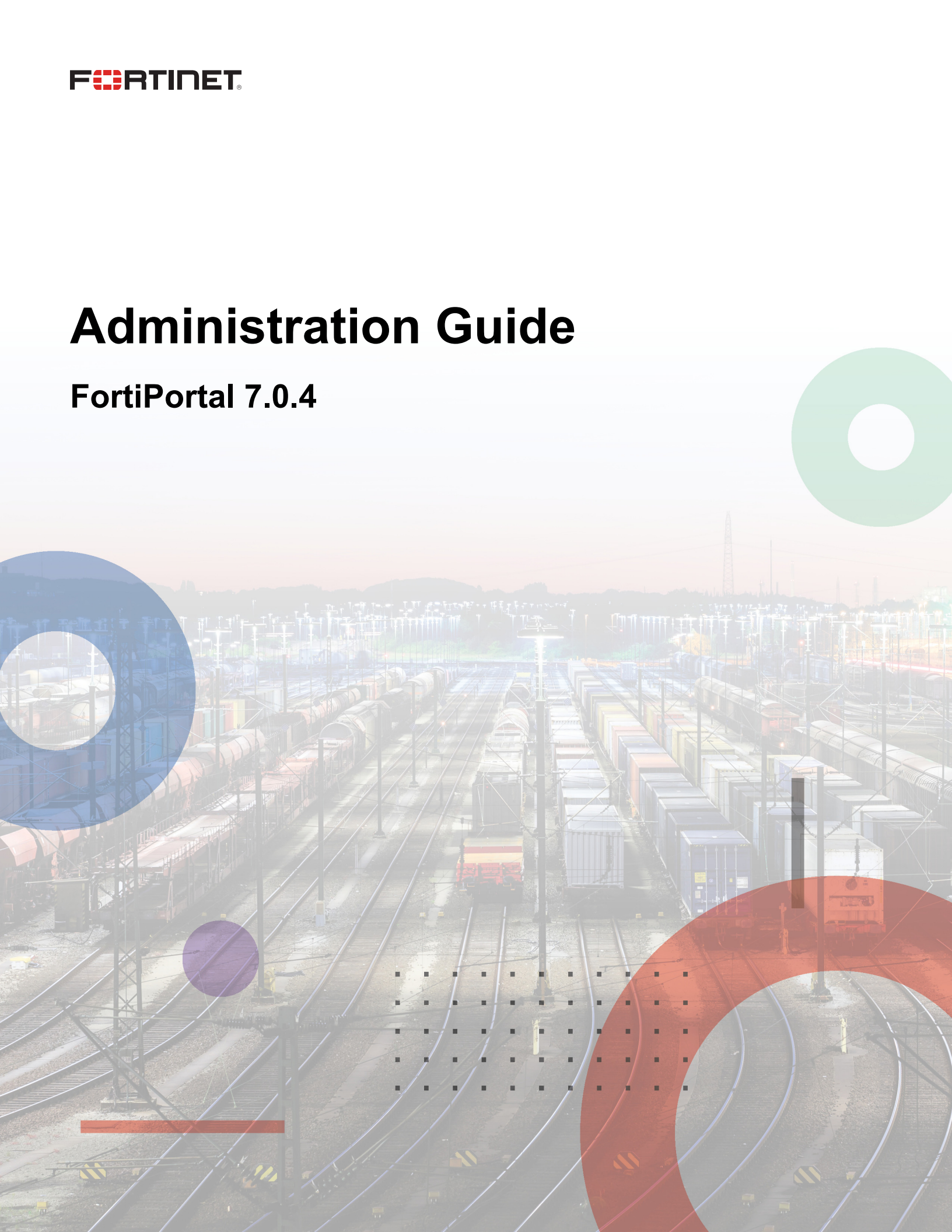


# Administration Guide

**FortiPortal 7.0.4**



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING 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](mailto:techdoc@fortinet.com)



September 14, 2023

FortiPortal 7.0.4 Administration Guide

37-704-908338-20230914

# TABLE OF CONTENTS

<b>Change Log</b>	<b>6</b>
<b>Overview</b>	<b>7</b>
Licensing	7
Mixed-license scalable cluster	7
FortiFlex	8
More information	9
Key features	9
Language support	10
Components	10
Organization devices	11
FortiPortal concepts	12
Sites	12
Remote authentication	12
Trusted and blocked hosts	12
Frequently asked questions	13
<b>Installation</b>	<b>14</b>
Installation on VMware	14
Downloading virtual machine image files	14
Installing FortiPortal VMs	15
Starting the VM	16
Basic setup	16
Sizing	16
Default login credentials	16
Configuring FortiPortal	17
FortiManager configuration	18
FortiAnalyzer configuration	19
Additional setup tasks	19
<b>Upgrading FortiPortal</b>	<b>20</b>
Upgrading from 7.0.3 to 7.0.4	20
Upgrading from 7.0.1 to 7.0.2	20
Upgrading from 6.0.12 or 6.0.13 to 7.0.2 or 7.0.3	21
Notes	22
<b>Header</b>	<b>24</b>
Help	24
Alerts	24
Change Password	24
API key	24
Logout	25
<b>Dashboard</b>	<b>26</b>
Widgets	26
System Information	26
Cluster Information	27
License Status	27

License Distribution .....	27
FortiManager Status .....	28
FortiAnalyzer Status .....	28
Top 10 Organizations .....	28
Firmware Management .....	28
Backup and restore .....	28
Backup and restore of standalone instances .....	28
Backup and restore of scalable cluster .....	29
<b>Organizations .....</b>	<b>30</b>
Organization page actions .....	30
Create or edit an organization .....	31
General .....	32
Contact .....	34
ADOMs .....	34
Sites .....	35
Users .....	37
User profiles .....	39
Authentication .....	40
Reports .....	41
Page actions .....	41
Additional organization configuration .....	42
<b>Devices .....</b>	<b>43</b>
FortiManager devices .....	44
Page actions .....	44
Add a FortiManager .....	44
Edit a FortiManager .....	44
Manage FortiGate, FortiSwitch, and FortiAP devices .....	45
FortiAnalyzer devices .....	46
Prerequisites .....	46
Page actions .....	46
Add a FortiAnalyzer .....	47
Edit a FortiAnalyzer .....	47
View FortiAnalyzer reports .....	47
<b>System .....</b>	<b>48</b>
Settings .....	49
General .....	49
Authentication .....	51
Blocked hosts .....	64
Scalable cluster .....	65
Email .....	67
Others .....	67
Profiles .....	68
Page actions .....	68
Create or edit a profile .....	68
Admins .....	69
Page actions .....	69
Create or edit an admin .....	70

---

Admin profiles .....	72
Theme .....	72
Theme options .....	72
Details of the theme configuration fields .....	73
Custom URLs and text .....	74
Select a predefined color scheme .....	76
Editing a custom color scheme .....	76
Disclaimers .....	95
Custom images .....	96
Resizing images .....	97
Additional Resources .....	99
Page actions .....	99
<b>Notifications .....</b>	<b>100</b>
Page actions .....	100
Create or edit a notification .....	100
<b>Audit .....</b>	<b>102</b>
Page actions .....	102
<b>Appendix A - Sizing recommendations .....</b>	<b>103</b>
<b>Appendix B - Installation on KVM .....</b>	<b>104</b>
Prerequisites .....	104
Downloading virtual machine image files .....	104
Deploying the FortiPortal Virtual Machine .....	104

# Change Log

Date	Change Description
2023-05-04	Initial release.
2023-05-11	Updated <a href="#">Remote authentication: SSO</a> on page 59.
2023-07-14	Updated <a href="#">Sizing recommendations</a> on page 103.
2023-09-14	Updated <a href="#">Prerequisites</a> on page 46.

# Overview

FortiPortal enables organizations to operate a cloud-based hosted security management and log retention service.

It provides organizations with centralized reporting, traffic analysis, configuration management, and log retention without the need to invest in additional hardware and software.

## Licensing

Two types of license are available for FortiPortal:

- Permanent: Perpetual license.
- Flexible (FortiFlex): Resources are allocated and billed on-demand.

Existing FortiPortal subscription licenses will be replaced with FortiFlex when renewed.



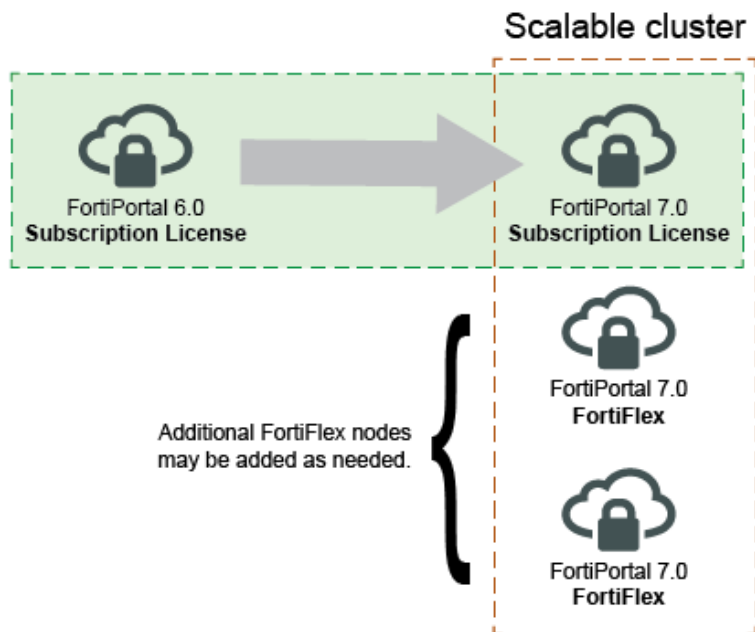
FortiPortal must have internet access (port 443) to `fortiguard.net` for licenses to be validated and installed.

---

## Mixed-license scalable cluster

A mixed-license cluster can be formed with nodes on a subscription license and nodes on FortiFlex. FortiFlex allows for more licenses to be added as needed.

The total license for the cluster is the license from the subscription nodes plus the licenses from the FortiFlex nodes.



Changing to a new license triggers a reboot of the FortiPortal instance.

When changing the license on a node in a scalable cluster, do not change the license on other nodes until the whole cluster is up and becomes stable after the reboot. Otherwise the license change may cause the cluster to be down and unrecoverable.

