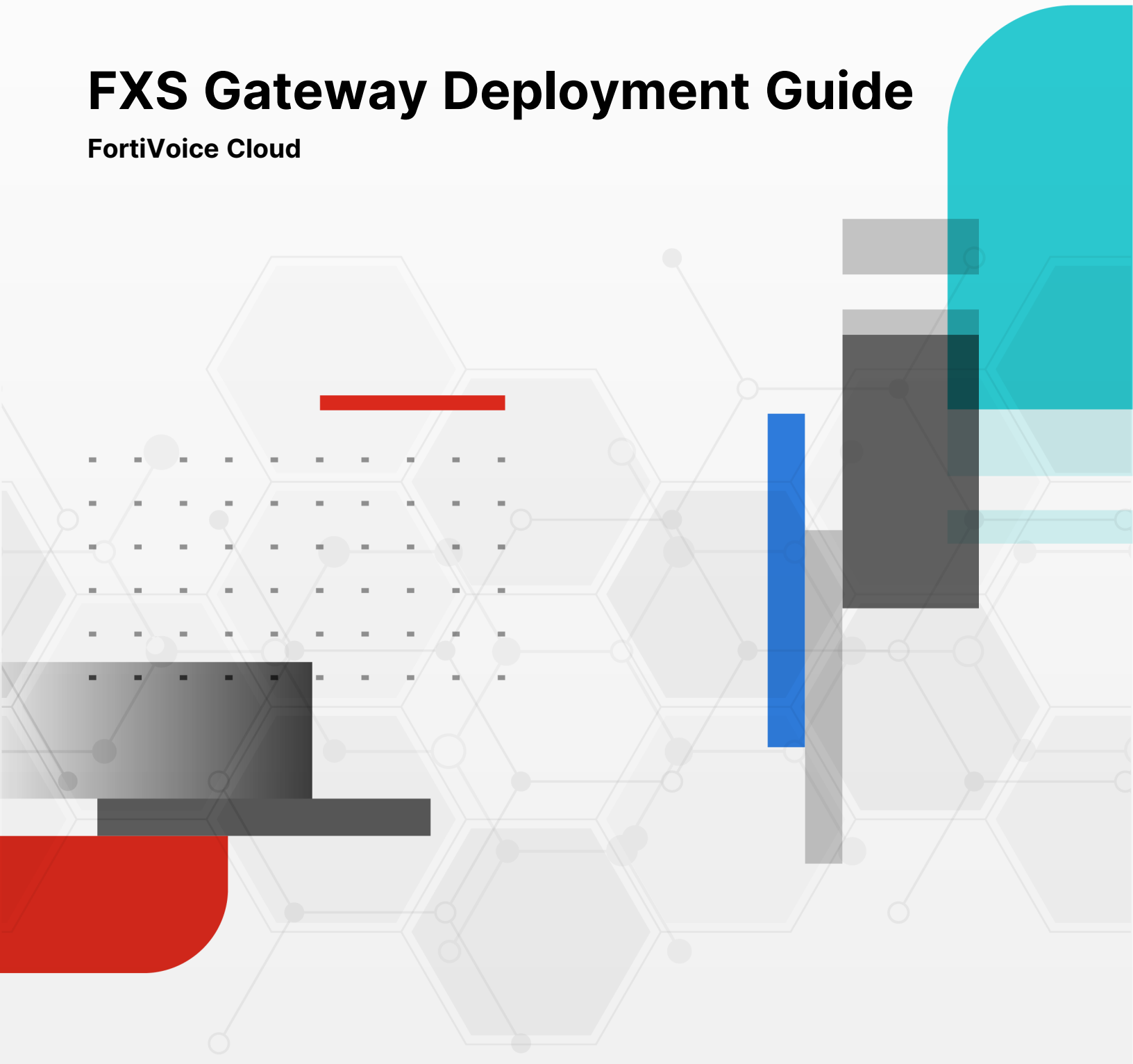
FXS Gateway Deployment Guide

FortiVoice Cloud



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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 27, 2025
FortiVoice Cloud FXS Gateway Deployment Guide
61-000-1015458-20251027

TABLE OF CONTENTS

Change log

Date	Change description
2025-10-27	Release of the FortiVoice Cloud FXS Gateway Deployment Guide

Overview

The FortiVoice foreign exchange subscriber (FXS) gateway works in conjunction with FortiVoice Cloud, a premier unified communication voice solution with all-inclusive calling and conferencing features, to expand resources and support additional analog phone extensions. With the FXS gateway, you can connect your traditional analog phones and fax machines to FortiVoice Cloud.

This document describes how to deploy a FortiVoice FXS gateway.

This section includes the following topics:

Supported models

The supported FortiVoice FXS gateway models are FortiVoice Gateway GS04, GS16, and GS24.

