



FortiVoice - FXS Gateway Deployment Guide

Version 6.4.2

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



April 13, 2021

FortiVoice 6.4.2 FXS Gateway Deployment Guide

26-642-586629-20210413

TABLE OF CONTENTS

Change log	4
Overview	5
Supported models	5
Topology	5
Deployment	7
Connecting to the FXS gateway	8
Configuring administrator and system settings	9
Upgrading the FXS gateway firmware	12
Adding an FXS gateway (auto-discovered)	13
Adding an FXS gateway (not auto-discovered)	15
Applying the FXS gateway configuration	16
Verifying the FXS gateway association	17
Editing a managed extension of the FXS gateway	17

Change log

Date	Change description
2021-04-14	Initial release of the FortiVoice 6.4.2 FXS Gateway Deployment Guide.

Overview

The FortiVoice foreign exchange subscriber (FXS) gateway works in conjunction with the FortiVoice phone system, an IP private branch exchange (PBX), to expand resources and support additional analog phone extensions. With the FXS gateway, you can connect your traditional analog phones and fax machines to a FortiVoice phone system.

This document describes how to deploy a FortiVoice FXS gateway.

This section includes the following topics:

- [Supported models on page 5](#)
- [Topology on page 5](#)

Supported models

The supported Fortinet FXS gateway model is FortiVoice Gateway GS16. This FXS gateway has 16 ports mapped to 16 analog phone extensions.

For more details about features and specifications, see the [FortiVoice Gateways Data Sheet](#).

The following FortiVoice phone systems can manage an FXS gateway:

- FortiVoice 100E and larger
- FortiVoice-VM-100 and larger

For details about the capacity of FortiVoice phone systems for managed gateways, see the [FortiVoice Phone System Capacities Data Sheet](#).

For more details about the FortiVoice phone systems, see the [FortiVoice Phone Systems Data Sheet](#).

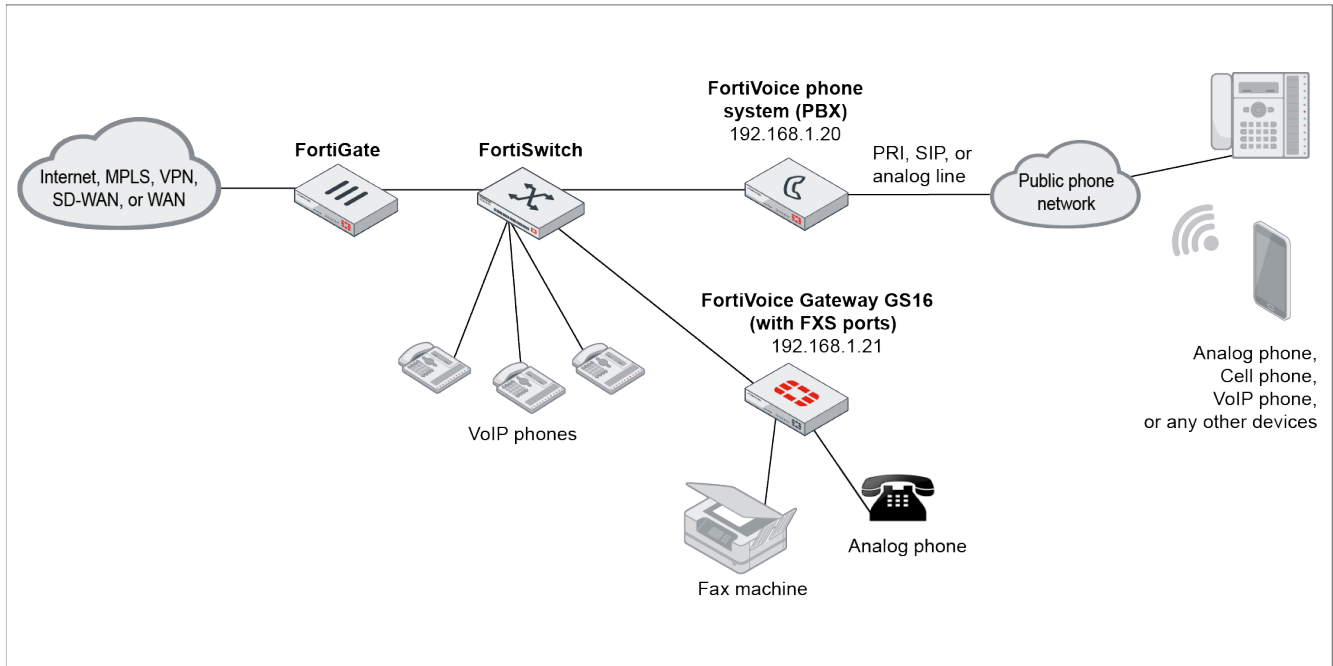
Topology

You can configure an FXS gateway to be on the same LAN as the FortiVoice phone system or over a VPN.