## FortiFlex

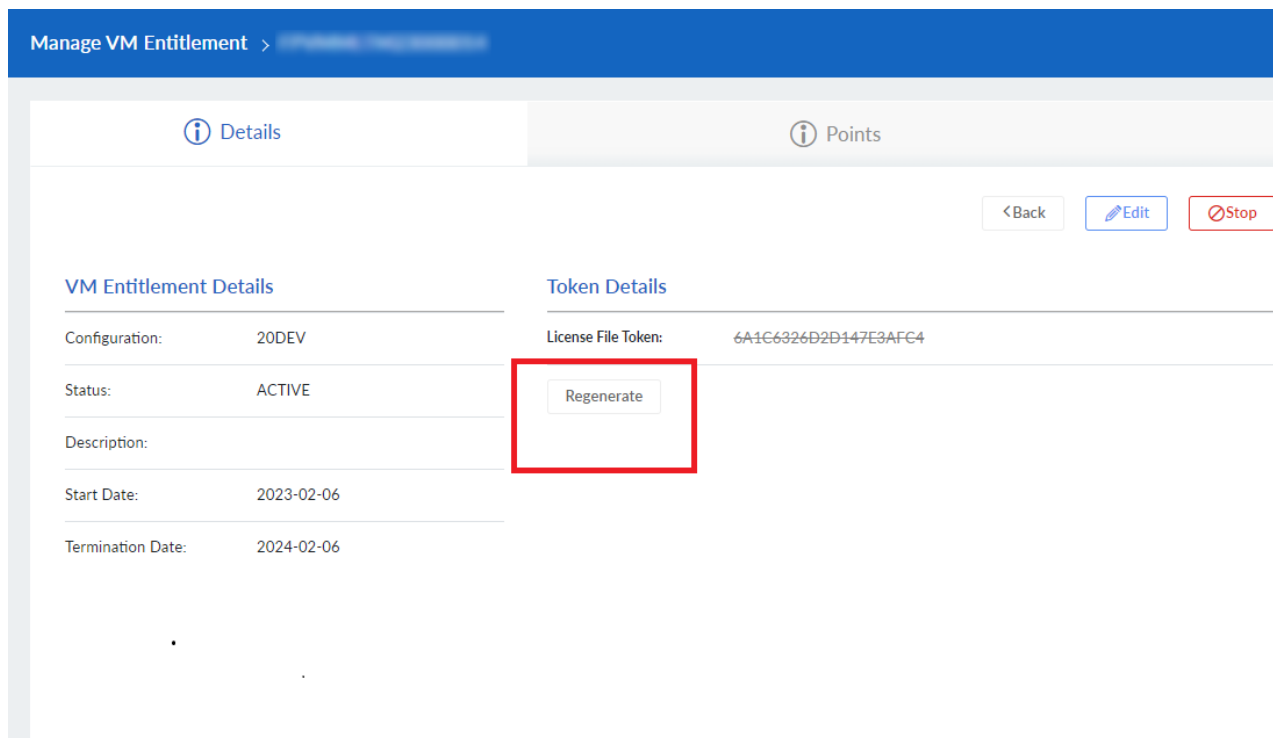
FortiPortal is part of the FortiFlex program.

MSSP partners can use points to create license entitlements for FortiPortal (7.0.3 and later). Moving to the FortiFlex licensing model does not introduce additional costs for existing FPC deployments.

### To create and use a FortiFlex entitlement for FortiPortal:

1. In FortiFlex, create a new VM configuration, with *Product Type* set to *FortiPortal Virtual Machine*.
2. In FortiFlex, create a new VM entitlement.
3. In FortiFlex, in the new VM entitlement, generate or regenerate a token.





4. Inject the FortiFlex license into the VM instance using the following command in the FortiPortal CLI:

```
execute vm-license <token>
```



The FortiFlex license injection command must be executed at least 5 minutes after the GUI is accessible when this FortiPortal instance has just started or upgraded.

## More information

For more information about licensing options, see [the FortiPortal data sheet at fortinet.com](#).

For more information about FortiFlex, see the [FortiFlex Administration Guide](#).

## Key features

FortiPortal provides the following features:

- Dashboard widgets for system and log status
- Log viewer with filters
- Drill-down analysis of user and network activity
- Report generator (with customization options)
- Wireless network status
- Device management

- Policy management
- Remote authentication using FortiAuthenticator



SNMP has been removed from FortiPortal 7.0 for technical reasons. It will be added in a future version.

---

## Language support

FortiPortal supports the following languages:

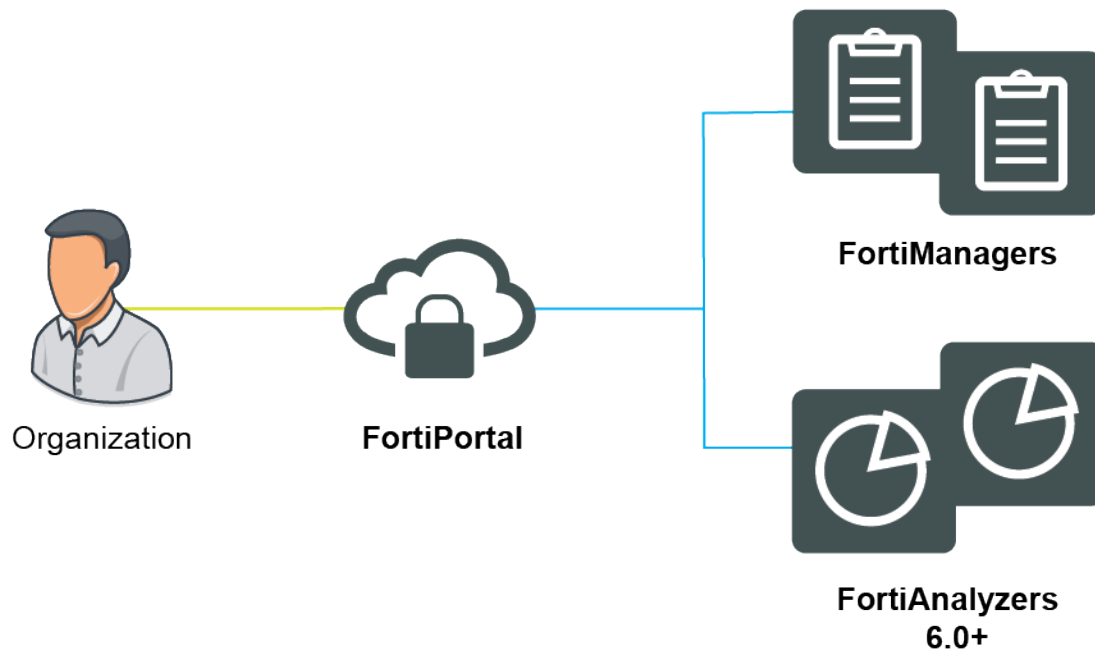
- English
- French
- German
- Portuguese
- Romanian
- Spanish
- Italian

## Components

In a typical network, FortiGate devices are managed by one or more FortiManagers. Optionally, FortiGate logs can be gathered by one or more FortiAnalyzers.

### FortiPortal

- Uses the FortiManager API to manage devices, objects, and policies.
- Aggregates FortiAnalyzer logs into a central database and performs security analytics on the logs.
- Provides an administrative web interface that allows the administrator to configure the services for each organization, and to manage the overall cloud service.
- Provides an organization web interface that enables each organization to access and analyze their data and administer their service.



For additional information about the organization web interface, see the [FortiPortal User Guide](#) (which is also available by selecting the help button in the organization web interface).

## Organization devices

FortiPortal requires that the organization FortiGate devices are managed by FortiManager.

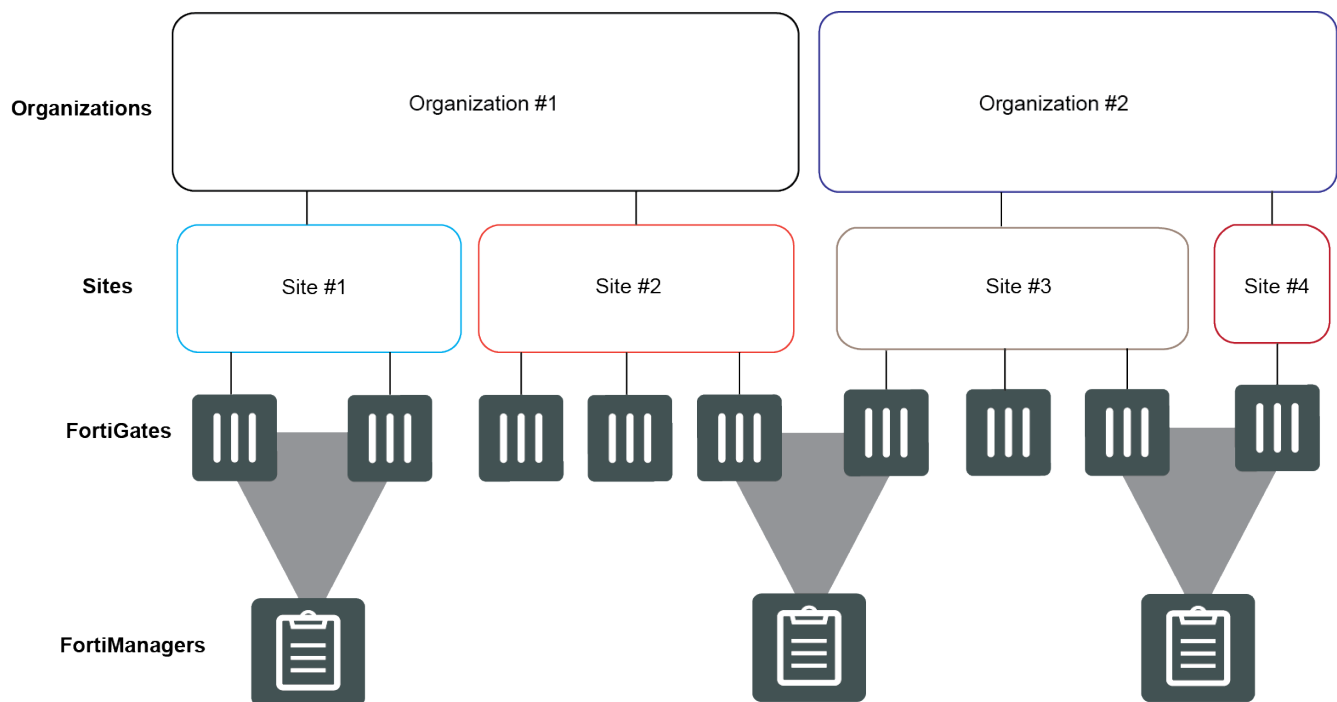
The FortiManager may reside in the organization network or in the cloud.