- GS04 has 4 FXS ports mapped to 4 analog phone extensions.
- GS16 has 16 FXS ports mapped to 16 analog phone extensions.
- GS24 has 24 FXS ports mapped to 24 analog phone extensions.

For more information about features and specifications, see the FortiVoice Gateways Data Sheet.

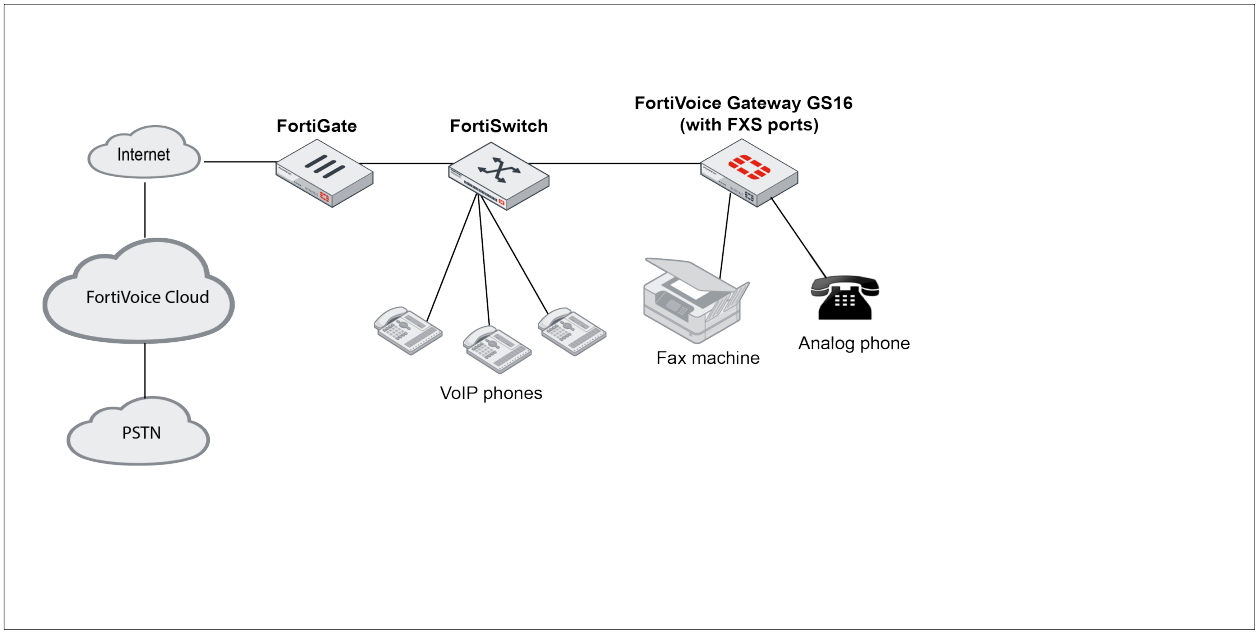
Topology

You can create a FortiVoice FXS gateway topology by using the Internet. Calls between extensions are always routed through FortiVoice Cloud.

FortiVoice Cloud 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 FortiVoice Cloud and connect to its GUI. For more information, see the FortiVoice Cloud Basic Administration Guide and FortiVoice Cloud Advanced Administration Guide.

To deploy an FXS gateway and then manage that device with FortiVoice Cloud, 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: • 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 GUI of the FXS gateway.	Connecting to the FXS gateway on page 8
Task 3	Configure the following system settings: • Network interfaces • Static routes • Administrator accounts • System options • SIP 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 11
Perform tasks 5 to 8 on FortiVoice Cloud, as applicable.		
Task 5	Add an FXS gateway.	Adding an FXS gateway to FortiVoice Cloud on page 12
Task 6	Apply the gateway configuration file from FortiVoice Cloud to the FXS gateway.	Applying the FXS gateway configuration on page 14
Task 7	Verify that the FXS gateway is associated correctly with FortiVoice Cloud.	Verifying the FXS gateway association on page 14
Task 8	Optionally, edit any of the 16 default managed extensions.	Optional - Editing a managed extension of the FXS gateway on page 15

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 GUI of the FortiVoice Gateway.

Scenario	Procedure
You are connecting to the device for the first time.	Perform the steps in Connecting to the GUI of the FortiVoice Gateway on page 8.
You have reset the device configuration to its default state.	Perform the steps in Connecting to the GUI of the FortiVoice Gateway on page 8.
You are a returning user who has completed the basic configuration of the device.	Access the GUI using the IP address, administrative access protocol, administrator account, and password that you have already configured, instead of the default settings. 1. Start a web browser and enter the URL: `https://<IP_address>/admin` Where `<IP_address>` is the IP address of the 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: `https://<IP_address>:446/admin`. 2. Enter the name and password associated with your account. 3. Click **Login**. You have completed this procedure. 4. Go to Configuring administrator and system settings on page 9 to make sure that you configure the required settings.