The FortiVoice phone system manages all configuration information for extensions and ports. However, the FXS gateway manages the following system settings:

- Network settings
- Administrator accounts
- System options
- SIP settings

The following image shows an example topology of a FortiVoice phone system managing a FortiVoice Gateway GS16:



Deployment



Before starting procedures in this guide, make sure to complete the basic setup of the FortiVoice phone system and connect to the web-based manager of that system. For more details, see the [FortiVoice Phone System Administration Guide](#).

To deploy an FXS gateway and then manage that device with a FortiVoice phone system, review the tasks and perform the procedures listed in the following workflow:

Task sequence	Description	Procedure
Perform tasks 1 to 4 on the FXS gateway.		
Task 1	Perform the following actions to complete the initial setup of the FXS gateway: <ul style="list-style-type: none">Physically install the FXS gateway.Connect the Ethernet port to your network.Connect the FXS port(s) to your analog phones and fax machines, as applicable.	
Task 2	Connect to the web-based manager of the FXS gateway.	Connecting to the FXS gateway on page 8
Task 3	Configure the following system settings: <ul style="list-style-type: none">Network interfacesStatic routesAdministrator accountsSystem optionsSIP settings, optional	Configuring administrator and system settings on page 9
Task 4	Upgrade the firmware of the FXS gateway to the latest GA release.	Upgrading the FXS gateway firmware on page 12
Perform tasks 5 to 8 on the FortiVoice phone system, as applicable.		
Task 5	Add an FXS gateway. The FortiVoice phone system can auto-discover an FXS gateway when they are both on the same LAN.	Perform one of the following procedures: <ul style="list-style-type: none">Adding an FXS gateway (auto-discovered) on page 13Adding an FXS gateway (not auto-discovered) on page 15
Task 6	Apply the gateway configuration file from the FortiVoice phone system to the FXS gateway.	Applying the FXS gateway configuration on page 16

Task sequence	Description	Procedure
Task 7	Verify that the FXS gateway is associated correctly with the FortiVoice phone system.	Verifying the FXS gateway association on page 17
Task 8	Optionally, edit any of the 16 default managed extensions.	Optional - Editing a managed extension of the FXS gateway on page 17

Connecting to the FXS gateway

After physically installing the FXS gateway and connecting its Ethernet and FXS ports, review the following table and perform the procedure that applies to your scenario to connect to the web-based manager of the FortiVoice Gateway.

Scenario	Procedure
You are connecting to the device for the first time.	Perform the steps in Connecting to the web-based manager of the FortiVoice Gateway on page 8 .
You have reset the device configuration to its default state.	Perform the steps in Connecting to the web-based manager of the FortiVoice Gateway on page 8 .
You are a returning user who has completed the basic configuration of the device.	<p>Access the web-based manager using the IP address, administrative access protocol, administrator account, and password that you have already configured, instead of the default settings.</p> <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 FXS gateway that you want to connect to. If the FXS gateway 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 system settings on page 9 to make sure that you configure the required settings.

Connecting to the web-based manager of the FortiVoice Gateway

To connect to the web-based manager of the FortiVoice Gateway 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. For details, see the [FortiVoice Phone System Release Notes](#).
- 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 FXS gateway.
3. Start your browser and enter the default URL <https://192.168.1.99/admin>.
4. To support HTTPS authentication, the FXS gateway ships with a self-signed security certificate, which it presents to users whenever they initiate an HTTPS connection to the FXS gateway. When you connect, 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 expected 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 an 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 FXS gateway.

- 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 system settings on page 9](#).

Configuring administrator and system settings

Perform this procedure to configure the following system settings on an FXS gateway:

- Network interface
- Static route
- Administrator accounts, optional

- System options
- SIP settings, optional



If you need more details about the configuration of system settings presented in this section, see the [Configuring system settings](#) section in the [FortiVoice Gateway Administration Guide](#).