- **FortiGate:**
  - Provides network security in the organization environment
  - Generates security and access logs
  - Also fulfills the AP Wireless Controller role
- **FortiManager:**
  - Manages a set of FortiGate devices
  - FortiManager provides device information to FortiPortal
  - May be placed within the organization network or in the cloud
- (Optional) **FortiAnalyzer:**
  - Provides log analysis and reporting
  - May be placed within the organization network or in the cloud
- (Optional) **FortiSwitch:**
  - Provide secure network switching integrated with FortiGate
  - Placed within the organization network
- (Optional) **FortiAP:**
  - Provide secure wireless network access points integrated with FortiGate
  - Placed within the organization network

## FortiPortal concepts

### Sites

- An organization can have multiple sites.
- A site is a logical grouping of devices (independent of which FortiManager manages the device).
- Devices are FortiGate, FortiSwitch, or FortiAP devices.



### Remote authentication

You can choose remote authentication of admin and organization users. Remote authentication provides a choice of FortiAuthenticator, RADIUS, or single sign-on (SSO). The remote authentication method may be overridden at the organization level.

If you set the authentication mode to remote, all user management functions reside with the remote system. FortiPortal user management capabilities (add/modify/delete users, reset password, change password) are blocked, as these apply only to local users.

For additional information regarding FortiAuthenticator, refer to the [FortiAuthenticator product documentation](#).

### Trusted and blocked hosts

If you are using local user authentication, you can use the trusted and blocked hosts capability as an added level of security.

Enable the blocked hosts feature to enforce a configurable blocklist for all admin and users.

Enable trusted hosts in organization settings and create an allowlist of trusted hosts for each organization user.

For an organization with trusted hosts enabled, the system also enforces the global blocklist for the users.

## Frequently asked questions

### What should I do when I upgrade or replace a FortiGate or FortiGate VM managed by FortiManager?

Use the following procedure to upgrade the FortiGate or FortiGate VM OS version (in some cases, the FortiGate VM license might be new and will have a different serial number):

1. Upgrade the version of FortiGate or FortiGate VM.
2. In FortiManager, update the ADOM version on FortiManager.
3. Poll from FortiPortal.



There will be polling issues if you create a new ADOM with the latest version, move the device to the new ADOM, and then delete the old ADOM. Use the recommended procedure instead.

---

### I can see data in the dashboard as a site administrator but not as user. How do I fix this?

Click the *Users* tab when editing an *Organization*, select a user, and then click *Edit*. Check if the user has permission to view information related to all sites and the devices associated with those sites.

For example, a user might not have access to a device that is associated with the site. The site administrator can view the device because a superuser can access all devices and sites.

# Installation

This chapter covers the following tasks:

- [Installation on VMware on page 14](#)
- [Basic setup on page 16](#)
- [Additional setup tasks on page 19](#)

FortiPortal provides a self-service management interface for organizations to monitor and configure security instances without direct FortiManager access. FortiPortal is a web application that runs on virtual machines.



Remember to protect your FortiPortal installation with an external firewall. Organization users should only connect to the portal interface. They should not directly connect to FortiManager.

---

## Installation on VMware

This chapter assumes some familiarity with the VMware vSphere Client terminology.

All VM instances run on VMware ESXi Server versions 6.0, 6.5, 6.7, and 7.0.

Before deploying FortiPortal on VMware, install the [VMware vSphere Client](#) on the management computer.



For KVM, see [Installation on KVM on page 104](#).

---

## Downloading virtual machine image files

**To download the VM files:**

1. Go to [FortiCloud](#) and log in to your account.
2. Go to *Support > Downloads > Firmware Download*.
3. Select FortiPortal.
4. Click the *Download* tab.
5. Navigate to the appropriate directory.
6. Download and extract the OVA package to a local folder on the management computer.

## Installing FortiPortal VMs

### To install FortiPortal:

1. Deploy a VM instance. See [Deploying a VM instance on page 15](#).
2. Configure VM hardware settings. See [Configuring VM hardware settings on page 15](#).
3. Power on the VM. See [Starting the VM on page 16](#).
4. Configure the portal parameters. See [Basic setup on page 16](#).

The first time you start the portal, you will have access only through the console window of your VM server environment. After you configure the initial parameters, you can access FortiPortal through the web-based portal.

## Deploying a VM instance

### To deploy a VM instance:

1. Launch the VMware vSphere client.
2. Enter the IP address or host name of your VMware server.
3. In the *Inventory* menu, select the physical server where you will install the VM.
4. Select *File > Deploy OVF Template* to launch the OVF Template wizard. The wizard will guide you through a series of deployment steps.
5. *Source*: Use the Browse function to locate the OVF file that you downloaded.
6. *OVF Template Details*: This page displays the following information: FortiPortal version, size of the download, and application size on disk.  
Click *Next*.
7. *End-user License Agreement*: Accept the end-user license agreement and click *Next*.
8. *Name and Location*: Enter a name for this virtual machine, select a location from the location inventory, and click *Next*.
9. *Storage*: Select the destination storage for the virtual machine files and click *Next*.
10. *Disk Format*: This page displays the storage device that you selected in the previous step, along with available space. Select *Thin Provision* and click *Next*.
11. *Network Mapping*: Select the destination network to map to the source network in your OVF and click *Next*.
12. *Ready to Complete*: Review the deployment settings. Select *Back* to make any changes. When ready, click *Finish*.

## Configuring VM hardware settings

### To configure the VM settings:

1. Select the newly created VM in the inventory list and go to *Getting started > Edit virtual machine settings*.
2. Adjust the CPU, memory, and storage settings and click *Save*.

The following are the minimum requirements:

- CPU: 4
- Memory: 16 GB
- Hard drive: 12 GB

See [Sizing recommendations on page 103](#) for more information.



FortiPortal interacts with FortiManager. To avoid the portal becoming a bottleneck, adjust the maximum CPU and memory sizes so that they equal the values for the FortiManager devices.

---

## Starting the VM

### To start the virtual machine:

1. In the inventory list, right-click the FortiPortal VM that you just deployed and click *Power On*.
2. Right-click on the instance and click *Open Console* to see the login prompt.

## Basic setup

This section covers the following tasks:

- [Sizing on page 16](#)
- [Default login credentials on page 16](#)
- [Configuring FortiPortal on page 17](#)
- [Basic setup on page 16](#)
- [FortiManager configuration on page 18](#)
- [FortiAnalyzer configuration on page 19](#)

## Sizing

FortiPortal sizing can be complex. Fortinet recommends that you work with your Fortinet systems engineer when possible.

The default storage disk size is 12 GB, which is the recommended minimum. If you have many organization logins and many devices, increase the memory and disk sizes for improved performance.

See [Sizing recommendations on page 103](#) for more information.



FortiPortal requires at least 16 GB of memory.  
The default memory size is 16 GB.

---

## Default login credentials

The following are the default user names and passwords for FortiPortal:



Component	Default User Name	Default password
Console/SSH	admin	portal1234
Portal GUI	spuser	test12345



The login credentials are separated between the portal GUI and console/SSH.

## Configuring FortiPortal

### To configure the portal:

- Before you can access the GUI, you must configure the VM with an IP address and administrative access using the CLI.
  - Log in to the console using the default console/SSH credentials. On the first login, you are required to change the *admin* user password.
  - In the CLI console, enter the following commands to configure the IP address and netmask:

```
config system interface
    edit port1
        set ip x.x.x.x/24
    end
```

If needed, configure additional ports (port2, port3, etc.) in the same manner.



Subnet ranges 10.43.0.0/16 and 10.42.0.0/16 are reserved for system internal use and can not be configured on any port.

- In the CLI console, enter the following commands to configure the default route for the instance:

```
config system route
    edit 1
        set device port1
        set gateway x.x.x.x
    end
```

- Optionally, in the CLI console, enter the following commands to configure the DNS servers for the instance:

```
config system dns
    set primary x.x.x.x
    set secondary y.y.y.y
end
```

- Optionally, in the CLI console, enter the following commands to configure the NTP server for the instance:

```
config system ntp
    config ntpserver
        edit 1
            set server x.x.x.x or <hostname>
        end
    end
```



The NTP source should be the same for all portal VMs to synchronize the log time stamps across all devices.

2. Connect to FortiPortal via the GUI using the configured IP address and the default portal GUI credentials. After logging in and successfully uploading the license file, you must change the login credentials.
3. Upload the license file. Select your valid license file and then click *Upload*. The license is validated and the *Dashboard* loads.
4. Change the *spuser* password. After the first login, you are required to change the password.

## Updating the SSL certificate file



If you are setting up a demo server, you can skip this procedure.

Use the following steps to import an SSL certificate.

In the Admin portal, go to *System > Settings > General* to display information about the SSL certificate.

*Certificate Information* displays the *Certificate* and *Private Key* file name. You can select and upload a new certificate and private key in PKCS #8 format.

## FortiManager configuration

### To configure FortiManager to work with FortiPortal:

1. ADOM mode must be enabled on FortiManager to work with FortiPortal. If needed, enable advanced adom-mode on FortiManager so that you can add VDOMs on the same physical device to different ADOMs.

In the FortiManager CLI, run this command to enable ADOMs (and optionally set the ADOM mode to *advanced*):

```
config system global
    set adom-status enable
    set adom-mode advanced
    y
end
```

2. On FortiManager, create an admin user with read/write permission:

```
config system admin user
    edit <username>
        set profileid Super_User
        set adom all_adoms
        set policy-package all_policy_packages
        set password <password>
        set rpc-permit read-write
    next
end
```

3. Enable workspace mode on FortiManager to work with FortiPortal:

```
config system global
    set workspace-mode normal
```

end

4. Add your FortiManager device to FortiPortal. You must poll FortiManager to see the device list.

For more information about adding FortiManagers to the portal, see [FortiManager devices on page 44](#).

## FortiAnalyzer configuration

### To configure FortiAnalyzer to work with FortiPortal:

1. ADOM mode must be enabled on FortiAnalyzer to work with FortiPortal. You must enable the interface permission `https` on FortiAnalyzer for the portal-facing interface.
2. On FortiAnalyzer, create an admin user with read/write remote procedure calls enabled:

```
config system admin user
  edit <user_name>
    set profileid Super_User
    set rpc-permit read-write
  end
```

For more information about adding FortiAnalyzers to the portal, see [FortiAnalyzer devices on page 46](#).