Connecting to the GUI of the FortiVoice Gateway

To connect to the GUI 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:
  - Google Chrome version 137
  - Microsoft Edge version 137
  - Mozilla Firefox Standard Release version 139
  - Apple Safari version 18.5
- 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 more information about accepting the certificate, see the documentation for your web browser.
6. In **Name**, enter `admin`.
7. Leave the **Password** field empty. In its default state, there is no password for this account.
8. Click **Login**.
   With a successful login, the GUI appears.
9. Set the password for this account:
   a. In the right corner of the GUI, click **admin**.
   b. Click **Change Password**.

   Enter 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

Configure administrator and system settings on the FortiVoice Gateway by completing the following procedures:

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 GUI 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 GUI 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**.

Configuring system options

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

1. In the GUI 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 GUI 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 11.

Upgrading the FXS gateway firmware

By default, when you apply the configuration on FortiVoice Cloud (*Managed System > Gateway > FXS Gateway > Actions > Apply Configuration*) to the gateway, firmware automatic upgrade function is enabled on the gateway. The gateway will automatically check for new firmware daily and then upgrade if it finds a higher version or a newer image than the current one.

Even with the firmware automatic upgrade function enabled, you can still manually upgrade the FXS gateway firmware based on the firmware version on your gateway. However, if the upgraded version is lower than what FortiVoice Cloud has for the gateway, it will be overwritten when FortiVoice Cloud does its daily automatic check.

Procedure steps

1. Identify the firmware version that is running on the gateway:
   a. In the GUI 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 Support website.
   b. Log in to your existing account or register for an account.
   c. Click **Support** and then in **Downloads**, click **Firmware Download**.
   d. In **Select Product**, select **FortiVoice**.
   e. In the **Release Notes** tab, review the FortiVoice 7.0 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.
   h. Go to Adding an FXS gateway to FortiVoice Cloud on page 12.
   i. 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 v7.00 directories to locate the firmware image file. For example, FVG_GS16-v70-build0094-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. Back up the configuration file:
   a. In the GUI 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 GUI reloads correctly and displays all changes, clear the cache of your web browser and restart it.
5. Verify that the firmware is successfully installed:
   a. In the **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 Adding an FXS gateway to FortiVoice Cloud on page 12.

Adding an FXS gateway to FortiVoice Cloud

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

- You are preconfiguring FortiVoice Cloud before deploying the FXS gateway.
- You are setting up FortiVoice Cloud and locating the FXS gateway on the Internet.

This procedure requires the access to the GUI of the PRI gateway. For more information, see the Logging in to the FortiVoice Gateway GUI section of the FortiVoice Cloud Gateway Administration Guide.

Procedure steps

1. Connect to the GUI of the FXS gateway that you want to add to FortiVoice Cloud.
2. Go to **Dashboard > Status > Managed Device**.

   For more information, see the Managed Device widget section of the FortiVoice Cloud Gateway Administration Guide.
3. Make sure **Status** shows **Unmanaged**. You can only generate a device code for a unmanaged gateway in **Cloud Mode**.

If it is in **Managed** status and you want to disconnect the gateway from FortiVoice Cloud and add it back, click **Reset** to set it to **Unmanaged**.

4. Enable **Cloud Mode**.
5. Click  to copy the **Device Code**.

   If you need a new code, click **Regenerate**.
6. If the **Cloud tunnel connection status** shows **Failed**, click **Restart Connection**.
   The gateway and the tunnel server must be connected because FortiVoice Cloud fetches the gateway information from the tunnel server using the device code.
7. Connect to the GUI of FortiVoice Cloud.

   For more information, see the Logging in to the FortiVoice admin portal section of the FortiVoice Cloud Advanced Administration Guide.
8. Go to **Managed System > Gateway**, and then click the **FXS Gateway** tab.
9. Click **New**.
10. Configure the following settings:

GUI field	Description
Enabled	Select to activate the configuration of the FXS gateway.
Device Code	Paste the device code that you copied from the FXS gateway GUI into the field and click **Fetch Device Information**. This enables FortiVoice Cloud to connect to and manage the gateway.
Name	Enter a unique name to identify the FXS gateway.
Display name	Not required. You can leave this field empty.
Serial number	The serial number of the FXS gateway that you are adding to FortiVoice Cloud. This is auto-populated and read-only after FortiVoice Cloud connects to the gateway by clicking **Fetch Device Information** in the **Device Code** field.
Type	The type of gateway that you are adding to FortiVoice Cloud. This is auto-populated and read-only after FortiVoice Cloud connects to the gateway by clicking **Fetch Device Information** in the **Device Code** field.
MAC address	The MAC address of the FXS gateway that you are adding to FortiVoice Cloud. This is auto-populated and read-only after FortiVoice Cloud connects to the gateway by clicking **Fetch Device Information** in the **Device Code** field.
Description	Optionally, add any applicable notes for this FXS gateway.