Editing a physical network interface

Perform this procedure to set the IP address, netmask, and administrative access protocols of the FXS gateway.

1. In the web-based manager of the FortiVoice Gateway, go to **System > Network**.
The **Network** tab displays the following 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 FXS gateway.
3. In **Addressing Mode, Manual**, go to **IP/Netmask** and edit the IP address and netmask of the interface. Make sure that this IP address is outside of the FortiGate DHCP range.
4. In **Advanced Setting**, make sure to enable the protocols that you want the network interface to use to accept connections to the FXS gateway.
5. In **Administrative status**, make sure that **Up** is selected for the network interface to be available to receive traffic.
6. Click **OK**.

Configuring a static route

Perform this procedure to configure a static route to the router.

1. In the web-based manager of the FortiVoice Gateway, go to **System > Network**, and then click the **Routing** tab.
2. Click **New**.
3. Make sure that **Enable** is selected.
4. In **Destination IP/Netmask**, enter the destination IP address and netmask of packets subject to this static route.
To create a default route that matches all destination IP addresses, enter **0.0.0.0/0**.
5. In **Interface**, select the interface that this route applies to.
6. In **Gateway**, enter the IP address of the router.
7. In **Comment**, enter any notes for this static route.
8. Click **OK**.

Creating an additional administrator account

Optionally, perform this procedure to create an additional administrator account with restricted permissions. By default, the FXS gateway has a single administrator account called *admin*.

Prerequisite

If you want to create or edit an admin profile, perform this task on the FortiVoice phone system first. For more details about the admin profile, see the [Configuring administrator profiles](#) section in the [FortiVoice Phone System Administration Guide](#).

Procedure steps

1. In the web-based manager of the FortiVoice Gateway, go to **System > Administrator**.
2. Click **New**.
3. In **Administrator**, enter the name for this administrator account.
The name can contain numbers (0-9), uppercase and lowercase letters (A- Z, a- z), hyphens (-), and underscores (_). Other special characters and spaces are not allowed.
4. In **Email address**, enter the email address of the administrator.
5. In **Admin profile**, select the admin profile. This profile determines which functional areas the administrator account can view or affect.
6. In the **New password** and **Confirm password**, enter the password for this account.
The password can contain any character except spaces.



Do not enter an FXS gateway administrator password that is less than six characters long. For better security, enter a longer password with a complex combination of characters and numbers, and change the password regularly. Failure to provide a strong password can compromise the security of your FXS gateway.

7. In **Trusted hosts**, enter the IPv4 or IPv6 address or subnet and netmask from which this administrator can log in.
For example, if your private network has an IP address of 192.168.1.0 and you want to allow the administrator to log in to the FXS gateway from your private network, enter `192.168.1.0/24`.
If you want the administrator to access the FXS gateway from any IP address, use `0.0.0.0/0`.
8. In **Select language**, select the language to display in the web-based manager when this administrator logs in.
9. In **Select theme**, select the theme to display in the web-based manager when this administrator logs in.
10. In **Description**, enter any notes for this account.
11. Click **Create**.

Configuring system options

Perform this procedure to set the system idle timeout and administration ports.

1. In the web-based manager of the FortiVoice Gateway, go to **System > Configuration**, and then click the **Option** tab.
2. In **Idle timeout**, enter the amount of time in minutes that an administrator can be inactive before the FXS gateway automatically logs out the administrator.
3. In **Administration Ports**, specify the TCP ports for the administrative access on all interfaces.
Default port numbers:
 - **HTTP port number**: 80
 - **HTTPS port number**: 443
 - **SSH port number**: 22
 - **TELNET port number**: 23
4. Click **Apply**.

Configuring SIP settings

Optionally, perform this procedure to configure SIP settings.

1. In the web-based manager of the FortiVoice Gateway, go to **System > Advanced Setting**, and then click the **SIP** tab.
2. In **SIP Transport**, enable the ports as required.
SIP communications commonly uses TCP or UDP port 5060.
Port 5060 is used for nonencrypted SIP signaling sessions.
Port 5061 is typically used for SIP sessions encrypted with the TLS protocol.
3. In **RTP Setting**, keep the default values.
4. Click **Apply**.
You have completed this procedure.
5. Go to [Upgrading the FXS gateway firmware on page 12](#).

Upgrading the FXS gateway firmware

Perform this procedure to upgrade the FXS gateway firmware.