## Additional setup tasks

After performing the basic installation, complete these additional setup tasks:

- To add additional FortiManager devices, see [FortiManager devices on page 44](#).
- To add wireless controllers, see [Manage FortiGate, FortiSwitch, and FortiAP devices on page 45](#).
- To add FortiAnalyzer devices, see [FortiAnalyzer devices on page 46](#).
- To create an organization, see [Create or edit an organization on page 31](#).
- To create sites, see [Sites on page 35](#).
- To create site administrators, see [Users on page 37](#).

# Upgrading FortiPortal

Follow the instructions below to upgrade to FortiPortal 7.0.4.

## Upgrading from 7.0.3 to 7.0.4

You can upgrade from FortiPortal 7.0.3 to 7.0.4 directly through the FortiPortal dashboard using the *Upgrade Firmware* button with the FortiPortal 7.0.4 OVA file. See [Firmware Management on page 28](#).

Suggested upgrade paths:

- 7.0.1 > 7.0.2 > 7.0.3 > 7.0.4.
- 6.0.12 > 7.0.2 > 7.0.3 > 7.0.4.



You can upgrade from FortiPortal 7.0.2 to 7.0.3 directly through the FortiPortal dashboard using the *Upgrade Firmware* button with the FortiPortal 7.0.3 OVA file. See the special instructions below for upgrades from earlier versions.

---

## Upgrading from 7.0.1 to 7.0.2

You can upgrade from FortiPortal 7.0.1 to 7.0.2.



Due to fundamental system changes, a direct upgrade from FortiPortal 7.0.1 to 7.0.2 is not possible. Follow the upgrade procedure below to upgrade from 7.0.1 to 7.0.2.

---



See [Upgrading from 6.0.12 or 6.0.13 to 7.0.2 or 7.0.3 on page 21](#) for information about upgrading FortiPortal 6.0.12 or 6.0.13 to 7.0.2 or 7.0.3.

---

### To upgrade FortiPortal to 7.0.2:

1. Save a backup of your existing FortiPortal 7.0.1 system:
  - a. Go to *Dashboard*.
  - b. In the *System Information* pane, select the *System Backup* icon in *System Configuration* to save a backup file onto the local computer.  
For a scalable cluster, back up the primary node.
2. Shut down your FortiPortal 7.0.1 VM.
3. Download and deploy the *FPC\_VM64-V7.0.1-build8000-release-Portal.ova* image. This image is available to download from the Fortinet Customer Service & Support website (<https://support.fortinet.com/>).

4. In this instance, go to *Dashboard > System Configuration*, click *Restore System*, and upload the backup file you saved previously. The system reboots when the restore process is complete.
5. In the *System Information* pane, in *Version*, click the *Upload Firmware* icon, click *Choose File* and locate the firmware image for FortiPortal 7.0.2 on your local computer.
6. Click *Upload*



Uploading a firmware image requires sufficient network bandwidth.  
When upgrading a scalable cluster, the upgrade may take 10-20 minutes, or longer, depending on server performance.

---

The firmware image uploads from your local computer to the FortiPortal, which will then reboot.  
The license may display *N/A* but it will become valid after about two hours.

**To upgrade the secondary nodes of a scalable cluster:**

1. Shutdown the secondary nodes.
2. Download and deploy two or more new FortiPortal 7.0.2 instances.
3. Join these new instances to the primary node in the scalable cluster.

## Upgrading from 6.0.12 or 6.0.13 to 7.0.2 or 7.0.3

FortiPortal may be upgraded from 6.0.12 or 6.0.13 directly to 7.0.2 or 7.0.3. You must first upgrade your system from any earlier version to 6.0.12.



See [Notes on page 22](#) for important details that may affect your upgrade.

---

**To upgrade FortiPortal 6.0.12 or 6.0.13 to 7.0.2 or 7.0.3:**

1. Create a MySQL backup file from your current FortiPortal database.  
The backup file can be created by running this command in your terminal:  
`mysqldump -u[Your_User_Name] -p[Your_Password] --all_databases > [Your_FileName]`  
Example: `mysqldump -uJohnDoe -pPassword --all_databases > MyFPCv6.sql`
2. Download the `upgrade_tool` script from the Fortinet Customer Service & Support website (<https://support.fortinet.com/>):
  - a. Log into FortiCloud.
  - b. Click *Support* in the header menu, then select *Firmware Download*.
  - c. In *Select Product*, select *FortiPortal*.
  - d. In the *Download* tab, navigate to *FortiPortal > v7.0.0 > 7.0 > 7.0.2*.

- e. Click `upgrade_tool` to download the script.

The same script is used for upgrading to 7.0.2 and 7.0.3.

This script processes your database backup file and outputs a new file you will upload to your new FortiPortal 7.0.2 or 7.0.3 installation.

The upgrade tool must be run in a Linux environment. The required version is Ubuntu 20.04 with Python 3.9.x or higher. Other operating system families such as Debian and CentOS are not verified and are not guaranteed to work successfully.

It requires root (`sudo`) access to run.

3. In your terminal, run `chmod +x upgrade_tool` to make it executable.
4. Run `sudo ./upgrade_tool`. When prompted, input your linux system password.
5. At the prompt `Please enter your file name:`, enter the path to the MySQL dump file you created in step 1. For example, `MyFPCv6.sql`.  
After the upgrade tool finishes running, a file `fpc_upgrade.bk` is created.
6. Shutdown the current FortiPortal VM.
7. Install a new FortiPortal 7.0.2 or 7.0.3 VM (see [Installation on page 14](#)).
8. In the new FortiPortal, go to *Dashboard > System Configuration*, click *Restore System*, and upload the `fpc_upgrade.bk` file. The system reboots when the restore process is complete.



The upgrade tool also generates a JSON file named `user_pwd` that contains pairs of usernames and temporary passwords for all of the users on your FortiPortal installation. Users may login with the temporary password and then update their passwords.



After you shutdown your current FortiPortal VM, you must wait two hours for the license to be released to use it on the new FortiPortal 7.0.2 or 7.0.3 VM.

## Notes

- Themes, alerts, and FortiAP devices are not retained in this upgrade process.
- You must re-enter the passwords for all connected FortiManagers and FortiAnalyzers.
- If SMTP email authentication is enabled, you must re-enter that password.
- User `spuser` from FortiPortal 6 is changed to `spuser_old`.
- The authentication method is reset to `local`.  
If re-enabling remote authentication, you must to re-enter the *Remote Server Key* (FortiAuthenticator and RADIUS) but other remote authentication info is retained.
- Users will need to use their temporary password from the `user_pwd` file generated by the upgrade tool to log in.
- The policy installation scheduler installation time is reset to `00:00`.
- The FortiManager device repo status is set to *Unknown*, as there is no such data in the previous version.
- Device display name are now in the format of `{adom}/{serial_number}/vdom`.
- All profiles now have a prefix of `v6-` (for example, `v6-System Admin`).
- Any role with a combination of multiple roles is converted into a new profile with a new name combining the roles (for example, `v6-foo_v6-bar`).

- FortiPortal 6.0 and 7.0 have different permission control designs. These are the permission changes made during the upgrade:
  - *Provider > Organization*: If *Customer*, *Sites*, and *Reports* permissions are different, *Organization* is set to *Custom*.
  - *Provider > Device*: If FortiManager and FortiAnalyzer have different permissions, *Device* is set to *Custom*.
  - *Provider > System*: If Settings/Profile/Admins/Themes have different permissions, *System* is set to *Custom*.
  - *Provider > Additional Resources*: Set to *Read*.
  - *Provider > Notification*: Set to *Read*.
  - *Provider > Audit*: Set to *Read/Write*.
  - *Customer > Insights*: If *Dashboard*, *Monitor*, *Health*, and *Logs* have different permission, *Insights* is set to *Custom*.
  - *Customer > Insights > Monitors*: Shares the same permissions as *Logs*.
  - *Customer > Insights > Logs*: If *Traffic*, *IPS*, *Sandbox*, *AV*, *DNS*, *App-Control*, *Web-Filter*, and *Event* have different permissions, *Logs* is set to *Custom*.
  - *Customer > Security*: If *Policy*, *Firewall*, *Network*, *Routing* have different permissions, *Security* is set to *Custom*.
  - *Customer > Security > Policy*: Everything under *Policy* retains permissions from FortiPortal 6.0.
  - *Customer > Security > Objects*: If not everything under *Objects* share the same permissions, *Firewall Objects* is set to *Custom*.
  - *Customer > Security > Network*: If not everything under *Network* shares the same permissions, *Network* is set to *Custom*.
  - *Customer > Security > Routing*: Set to *None*.
  - *Customer > SD-WAN*: If *Monitoring* and *Configuration* have different permissions, *SD-WAN* is set to *Custom*.
  - *Customer > Switch*: Set to *None*.
  - Any other permissions that are new in FortiPortal 7.0 are set to *None*.

## Header

The header appears on all pages in FortiPortal.

Click the icons on the right side of the header to access these functions:

- [Help](#)
- [Alerts](#)
- [Change Password on page 24](#)
- [API Key](#)
- [Logout](#)

## Help

Click the *Help* icon to open the FortiPortal help documentation.

## Alerts

Click the *Alerts* icon to open a *Notifications* window. By default, the window displays alerts from the last 60 minutes.

See [Notifications on page 100](#) for more information.

## Change Password

**To change your password:**

1. In the header, click on the cog icon, then click *Change Password*.
2. Enter your existing password and a new password, confirm the new password, then click *Save*. The new password will take effect on your next login attempt.

## API key

Click the cog icon, then click *API Key* to open the *New API Key* dialog.

See the [FortiPortal API Guide](#) for more information.