11. Click **Create**.
    FortiVoice Cloud creates the default managed extensions for your first FXS gateway. Taking GS16 as an example, FortiVoice Cloud creates 16 default managed extensions from 7801 to 7816 for your first FXS gateway. With any subsequent FXS gateway addition, FortiVoice Cloud continues to add a range of 16 extensions to the

existing managed extension list. For example, FortiVoice Cloud adds extensions 7817 to 7832 for the second FXS gateway.

If FortiVoice Cloud 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, FortiVoice Cloud has extension 7812. With the addition of the first FXS gateway GS16, FortiVoice Cloud 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**.

12. Go to Applying the FXS gateway configuration on page 14.

Applying the FXS gateway configuration

FortiVoice Cloud stores a gateway configuration file. Perform this procedure to apply this gateway configuration file to the FXS gateway.

Procedure steps

1. Connect to the GUI of FortiVoice Cloud.
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 **Actions** > **Apply Configuration**.
   FortiVoice Cloud displays the following message:
   Do you want to update the 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:
   The gateway update is complete.
   Successful:<gateway_name>
6. Click **OK**.
   You have completed this procedure.
7. Go to Verifying the FXS gateway association on page 14.

Verifying the FXS gateway association

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

Procedure steps

1. Connect to the GUI of FortiVoice Cloud.
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 15.

Editing a managed extension of the FXS gateway

After adding a FortiVoice Gateway to FortiVoice Cloud, each of its FXS port is associated with a generated extension number. To edit an FXS gateway extension, perform this procedure.

Procedure steps

1. Connect to the GUI of FortiVoice Cloud.
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 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
Enabled	Select to activate the extension.
Number	The extension number. For more information about the extension number pattern, see the Configuring FortiVoice Cloud options section in the FortiVoice Cloud Advanced Administration Guide. **Edit Preference**: For more information about extension user preferences, see the Setting extension user preferences section in the FortiVoice Cloud Advanced Administration Guide.
User ID	The system automatically generates this ID based on the gateway and port. This parameter is read only.
Display name	The caller ID for internal calls. Enter the name that the phone can display when it receives a call from this extension.
External caller ID	The caller ID you want to display on a called phone instead of the FortiVoice main number.
Voice DID Number	Click to map a DID number to this extension for voice communication.
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.
Emergency zone type	Select how you want the assignment of an emergency zone to be made:

GUI field	Description
	• *Static*: Manually select the *Emergency zone* profile for the extension. • *Dynamic*: This is not recommended for gateways deployed in FortiVoice Cloud. You allow the gateway to identify where the phone of the emergency caller is on the network. When a phone user calls an emergency number, the gateway checks where the calling phone is and assigns a matching emergency zone profile to the phone. This assignment is useful when phone users move their phones to different places on the network.
Emergency zone	Select the emergency zone profile for the gateway. You can click *New* to create a new profile or *Edit* to modify the selected one. For more information, see Configuring emergency zone profiles in FortiVoice Cloud Advanced Administration Guide.
Fax Enabled	Enable to allow the gateway to send and receive faxes.
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**.
User password	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. To let the system create the user password, click **Generate**. To show the user password, click the eye icon  .
LDAP profile	If you selected **LDAP** as the **Authentication type**, select or create an LDAP profile to apply to this extension. For more information about the LDAP profile configuration, see the Configuring LDAP profiles section in the FortiVoice Cloud Advanced Administration Guide.
Authentication ID	During the configuration of the LDAP profile, you have two options for the user authentication: • 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

GUI field	Description
	LDAP profile. Example: `jdoe`. • If you select **Search User and Try Bind DN**, leave the authentication ID field blank.
User Setting, Phone Access	
Voicemail PIN	For the extension user to access the extension voicemail and the user web portal, enter the password. To let the system create the voicemail PIN, click **Generate**. To show the voicemail PIN, click the eye icon .
Personal code	Enter the extension specific account code used to restrict calls. To make a restricted call, you need this code. To let the system create the personal code, click **Generate**.
User Setting, Cloud	FortiFone-x80 phones use these settings to log in to FortiVoice Cloud.
Cloud ID	This is the system-generated ID. Ignore "-" when entering this ID on the phone.
Extension	The extension number of the phone.
Cloud PIN	Click **Generate** to get a PIN.

6. To save the changes, click **OK**.
   You have completed this procedure.
7. Send the extension changes to the FXS gateway by following the instructions in Applying the FXS gateway configuration on page 14.

www.fortinet.com