Procedure steps

1. Identify the firmware version that is running on the gateway:
 - a. In the web-based manager of the FortiVoice Gateway, go to **Dashboard**.
 - b. In the **Status** tab, go to the **System Information** widget and 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 gateway firmware:
 - a. Go to the [Fortinet Technical 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. In the **Release Notes** tab, review the FortiVoiceEnterprise 6.4 list to identify the latest firmware version.
 - f. Compare the firmware version and build number with the firmware version that is running on the gateway.
 - g. If the build number of the firmware version running on the gateway matches the one on the Fortinet Support website, then you do not need to perform an upgrade. You have completed this procedure. Go to one of the following procedures:
 - [Adding an FXS gateway \(auto-discovered\) on page 13](#)
 - [Adding an FXS gateway \(not auto-discovered\) on page 15](#)
 - h. If the build number of the firmware version running on the gateway is an earlier build, then you need to prepare for an upgrade:
 - i. Review the [FortiVoice Phone System Release Notes](#). This document includes the most current upgrade information such as supported upgrade paths and may also 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, FVG_GS16-v64-build0343-FORTINET.out.

- iii. To download the firmware image file to your management computer, 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 web-based manager of the FortiVoice Gateway, go to **Dashboard**.
 - b. In the **Status** tab, go to the **System Information** widget and 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 **System Information** widget, go to the **Firmware version** row.
 - b. Click **Update**.
 - c. Locate the firmware file and then upload that file.
Your web browser uploads the firmware file to the gateway.
 - d. To confirm, click **Yes**.
The gateway installs the firmware and restarts.
 - e. To make sure that the FortiVoice Gateway 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 **System Information** widget, go to the **Firmware version** row.
 - b. Make sure that the firmware version is the one that you upgraded to.
You have completed this procedure.
6. Go to one of the following procedures:
 - [Adding an FXS gateway \(auto-discovered\) on page 13](#)
 - [Adding an FXS gateway \(not auto-discovered\) on page 15](#)


Adding an FXS gateway (auto-discovered)

The FortiVoice phone system can auto-discover an FXS gateway when they are on the same LAN. With an auto-discovered device, you can create a new configuration for that gateway or replace an existing gateway configuration.

Procedure steps

1. Connect to the web-based manager of the FortiVoice phone system.
2. Go to **Managed System > Gateway**, and then click the **FXS Gateway** tab.
3. Click **Unmanaged Gateway**.
The dialog opens and displays all the gateways discovered on the LAN of the FortiVoice phone system.
4. Select the FXS gateway that you want to add.
5. In the **Actions** drop-down list, select one of the following actions:
 - **Create New Device** to add the gateway as a new entry into the FortiVoice phone system. Go to [step 6](#).
 - **Replace Existing Device** to choose which gateway to replace. You can use this option when a device is defective. Go to [step 9](#).

6. If you selected **Create New Device**, then configure the following settings:

GUI field	Description
Name	Enter a unique name to identify the FXS gateway.
Enable	Select to activate the configuration of the FXS gateway.
Display name	Not required. You can leave this field empty.
Hostname/IP address	<p>The hostname or IP address of the auto-discovered FXS gateway. For an auto-discovered FXS gateway, the FortiVoice phone system autopopulates this field.</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 FXS gateway and get the MAC address of the gateway. This action can confirm that the systems can communicate and that the password is valid. <p>Connect Device: This procedure does not use this button (with this button, you would access the FortiVoice Gateway web-based manager in a separate tab in your web browser).</p>
Admin user name	<p>Enter the user name of the administrator account used for logging in to the FXS gateway.</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> <p>The default is no password.</p>
Serial number	The serial number of the gateway that you are adding to the FortiVoice phone system. For an auto-discovered FXS gateway, the FortiVoice phone system autopopulates this field.
Type	The type of gateway that you are adding to the FortiVoice phone system.
MAC address	The MAC address of the gateway that you are adding to the FortiVoice phone system.
Description	Optionally, add any applicable notes for this gateway.

7. Click **Finish**.

The FortiVoice phone system creates 16 default managed extensions from 7801 to 7816 for your first FXS gateway. With any subsequent FXS gateway addition, the FortiVoice phone system continues to add a range of 16 extensions to the existing managed extension list. For example, the FortiVoice phone system adds extensions 7817 to 7832 for the second FXS gateway.