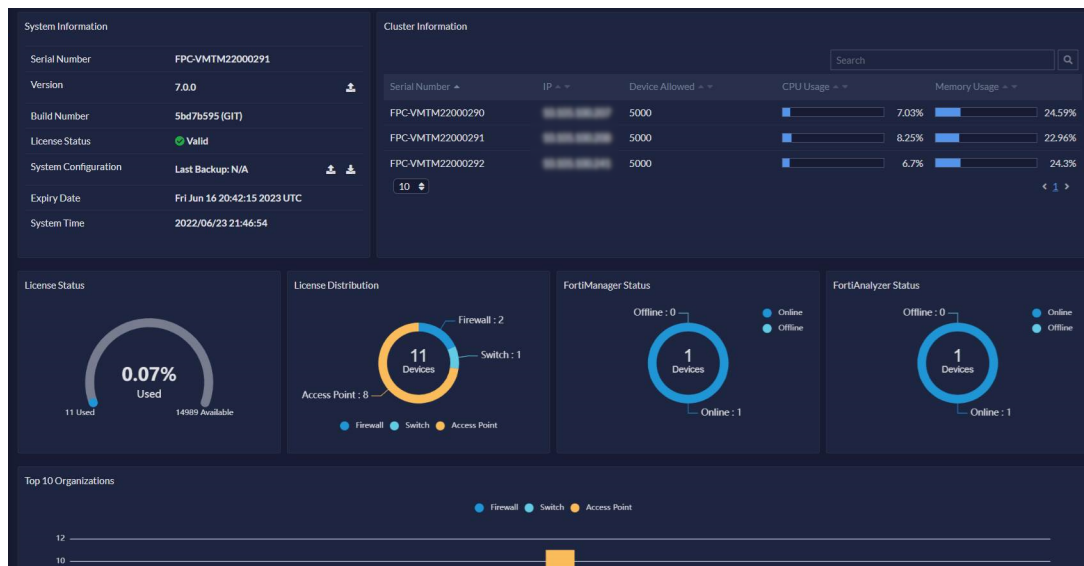


## Logout

Click the *Logout* icon to log out immediately.

# Dashboard

The dashboard displays information about the system and connected devices, presented in an array of widgets.



After FortiPortal begins to receive logs from connected devices, you might experience a delay of up to 15 minutes before the aggregated data appears on the dashboard.

## Widgets

### System Information

The *System Information* widget includes the following information:

Field	Description
Serial Number	FortiPortal serial number.
Version	FortiPortal version. Click the <i>Upload Firmware</i> icon to open the <i>Firmware Management</i> dialog. See <a href="#">Firmware Management</a> .
Build Number	FortiPortal build number.
License Status	FortiPortal license status. To upload a license, see <a href="#">Upload a license on page 50</a> .
System Configuration	Last backup and restore activity.

Field	Description
	See <a href="#">Backup and Restore</a> .
Expiry Date	Expiry date of the license.
System Time	The system time. To change the system time, update the <i>Time Zone</i> option in <a href="#">General on page 49</a> .
CPU Usage	Percentage of CPU usage. Displays only when scalable cluster is not enabled. When scalable cluster is enabled, this information is displayed for each instance in the <i>Cluster Information</i> widget.
Memory Usage	Percentage of memory usage. Displays when scalable cluster is not enabled. Displays only when scalable cluster is not enabled. When scalable cluster is enabled, this information is displayed for each instance in the <i>Cluster Information</i> widget.
Restart	Click to reboot the FortiPortal instance. Displays only when scalable cluster is not enabled.
Shutdown	Click to shutdown the FortiPortal instance. Displays only when scalable cluster is not enabled.

## Cluster Information

Scalable cluster-related information, including instance serial numbers, IP addresses, devices allowed, and CPU and memory usage.

This widget only appears if this FortiPortal instance is a member of scalable cluster.



- Use the search bar to look for cluster related information.
- Some columns have a sorting feature, allowing you to sort data in ascending or descending order.
- Use the *Show x entries* dropdown to set the number of entries per page.

## License Status

Percentage of devices used in the license.

## License Distribution

Number of FortiGate, FortiSwitch, and FortiAP devices in the license.

## FortiManager Status

FortiManager devices status.

## FortiAnalyzer Status

FortiAnalyzer devices status.

## Top 10 Organizations

Displays device counts for the top 10 organizations.

## Firmware Management



Before proceeding to upgrade your system, it is recommended that you back up your configuration. See [Backup and restore on page 28](#).

---

### To upgrade FortiPortal firmware:

1. Go to *Dashboard*.
2. In the *System Information* pane:
  - a. In *Version*, click the *Upload Firmware* icon.  
The *Firmware Management* dialog opens.
  - b. In *Upload Firmware*, click *Choose File* and locate the firmware image on your local computer.
  - c. Click *Upload*.  
The firmware image uploads from your local computer to FortiPortal, which then reboots.

## Backup and restore

### Backup and restore of standalone instances

Follow the procedures below to backup and restore the configuration of a standalone instance. If you are backing up or restoring a scalable cluster, see [Backup and restore of scalable cluster on page 29](#).

### To create a backup of the configuration:

1. Go to *Dashboard*.
2. In the *System Information* pane:
  - a. In *System Configuration*, click the *Backup System* icon to download a backup file to your local computer.

**To restore a backed-up configuration:**

1. Go to *Dashboard*.
2. In the *System Information* pane:
  - a. In *System Configuration*, click the *Restore System* icon.
  - b. In the dialog that appears, click *Choose File* and locate the backup file on your local computer.
  - c. Click *Upload*.FortiPortal reboots to complete the process.

## Backup and restore of scalable cluster

**To create a backup of the configuration:**

1. In the primary node of the cluster, go to *Dashboard*.
2. In the *System Information* pane:
  - a. In *System Configuration*, click the *Backup System* icon to download a backup file to your local computer.

**To restore a backed-up configuration:**

1. Deploy a new FortiPortal7.0.4 instance.
2. Restore the backup file onto the new instance and make it primary node in a new cluster.
3. Deploy two or more new FortiPortal7.0.4 instances.
4. Join these new instances to the primary node in the scalable cluster.



Backup from a scalable cluster and restore to another existing cluster directly is highly NOT recommended.

---

# Organizations

Use the *Organizations* tab to view information for each organization and add, edit, or delete organizations.

The table displays the following information for each organization:

- *Organization*: The name of the organization. Links to the organization portal.
- *Sites*: Number of sites.
- *Devices*: Number of devices.
- *Assigned Reports*: The number of assigned and available reports.
- *Device Configuration Status*: Summary count of devices by configuration status (*Synchronized*, *Modified*, and *Unknown*).
- *ADOM Versions*: The number of devices per ADOM version.

## Organization page actions

The following actions are available:

- *Create*: Add an organization. See [Create or edit an organization on page 31](#).
- *Edit*: Edit the selected organization. See [Create or edit an organization on page 31](#).
- *Delete*: Delete the selected organizations.
- *Search*: Search by text in organization name.
- *Sort*: Sort data in ascending or descending order by column.
- *Show N entries*: Limit the number of organizations displayed in the table to 20 or 50.

## Create or edit an organization

### To edit an organization:

1. In the *Organizations* table, select an organization.
2. Click *Edit*.

The organization edit window opens with the following tabs:

- [General on page 32](#)
- [Contact on page 34](#)
- [ADOMs on page 34](#)
- [Sites on page 35](#)
- [Users on page 37](#)
- [Authentication on page 40](#)
- [Reports on page 41](#)

### To create an organization:

1. Go to *Organizations* and click *Create*.  
The *Create New Organization* dialog opens.
2. Enter the following information:

Field	Description
Organization Name	Enter the organization business name, which must be unique within this FortiPortal.
Email	Email of the primary organization contact.
First Name	First name of the primary organization contact.
Last Name	Last name of the primary organization contact.
Create ADOM	Enable to create a new ADOM on the selected devices.
ADOM Name	If <i>Create ADOM</i> is enabled, enter a name for the new ADOM.
Version	If <i>Create ADOM</i> is enabled, select the ADOM version for the new ADOM.
FortiManager	If <i>Create ADOM</i> is enabled, select the FortiManager where the ADOM will be created.
FortiAnalyzer	If <i>Create ADOM</i> is enabled, select the FortiAnalyzer where the ADOM will be created.
Clone from ADOM	If <i>Create ADOM</i> is enabled, select the ADOM to clone to create the new ADOM.

3. Click *Save*.  
The organization edit window opens. See [To edit an organization: on page 31](#) for more information.  
Also see [Additional organization configuration on page 42](#).

---


## General

The *General* form contains basic information about the organization.



## To configure general settings for an organization:

1. In the *General* form, enter the following information:

Field	Required	Description
Organization Name	Y	Enter the organization business name, which must be unique within this FortiPortal.
Email	Y	Enter the first name of the primary organization contact.
First Name	Y	Enter the last name of the primary organization contact.
Last Name	Y	Enter the email address of the primary organization contact.
Locale	N	If you disable <i>Use MSSP Locale</i> , you can select a language for this organization. When an organization user logs in, pages will display in this language. For Administrative users, the system will continue to use the language set in <i>System &gt; Settings &gt; General</i> .
Domains	N	Enter a domain and then press <i>Enter</i> or click on the <i>Create &lt;name&gt;</i> link displayed as you type. The new domain appears in the field. Remove domains by clicking the X next to the domain. Use this field for the organization domain. To specify a domain for the administrator, see <a href="#">Authentication on page 51</a> . <div> When using remote authentication, a customer may have users defined in more than one domain.</div>
Use MSSP Locale	N	Enable or disable the MSSP locale (the language configured in <a href="#">General on page 49</a> ).
Require Pattern Validation	N	Enable or disable pattern validation.
Enable Trusted Hosts	N	Enable or disable trusted hosts for this organization. For additional information about trusted hosts, see <a href="#">Users on page 37</a> .
Attach Logo	N	Upload an image file. Select the file and click <i>Upload</i> . The maximum file size is 1 MB. The format can be jpg, gif, bmp, or png. The maximum file dimension is 144 pixels wide by 48 pixels tall.
Policy Installation Scheduler	N	Schedule automatic policy installation at a particular time (daily or weekly). All the pending policy updates will be installed at the configured schedule. If you select <i>None</i> , the installation scheduler is not invoked for this customer. If you select <i>Daily</i> , select the installation time. If you select <i>Weekly</i> , select the day and time for the policy installation.

2. Click *Save*.



Click *Reset* to reset entries and selections in the form.  
Click *Cancel* to exit without saving.

## Contact

Enter contact information for the organization.

### To configure contact information for an organization:

1. In the *Contact* form, enter the following information:

Field	Required	Description
Address 1	N	Enter the address of the organization.
Address 2	N	Use this field to continue the address.
City	N	Enter the city.
State	N	Enter the state.
Country	N	From the dropdown, select a country.
Zip	N	Enter ZIP code.
Phone	N	Enter the phone number.
Fax	N	Enter the fax number.

2. Click *Save*.



Click *Reset* to reset entries and selections in the form.  
Click *Cancel* to exit without saving.

