the main office to directly change the administrator password used for logging in to the branch unit instead of changing that password in the web-based manager of the branch unit. 1. Select the check box to change the administrator password for logging in to the branch unit. 2. Click **Change password** to show the **New password** and **Confirm password** fields. 3. Enter the new password in both fields. 4. Click **OK**.
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.
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.
Survivability	This section includes settings related to how the branch unit operates.
Management mode	Make sure to select **Fully managed**. **Fully managed - without branch paging** 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

GUI field	Description
	• 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 default is 5060.
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 5 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 fall back 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**).

GUI field	Description
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**
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.
Branch extensions	To select extensions that reside at the branch location, click **Configure Members**. Select extensions from the Available list and use the right arrow to move them to the Selected list. When you are done, click **OK**.
Branch paging	Use branch paging to broadcast an audio message to branch extensions (phones) or an overhead paging system.
FXO port	This option is only available when you edit a survivability branch. 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.
Number	This option is only available when you edit a survivability branch. Enter the number to engage the paging system. You must use the same number that you entered in the Create a paging user privilege section (step 2 i., Area code/Number) of Configuring an account code and user privilege for branch paging on page 24. For example, 12$.
Accept same branch paging **Reject paging by default**	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:  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: 

GUI field	Description
	Note: The **Reject paging by default** option requires that you completed the Configuring an account code and user privilege for branch paging on page 24 procedure.
Accept failover local paging	If the main office is down and you want to do paging from the branch office, then select this option. **Authentication code**: This code is not required.
Speed Dials	This option is only available when you edit a survivability branch. Use this section to add a paging speed dial rule.
Name	Enter a name for the speed dial mapping.
Code	Enter a code for the speed dial pattern that you completed in Configuring a speed dial pattern for branch paging on page 26. For example, 0XXX.
Number	The speed dial number is comprised of the following: • Digits used to engage the paging system, as specified earlier in this table (see the **Number** field in the **Branch paging** section). • Digits for the speed dial pattern (as specified in Configuring a speed dial pattern for branch paging on page 26). For example, 12,XXX.
Description	Optionally, add a description for the speed dial.
Description	Optionally, add any applicable notes for this survivability branch.

4. Click **Create**.
   You have completed this procedure.
5. Go to Applying the branch configuration on page 31.

Applying the branch configuration

Use this procedure to apply the branch configuration from the main office FortiVoice phone system to the FortiVoice LSG unit.

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**.
   A dialog box displays the following message: *Do you really want to update selected gateway?*
5. To confirm, click **Yes**.
   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 32.

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.

1. Connect to the web-based manager of the FortiVoice LSG unit at the branch office
2. Go to **Status > Dashboard**, and click the **Console** tab.
   The Console window opens.
3. To connect, click 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. Go to Connecting the phones to the network on page 32.
   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 27) 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.

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.