If the FortiVoice phone system already has an extension that is included in the range of default managed extensions to be created, the numbering of new extensions will account for the existing extension. For example, the FortiVoice phone system has extension 7812. With the addition of the first FXS gateway, the FortiVoice phone system would create 16 managed extensions from 7801 to 7817 (not 7816).

To access the extension list, go to **Extension > Extension**, and then click **Managed Extension**.

8. You have completed this procedure. You can now go to [Applying the FXS gateway configuration on page 16](#).

9. If you selected **Replace Existing Device**, then follow the system prompts to choose which gateway configuration you want to replace and then replace it. Both existing and replacement devices must be the same type.
10. You have completed this procedure. You can now go to [Applying the FXS gateway configuration on page 16](#).

Adding an FXS gateway (not auto-discovered)


Perform this procedure to add an FXS gateway to the FortiVoice phone system in cases such as in the following examples:

- You are preconfiguring the FortiVoice phone system before deploying the FXS gateway.
- You are setting up the FortiVoice phone system and locating the FXS gateway on a VPN. Therefore, the devices are not on the same LAN.

Procedure steps

1. Connect to the web-based manager of the FortiVoice phone system.
2. Go to **Managed System > Gateway**, and then click the **FXS Gateway** tab.
3. Click **New**.
4. Configure the following settings:

GUI field	Description
Name	Enter a unique name to identify the FXS gateway.
Enable	Select to activate the configuration of the FXS gateway.
Display name	Not required. You can leave this field empty.
Hostname/IP address	<p>Enter the hostname or IP address of the FXS gateway.</p> <p>If the FXS gateway is configured to use a non-default HTTPS port, then add <code>:<port number></code> after the IP address. For example, <code>192.168.1.21:4430</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 FXS gateway to get the serial number and the MAC address of the gateway. This action can confirm that the systems can communicate and that the password is valid. <p>Connect Device: This procedure does not use this button (with this button, you would access the FortiVoice Gateway web-based manager in a separate tab in your web browser).</p>
Admin user name	<p>Enter the user name of the administrator account used for logging in to the FXS gateway.</p> <p>The default is admin.</p>

GUI field	Description
Admin password	Enter the password associated with the Admin user name. To show the password, click the eye icon  . The default is no password.
Serial number	The serial number of the FXS gateway that you are adding to the FortiVoice phone system.
Type	The type of gateway that you are adding to the FortiVoice phone system.
MAC address	The MAC address of the FXS gateway that you are adding to the FortiVoice phone system.
Survivability branch	The FortiVoice LSG solution can support a FortiVoice FXS gateway at a branch office. To link this FXS gateway with a survivability branch, select that branch from the list. For details about deploying a FortiVoice LSG unit, see the FortiVoice Local Survivable Gateway Deployment Guide .
Description	Optionally, add any applicable notes for this FXS gateway.

5. Click **Create**.

The FortiVoice phone system creates 16 default managed extensions from 7801 to 7816 for your first FXS gateway. With any subsequent FXS gateway addition, the FortiVoice phone system continues to add a range of 16 extensions to the existing managed extension list. For example, the FortiVoice phone system adds extensions 7817 to 7832 for the second FXS gateway.

If the FortiVoice phone system already has an extension that is included in the range of default managed extensions to be created, the numbering of new extensions will account for the existing extension. For example, the FortiVoice phone system has extension 7812. With the addition of the first FXS gateway, the FortiVoice phone system would create 16 managed extensions from 7801 to 7817 (not 7816).

To access the extension list, go to **Extension > Extension**, and then click **Managed Extension**.

6. Go to [Applying the FXS gateway configuration on page 16](#).

Applying the FXS gateway configuration

The FortiVoice phone system stores a gateway configuration file. Perform this procedure to apply this gateway configuration file to the FXS gateway.

Procedure steps

1. Connect to the web-based manager of the FortiVoice phone system.
2. Go to **Managed System > Gateway**, and then click the **FXS Gateway** tab.
3. In the list, select the gateway to which you want to apply the configuration file.
4. Click **Apply Configuration**.

If the FXS gateway is not linked to a survivability branch, the FortiVoice phone system displays the following message:

Do you really want to update selected gateway?

If the FXS gateway is linked to a survivability branch, the FortiVoice phone system displays the following message:

The config would be applied to both LSG and GW's. Do you really want to update selected gateway?