## ADOMs

Select the devices enabled for this organization.

For more information, see [Devices on page 43](#).

### To configure ADOMs for an organization:

1. In the *ADOMs* form, select the ADOMs to enable for this organization.
2. Click the *Edit* (pen) icon to give the ADOM an alias to prevent customers from knowing the MSSP configuration.
3. Click *Save*.



Click *Reset* to reset entries and selections in the form.

Click *Cancel* to exit without saving.

---

## Sites

Use the *Sites* tab to view and configure organization site information.

The table displays the following information for each site:

- *Name*: The site name, unique within the organization's sites.
- *Email*: The primary contact email.
- *VDOMs*: The VDOMs assigned to this site.
- *APs*: FortiAP devices assigned to this site.
- *FortiSwitches*: FortiSwitches assigned to this site.

### To configure sites for an organization:





1. In the *Sites* tab:
  - a. Click *Create* to create a new site.
  - b. Select a site and click *Edit* to edit a site.



When editing a site, the fields are same as those that appear when creating a site.

---

2. In the form, enter or update the following information:

Field	Required	Description
Name	Y	Enter a name for the site, which must be unique across this organization's sites.
Contact Name	Y	Enter the name of the organization contact for this site.
Email	Y	Enter the email address of the organization contact for this site.
Phone	N	Enter the phone number of the organization contact for this site.
Sandbox	N	Enable or disable sandbox capability for all the selected devices.   An extra license is required for each device that you enable with sandbox.
Managed FortiGates	N	Select the FortiGate devices to associate with this site. Ensure that you add only the devices with the correct ADOM for this organization. Use the search box to filter the choices available.   Select a device and then select the pen icon to give the device an alias to prevent customers from knowing the configuration.
Managed FortiSwitches	N	Select the FortiSwitch devices to associate with this site. Use the search box to filter the choices available.   Select a device and then select the pen icon to give the device an alias.
Managed FortiAPs	N	Select the FortiAP devices to associate with this site. Use the search box to filter the choices available.   Select a device and then select the pen icon to give the device an alias.

3. Click Save.



To delete sites, select sites and click *Delete*.

---

## Users

View organization user information, add, edit, or delete organization users, and, if enabled, configure trusted hosts (See [Trusted Hosts on page 39](#)).

The table displays the following information about the local administrative users configured for this organization:

- *Name*: The user's username. Automatically set to the user's email address.
- *First Name*: The user's first name.
- *Last Name*: The user's last name.
- *Email*: The user's email address.
- *Status*: The user's status, either *Active* or *Inactive*.
- *Profile*: The permissions profile assigned to the user.
- *User Type*: The type of user, *Local* or *Remote*.
- *Two-Factor*: Displays whether two-factor authentication is disabled or enabled for this user.



These users are local. The described commands are available only when *Authentication Access* is set to *Local* in *System > Settings > Authentication*.

---

### To configure users for an organization:


1. In the *Users* tab:
  - a. Click *Create* to create a new user.
  - b. Select a user and click *Edit* to edit the user.



When editing a user, the fields are same as those that appear when creating a user.

---

2. Enter or update the following information:

Field	Required	Description
First Name	Y	Enter the first name of the user.
Last Name	Y	Enter the last name of the user.
Email	Y	Enter the email address of the user.
Password	Y	Enter a password for the user.
		 <p>The password must meet the requirements set by the password policy.</p>
Confirm Password	Y	Confirm the entered password.
Enable Password Policy	N	<p>Enable or disable a password policy for this user.</p> <p>If enabled:</p> <ul style="list-style-type: none"> <li>In <i>Must Contain</i>, select the following types of characters that the password must contain: <ul style="list-style-type: none"> <li><i>Uppercase Letters</i></li> <li><i>Lowercase Letters</i></li> <li><i>Numbers (0-9)</i></li> <li><i>Special Characters</i></li> </ul> </li> <li>In <i>Minimum Length</i>, enter the minimum number of characters a password must contain.</li> </ul> <p>This field is only available when creating a new user.</p>
Contact Information		
Address 1	N	Enter the address of the user.
Address 2	N	Use this field to continue the address.
City	N	Enter the city name.
State	N	Enter the state or province name.
Country	N	Enter the country name.
Zip	N	Enter the postal code.
Phone	N	Enter the phone number.
Fax	N	Enter the fax number.
Profile	Y	From the dropdown, select a profile. See <a href="#">Profiles on page 68</a> .
Sites	Y	From the dropdown, select one or more sites.
Active	N	Set the user status as active or inactive.
Enable Two-factor Authentication	N	Enable or disable two-factor authentication.

3. Click **Save**.



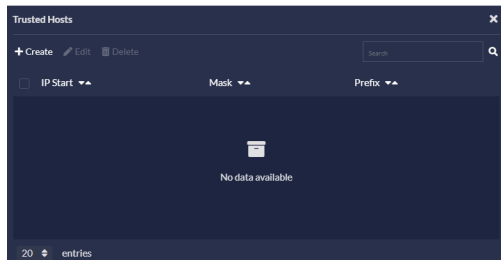
To delete users, select users and click *Delete*.

## Trusted Hosts

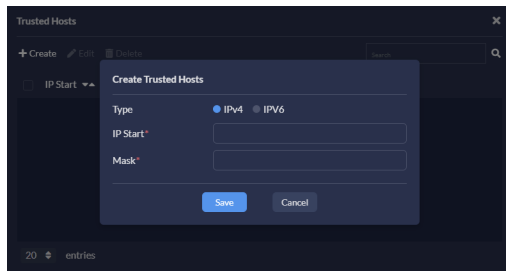
If you have enabled the *Trusted Host* option for this organization in [General on page 32](#), the system creates an allowlist of trusted hosts for each user.

### To create or edit trusted hosts:

1. In the *Users* tab, select a user and click *Trusted Hosts*.  
The *Trusted Hosts* window opens that displays a list of trusted hosts for the user.



2. Click *Create* or select a host and click *Edit*.



3. Enter the following information:

Field	Required	Description
Type	Y	Select <i>IPv4</i> or <i>IPv6</i> .
IP Start	Y	Enter the start address for the range covered by this entry.
Mask	Y	If <i>Type</i> is set to <i>IPv4</i> , define the range of IP addresses covered by this entry.
Prefix	Y	If <i>Type</i> is set to <i>IPv6</i> , define the range of IP addresses covered by this entry.

4. Click **Save**.

## User profiles

User profiles enable you to authorize each user to view and modify only the content that is required for that user.

---

Each profile defines the access rights of the user to specific portal components. Content access may be restricted, read-only, or read-write. Some components allow for custom permissions as well.

You can assign one or more profiles to a user. For example, a user with *Read/Write* permission on *Reports* and *Read* permission on the other components in the assigned profile will have read/write access to the *Reports* component and read-only access to the remaining components.

The system provides a set of default user profiles. Create new profiles or customize the default profiles in *System > Profiles*. See [Profiles on page 68](#) for more information.

## Default organization user profiles

Profile	Description
Customer Admin	Read-write access to all components for the organization
Customer Monitor	Read-only access to all components for the organization



In previous versions, profiles were referred to as "roles". In the GUI, "roles" is still occasionally used, and is synonymous with "profiles".

## Authentication

Use the *Authentication* tab to configure an organization to use separate SSO authentication servers for improved security.

See [Authentication on page 51](#) for more information.



## To configure authentication settings for an organization:

1. In the *Authentication* tab, enter the following information:

Field	Required	Description
Override Authentication Settings	N	Enable to override authentication settings set up in <a href="#">Authentication on page 51</a> . <b>Note:</b> This option is disabled by default.
SSO IDP Entity URL	Y	Enter the IDP Entity URL (ID) or URN for SAML provided by the IDP server.
IDP Sign On Service Endpoint URL	Y	Enter the endpoint URL for IDP (Post) provided by the IDP server.
IDP Sign On Service Redirect Endpoint URL	Y	Enter the endpoint URL for IDP (Redirect) provided by the IDP server.
IDP Logout Service Endpoint	Y	Enter the IDP logout URL provided by IDP.
SSO Certificate	Y	Enter the certificate provided by the IDP to decrypt the signed response.
View/Change SSO Roles		Click to map the SSO roles with the local profiles.

2. Click **Save**.



Click *Reset* to reset entries and selections in the form.  
Click *Cancel* to exit without saving.

## Reports

The administrator can create reports for the organization. Similarly, the organization can also create reports. The ability (for a specific user) to create reports or run reports is based on the profile assigned to that user. See [User profiles on page 39](#) for more information.

Use the *Reports* tab to view information about the reports that are available to this organization and assign reports to the organization.

Reports are only available if a FortiAnalyzer has been connected to a FortiManager ADOM assigned to this organization.

## Page actions

The *Reports* tab contains the following actions:

- *Assign*: Assign the selected report templates to this organization. Organization users can download a PDF file of the content.
- *Unassign*: Unassign the selected report templates from this organization.

- 
- **Search:** Search reports by name.
  - **Select:** Select one or more reports to assign to or unassign from a customer.
  - **Show x entries:** Limit number of entries that are displayed (20, 50, or All).
- 



- If you assign a report to a customer for a given ADOM, the other reports for that ADOM are unavailable to other customers.
  - Make sure that the device names (ADOM, FortiGate unit, or VDOM) match on the FortiAnalyzer unit and FortiManager unit.
  - All devices under the ADOM must be associated with the same customer for the customer to be able to view the FortiAnalyzer reports.
- 

## Additional organization configuration

For the *Bandwidth* widget to display in the organization device health dashboard, you must enable monitoring bandwidth on the FortiGate port by using the following CLI commands:

```
config system interface
  edit <name> # name of the FortiGate interface
    set monitor-bandwidth enable
  next
end
```

# Devices

Manage connected FortiManager and FortiAnalyzer devices.

See [FortiManager devices on page 44](#) and [FortiAnalyzer devices on page 46](#).

## FortiManager devices

View and manage connected FortiManager devices.

### Page actions

The following actions are available:

- *Create*: Add a FortiManager. See [Add a FortiManager on page 44](#).
- *Edit*: Edit the selected FortiManager. See [Edit a FortiManager on page 44](#).
- *Delete*: Delete the selected FortiManager.
- *Poll Now*: Poll the selected FortiManager.
- *Device Repo*: View a list of FortiGates, FortiSwitches, and FortiAPs managed by the selected FortiManager. See [Manage FortiGate, FortiSwitch, and FortiAP devices on page 45](#).
- *Search*: Search by FortiManager name and IP address.
- *Show x entries*: Limit the number of entries that are displayed (20 or 50).
- *Sort*: Sort columns in ascending or descending order.