5. Click **OK**.

The FortiVoice phone system applies configuration changes to the extensions of the FXS gateway.

With a successful upgrade, the FXS gateway displays the following message:

Gateway upgrade finished.

Successful:<gateway_name>

6. Click **OK**.

You have completed this procedure.

7. Go to [Verifying the FXS gateway association on page 17](#).

Verifying the FXS gateway association

Perform this procedure to verify that the association of the FXS gateway with the FortiVoice phone system is successful.

Procedure steps

1. Connect to the web-based manager of the FortiVoice phone system.
2. Go to **Extension > Extension**, and then click the **Managed Extension** tab.
3. Verify that the **Gateway Device** column shows the gateway that the extension is associated with.
You have completed this procedure and the FXS gateway deployment.
4. If you want to edit a managed extension, go to [Editing a managed extension of the FXS gateway on page 17](#).


Editing a managed extension of the FXS gateway



The FortiVoice Gateway GS16 has 16 FXS ports. After adding the gateway to the FortiVoice phone system, each port is associated with a generated extension number. To edit an FXS gateway extension, perform this procedure.

Procedure steps

1. Connect to the web-based manager of the FortiVoice phone system.
2. Go to **Extension > Extension**, and then click the **Managed Extension** tab.
The list includes extensions for all gateways.
3. In **Gateway device**, select the FortiVoice Gateway GS16 which has the extension that you want to edit.

4. Double-click the extension that you want to edit.
5. Edit the following parameters, as applicable:

GUI field	Description
Number	The extension number. For details about the extension number pattern, see the Configuring PBX options section in the FortiVoice Phone System Administration Guide . Edit Preference: For details about extension user preferences, see the Setting extension user preferences section in the FortiVoice Phone System Administration Guide .
User ID	The system automatically generates this ID based on the gateway and port. This parameter is read only.
Enable	Select to activate the extension.
Display name	The caller ID for internal calls. Enter the name that the phone can display when it receives a call from this extension. To access and modify the External caller ID and Emergency caller ID , click the plus sign  .
Description	Optionally, add notes for the managed extension.
Device Setting	
Gateway device	The name of the gateway device. This option is read only.
Gateway fxs port	The gateway FXS port associated with the extension. This option is read only.
Direct call	If you want the phone to perform a direct call to a specified number after you pick up the phone handset, enable this option. Number: Enter the phone number for the direct call.
User Setting, Management	
User privilege	Select or add the user privilege that you want to apply to the extension. A user privilege includes a collection of phone services and restrictions that you can apply to each extension. You can edit the default user privilege but you cannot delete it.
Department	Select or add the department that the extension belongs to.
User Setting, Web Access	Configure web user portal and soft client access from mobile or desktop devices.
Authentication type	Select the extension's authentication type: Local or LDAP .

GUI field	Description
User password	<p>If you selected Local as the Authentication type, enter the password for user web portal access. This password can be much longer and stronger to mitigate the risk of password guess attack and preserve the voicemail PIN for phone access only.</p> <p>To let the system create the user password, click Generate.</p> <p>To show the user password, click the eye icon .</p>
LDAP profile	<p>If you selected LDAP as the Authentication type, select or create an LDAP profile to apply to this extension.</p> <p>For more details about the LDAP profile configuration, see the Configuring LDAP profiles section in the FortiVoice Phone System Administration Guide.</p>
Authentication ID	<p>During the configuration of the LDAP profile, you have two options for the user authentication:</p> <ul style="list-style-type: none"> • If you select Try Common Name with Base DN as Bind DN, update the authentication ID field to match the common name attribute (example, uid) that you entered in the Common name ID field of the LDAP profile. Example: <code>j.doe</code>. • If you select Search User and Try Bind DN, leave the authentication ID field blank.
User Setting, Phone Access	
Voicemail PIN	<p>For the extension user to access the extension voicemail and the user web portal, enter the password.</p> <p>To let the system create the voicemail PIN, click Generate.</p> <p>To show the voicemail PIN, click the eye icon .</p>
Personal code	<p>Enter the extension specific account code used to restrict calls. To make a restricted call, you need this code.</p> <p>To let the system create the personal code, click Generate.</p>

- To save the changes, click **OK**.
You have completed this procedure.
- Send the extension changes to the FXS gateway by following the instructions in [Applying the FXS gateway configuration on page 16](#).



FORTINET[®]



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