### Add a FortiManager

Assuming that you have already created a dedicated admin user for FortiPortal on the FortiManager, do the following to add a FortiManager:

1. In *Devices > FortiManager*, click *Create*.
2. Input the fields, as described in [Edit a FortiManager on page 44](#).
3. Click *Add*.


When you add a FortiManager, FortiPortal polls the FortiManager immediately to obtain information about its managed devices. FortiPortal subsequently polls the FortiManager at the configured polling frequency.

### Edit a FortiManager

**To edit the selected FortiManager:**

1. Go to *Devices > FortiManager*.
2. Select a FortiManager device and click *Edit*.

3. In the form, enter or update the following information:

Field	Required	Description
Name	Y	Enter a unique name for the FortiManager.
Host	Y	Enter the IP address or domain name of the FortiManager.
Username	Y	Enter the username of a valid FortiManager administrator.
Password	Y	Enter the password for the FortiManager administrator.
Confirm Password	Y	Confirm the password.
Port	Y	Enter the port number used to connect with the FortiManager. The default is 443.
Polling Frequency		Select how frequently FortiPortal will poll the FortiManager to update the device information. Defaults to <i>No Polling</i> .
<div><p>If you set the frequency to <i>No Polling</i>, FortiPortal will never poll the FortiManager. Valid values include <i>Daily</i>, <i>Weekly</i>, or <i>Monthly</i>. You can poll the FortiManager at any time by clicking <i>Poll Now</i> in the list of connected FortiManager devices.</p></div>		

4. Click **Save**.

## Manage FortiGate, FortiSwitch, and FortiAP devices

Select a *FortiManager* and click *Device Repo* to view a list of the FortiGate, FortiSwitch, and FortiAP devices managed by this FortiManager.

The system displays an additional search box, for searching within the list of devices.

For each FortiManager device, the system displays the following:

- **FortiGates:**
  - *Device:* The name of the managed FortiGate device.
  - *Status:* The synchronization status of the FortiGate device.
  - *Organization:* The organization this device has been assigned to.
- **FortiSwitches:**
  - *Switch:* The name of the managed FortiSwitch device.
  - *From Devices:* The parent FortiGate device.
- **FortiAPs:**
  - *Access Point:* The name of the managed FortiAP device.
  - *From Devices:* The parent FortiGate device.



FortiPortal can add FortiGate devices configured in the Fortinet Security Fabric. FortiGate devices added from the Security Fabric are identified by the \* sign next to the Security Fabric root, and the name of the Security Fabric it belongs to is also displayed.

## FortiAnalyzer devices

View and manage connected FortiAnalyzer devices.

When you add a FortiAnalyzer device to FortiPortal, you make the reports on that FortiAnalyzer available to organizations. See [Reports on page 41](#) for more information.

The table displays the FortiAnalyzer name, IP address, status, and version for each FortiAnalyzer.

### Prerequisites

Before you add a FortiAnalyzer device to FortiPortal, configure the following FortiAnalyzer settings:

1. 1. In the FortiAnalyzer CLI, set the permission level for the user to login via remote procedure call (RPC):

```
config system admin user
  edit <the admin user name assigned to FortiPortal>
    set rpc-permit read-write
  end
```
2. 2. On the FortiAnalyzer, set port1 (or whichever port is connected to the FortiPortal) to allow HTTPS access:
  - a. In the GUI, go to *System Settings > Network*.
  - b. Select the appropriate port and click *Edit*.
  - c. In the *Administrative Access* field, enable *HTTPS* and click *OK* to save.

Alternatively, in the CLI, run the following command to enable administrative access through HTTPS:

```
config system interface
  edit port1
    set allowaccess https
  end
```

### Page actions

The following actions are available:

- *Create*: Add a FortiAnalyzer device. See [Add a FortiAnalyzer on page 47](#).
- *Edit*: Edit the selected FortiAnalyzer. See [Edit a FortiAnalyzer on page 47](#).
- *Delete*: Delete selected FortiAnalyzer devices.
- *Poll Now*: Poll the selected FortiAnalyzer to obtain the most recent data.
- *Reports*: Display a list of FortiAnalyzer reports for the selected FortiAnalyzer device. See [View FortiAnalyzer reports on page 47](#).
- *Search*: Search by FortiAnalyzer name.
- *Show x entries*: Limit the number of entries that are displayed (20 or 50).
- *Sort*: Sort columns in ascending or descending order.

## Add a FortiAnalyzer

Assuming that you have already created a dedicated admin user for FortiPortal on the FortiAnalyzer and followed the step in [Prerequisites on page 46](#), do the following to add a FortiAnalyzer:


1. In *Devices > FortiAnalyzer*, click *Create*.
2. Input the fields, as described in [Edit a FortiAnalyzer on page 47](#).
3. Click *Add*.

When you add a FortiAnalyzer, FortiPortal polls the FortiAnalyzer immediately to obtain information about reports. FortiPortal subsequently polls the FortiManager at the configured polling frequency.

## Edit a FortiAnalyzer

To edit the FortiAnalyzer:

1. Go to *Devices > FortiAnalyzer*.
2. Select a FortiAnalyzer device and click *Edit*.
3. In the form, enter or update the following information:

Field	Required	Description
Name	Y	Enter a name for the FortiAnalyzer. The combination of FortiAnalyzer name and VDOM must be unique within this FortiPortal.
Host	Y	Enter the IP address or domain name of the FortiAnalyzer.
Username	Y	Enter the username for the FortiAnalyzer user assigned to this FortiPortal.
Password	Y	Enter the password for the FortiAnalyzer user.
Confirm Password	Y	Confirm the password.
Port	Y	Enter the port number used to connect to the FortiAnalyzer. The default port is 443.
polling		Displays how often FortiPortal will poll FortiAnalyzer to update the report information.
<div> The default value is daily. The polling frequency is not configurable.</div>		

5. Click *Save*.

## View FortiAnalyzer reports

Select a FortiAnalyzer and click *Reports* to view the available reports.

The pane displays reports listed by ADOM.

# System

Manage system settings and other configuration:

- [Settings on page 49](#)
- [Profiles on page 68](#)
- [Admins on page 69](#)
- [Theme on page 72](#)
- [Additional Resources on page 99](#)



# Settings

Go to *System > Settings* to configure the system settings.

*Settings* contains the following tabs:

- [General on page 49](#)
- [Authentication on page 51](#)
- [Blocked hosts on page 64](#)
- [Scalable cluster on page 65](#)
- [Email on page 67](#)
- [Others on page 67](#)




## General

Use the *General* tab to configure the general administrative settings.

### To configure general settings:

1. Go to *System > Settings*.  
The *General* tab opens.

2. In the *General* tab, enter the following information:

Field	Required	Description
Session Timeout	Y	Set the timeout for user sessions on both the administrative and organizational web interfaces, in minutes (15 - 3240, default = 30).
Language	Y	Select the desired language (default = English).
 If you change the language, save the settings and log out. The change takes effect upon subsequent logins.		
Time Zone	Y	Select the appropriate time zone to use.
Enable Blocked Host	N	Enable or disable blocked hosts. When enabled, the system provides a blocklist, for blocking rogue log-in attempts. See <a href="#">Blocked hosts on page 64</a> .
<i>Certificate Information</i>		
Certificate	N	Upload a new certificate for FortiPortal.
Private Key	N	Upload a new private key for FortiPortal.
 The <i>Private Key</i> is in PKCS#8 format.		
<i>Upload License</i>		
License	N	See <a href="#">Upload a license on page 50</a> .
 The system automatically restarts the FortiPortal VM to apply the license.		
<i>System</i>		
System Logs	N	Click the <i>Export</i> button to download system logs.

3. Click **Save**.

## Upload a license

You only need a single license file for FortiPortal. After you upload the FortiPortal license, the license details are shown in the *Dashboard*, including the number of devices allowed, the number of devices used, the number of Fortinet Access Points (FAPs) allowed, the number of FAPs used, and the FortiManager and FortiAnalyzer status.

The number of devices used is the number of devices (VDOMs) that a site administrator assigns to a site. Other devices that FortiPortal has access to from FortiManager do not count towards this number until they are assigned to a site.

If the administrative user creates a site, assigns a device to it, and the administrative user has selected the *Sandbox* checkbox so that FortiPortal will process logs from the customer's FortiSandbox devices, those devices are counted as part of the number of devices used. Refer to the [Dashboard](#).

When the administrative user removes a device from the site, the number of devices used decreases by one, and the number of devices allowed increases by one. Refer to the [Dashboard](#).

The *Expiry Date* in the *Dashboard* shows when the FortiPortal license expires.






FortiPortal periodically checks for license status update with FortiGuard. When the license is renewed, the interface is available again.




## Authentication

In the *Authentication* tab, you can configure the user authentication (and related) settings.


### To configure authentication settings:

1. Go to *System > Settings > Authentication*.  
The *Authentication* tab opens.
2. In the *Authentication* tab, enter the following information:

Field	Required	Description
Authentication Access	N	<p>Set to <i>Local</i> or <i>Remote</i>. After changing this setting, you must log in again.</p> <hr/> <p> By default, <i>Authentication Access</i> is set as <i>Local</i>.</p> <hr/> <p> If FortiPortal is operating as a scalable cluster, the system will restart when you change the authentication configuration from local to remote or from remote to local.</p> <hr/> <p>See <a href="#">Authentication Access</a> on page 55.</p>
Enable Two-factor Authentication	N	<p>Enable or disable two-factor authentication (2FA) for local or remote users. FortiPortal only supports using the FortiToken Mobile application as the 2FA method. SMS and email are not supported.</p> <hr/> <p> For 2FA, a FortiToken license needs to be applied and registered in the same account where the FortiPortal license is registered.</p> <hr/>

Field	Required	Description
		 <p>Email information is mandatory for 2FA users.</p>
		 <p>If the user name is the email and no <i>Tenant Identification Attribute</i> is set, the domain part of the email can be used for tenant identification.</p>
		See <a href="#">Two-factor authentication in FortiPortal example on page 63</a> .
Remote Server	Y	<p>Select <i>FortiAuthenticator</i>, <i>Radius</i>, or <i>SSO</i> as the remote server type.</p> <p><b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i>.</p>
Remote Server Port	Y	<p>Enter the port for the authentication server (default is 443)</p> <p><b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>FortiAuthenticator</i> or <i>Radius</i>.</p>
Remote Server IP Address	Y	<p>Enter the IP address of the authentication server.</p> <p><b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>FortiAuthenticator</i> or <i>Radius</i>.</p>
Remote Server Key	Y	<p>Enter the secret key for REST API requests.</p> <p><b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>FortiAuthenticator</i> or <i>Radius</i>.</p>
Self Service Portal	N	<p>Enter the URL of the SSO provider's user self service portal where users can manage their SSO settings, if applicable.</p> <p><b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i>.</p>
Support Idp-Initiated SSO		<p>Enable or disable IDP-Initiated SSO. This should be enabled when <i>IDP-initiated</i> SSO is enabled on your SAML server.</p> <p><b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is set as <i>SSO</i>.</p>
Domains	N	<p>Enter a domain and then press <i>Enter</i> or click on the <i>Create &lt;name&gt;</i> link displayed as you type. The new domain appears in the field.</p> <p>Remove domains by clicking the X next to the domain.</p> <p>Use this field to specify the domain, URL, or URN for the site administrator.</p> <p>To specify the domain for an organization, see <a href="#">General on page 32</a>.</p>
		 <p>The site administrator may allow administrative users to be defined in more than one authentication domain.</p>

Field	Required	Description
		<b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> .
Remote Server User	Y	Administrator user name for the authentication server. This user must have sufficient permission to initiate REST API requests. <b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>FortiAuthenticator</i> .
Authentication Protocol	Y	Required. Select <i>PAP</i> , <i>CHAP</i> , or <i>MSCHAPv2</i> authentication protocol. <b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>Radius</i> .
View/Change Radius Roles	Y	Click to map the RADIUS roles with local roles. See <a href="#">Radius Roles on page 55</a> . <b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>Radius</i> .
SSO IDP Entity URL	Y	Enter the IDP Entity URL (ID) or URN for SAML provided by IDP server. <b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>SSO</i> .
IDP Sign On Service Endpoint URL	Y	Enter the endpoint URL for IDP (Post) provided by IDP server. <b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>SSO</i> .
IDP Sign On Service Redirect Endpoint URL	Y	Enter the endpoint URL for IDP (Redirect) provided by IDP server. <b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>SSO</i> .
SSO Application ID	Y	Enter the SSO application ID provided by the IDP. <b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>SSO</i> .
SSO Audience URL	Y	Enter the URL used for audience within the assertion (format: <code>https://&lt;FPC_PORTAL&gt; /fpc/saml/SSO</code> ). <b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>SSO</i> .
Role Attribute	Y	Enter the attribute parameter name that maps to the corresponding profile in FortiPortal. <b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>SSO</i> .
Tenant Identification Attribute	N	Enter or select a value that FortiPortal uses under SSO or RADIUS to map a user to a specific organization. See <a href="#">Tenant identification and domains on page 62</a> for more information about how this works with SSO. This feature works similarly to the <i>Tenant Identification Attribute</i> in RADIUS, except that in SSO, FortiPortal allows you to enter the name of the attribute in this form.

Field	Required	Description
		<p>If you configure "My Customer Id" as the attribute value, FortiPortal expects the following in the authentication response from the SSO server:</p> <p>For a RADIUS server, the Tenant Identification Attribute value is a Fortinet Vendor Attribute value. The server will send "Fortinet" in the authentication response.</p> <hr/> <div>  <p>FortiPortal treats the attribute values from either RADIUS or SSO server equally.</p> </div> <hr/> <p><b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>SSO</i> or <i>Radius</i>.</p>
SSO Error URL	N	<p>If your SSO IDP provides an error URL where users can find additional help if an SSO error occurs, enter the URL. Not all IDPs provide an error URL. FortiPortal does not send any additional information to this URL.</p> <p><b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>SSO</i>.</p>
IDP Logout Service Endpoint	Y	<p>Enter the IDP logout URL provided by IDP.</p> <p><b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>SSO</i>.</p>
SSO Certificate	Y	<p>Enter the certificate provided by the IDP used to decrypt the signed response.</p> <p><b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is <i>SSO</i>.</p>
Site Attribute	N	<p>Enter the attribute parameter name that specifies which sites the customer user can access.</p> <p>When the <i>Remote Server</i> is <i>SSO</i>, enter the site attribute.</p> <p>For example, an attribute name of "site" might have the values "site1" and "site2". A customer user assigned to "site" would be able to access "site1" and "site2".</p> <pre>&lt;saml:Attribute   Name="site"   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"&gt;   &lt;saml:AttributeValue     xsi:type="xs:string"&gt;site1&lt;/saml:AttributeValue&gt;   &lt;saml:AttributeValue     xsi:type="xs:string"&gt;site2&lt;/saml:AttributeValue&gt; &lt;/saml:Attribute&gt;</pre> <p>When the <i>Remote Server</i> is <i>FortiAuthenticator</i> or <i>Radius</i>, select a site attribute from the dropdown. By default, <i>Fortinet-Fpc-Tenant-user-sites</i> is available.</p> <p>You can select a different value if you define an attribute for a site on the FortiAuthenticator or the RADIUS server.</p>

Field	Required	Description
		<b>Note:</b> If the <i>Site Attribute</i> is empty, the customer user is assigned all the sites owned by the organization. <b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> .
Email Attribute	N	Enter the user-defined email attribute name. <b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is SSO.
View/Change SSO Roles	N	Click to map the SSO roles with the local roles. See <a href="#">SSO Roles on page 56</a> . <b>Note:</b> This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> and <i>Remote Server</i> is SSO.

3. Click Save.

## Authentication Access

If the authentication access is local, the administrator and customer user log-in credentials are checked in the local user databases. With the local option, you must add an SP user entry for each administrative user, and a user for each organization user.

If the authentication access is remote, the administrator and customer user log-in credentials are checked in the remote RADIUS server, FortiAuthenticator user database, or SSO IDP database. Local customer users *cannot* be used when remote authentication is selected.

See [Remote authentication: FortiAuthenticator on page 57](#), [Remote authentication: RADIUS on page 58](#), and [Remote authentication: SSO on page 59](#).

## Radius Roles

Click *View Radius Roles* in the *Authentication* tab to configure the mapping between FortiPortal profiles and RADIUS roles. For each RADIUS role mapping, the window displays the *Role Name*, *Role Type* (*Service Provider* or *Customer*) and a list of *FPC* (FortiPortal) roles that map to the RADIUS role.



In previous versions, profiles were referred to as "roles". In the GUI, "roles" is still occasionally used, and is synonymous with "profiles".

The *Radius Roles* window contains the following options:

- *Create*: Create a RADIUS role mapping.
- *Edit*: Edit the selected RADIUS role mapping.
- *Delete*: Delete one or more selected RADIUS role mappings.
- *Search*: Search for RADIUS role mappings by name.
- *Show x entries*: Limit the number of entries that are displayed at once (20 or 50).
- *Sort*: Sort columns in ascending or descending order.

### To create a RADIUS role mapping:

1. Go to *System > Settings > Authentication*.
2. Set *Authentication Access* to *Remote*.
3. In the *Remote Server* dropdown, select *Radius*.
4. Click *View/Change Radius Roles*.  
The *Radius Roles* window opens.
5. In the *Radius Roles* window, click *Create*.
6. In the *Create Role* window, enter the following information:

Field	Required	Description
Role Name	Y	The RADIUS role name. The name must match a role name on the RADIUS server.
Role Type	Y	<i>Service Provider</i> or <i>Customer</i> .
FPC Roles	Y	Select the FortiPortal profile to associate with this RADIUS role.

7. Click *Save*.

## SSO Roles

Click *View SSO Roles* in the *Authentication* tab to configure the mapping between FortiPortal profiles and SSO roles. For each SSO role mapping, the window displays *Role Name*, *Role Type* (*Service Provider* or *Customer*) and a list of (FortiPortal) profiles that map to the SSO role.

The *SSO Roles* window contains the following actions:

- *Create*: Create an SSO role mapping.
- *Edit*: Edit the selected SSO role mapping.
- *Delete*: Delete one or more selected SSO role mappings.
- *Search*: Search for SSO role mappings by name.
- *Show x entries*: Limit the number of entries that are displayed at once (20 or 50).
- *Sort*: Sort columns in ascending or descending order.

### To create an SSO role mapping:

1. Go to *System > Settings > Authentication*.
2. Set *Authentication Access* to *Remote*.
3. In the *Remote Server* dropdown, select *SSO*.
4. click *View SSO Roles*.  
The *SSO Roles* window opens.
5. In the *SSO Roles* window, click *Create*.



6. In the *Create Role* window, enter the following information:

7.

Field	Required	Description
Role Name	Y	The SSO role name. The name must match a role name on the SSO server.
Role Type	Y	<i>Service Provider</i> or <i>Customer</i> .
FPC Roles	Y	Select the FortiPortal profile to associate with this SSO role.

8. Click **Save**.

## Remote authentication: FortiAuthenticator

You need to set up both FortiAuthenticator and FortiPortal before you can use FortiAuthenticator for remote authentication.

### Configuring FortiAuthenticator

Before using FortiAuthenticator for remote authentication, go to *System > Messaging > SMTP Servers* in FortiAuthenticator and make certain that the SMTP server is working. If the SMTP server is not working, configure a new SMTP server and then select it in *System > Messaging > Email Services*.

#### To configure FortiAuthenticator:

1. Configure an administrator user or use the default `admin` user with a valid email address.
2. Enable *Web service access*.

Edit Local User

Username:admin

☐ Disabled

☒ Password authentication

Change Password

☐ One-Time Password (OTP) authentication

☐ FIDO authentication

☐ Allow RADIUS authentication

☐ Force password change on next logon

☐ Sync in HA Load Balancing mode

User Role

Role:AdministratorSponsorUser

☒ Full permission

☐ Web service access

☐ Restrict admin login from trusted management subnets only



When *Force password change on next logon* is enabled, FortiPortal will require the user to change their password after their first login.

3. Save the REST API key that you will receive by email.

## Configuring FortiPortal

When you configure *Authentication Access* as *Remote* in *System > Settings > Authentication*, the remote server is set to *FortiAuthenticator* by default, and the system displays additional settings to configure.



If you change the authentication configuration from local to remote or from remote to local, you must restart FortiPortal.

### To configure FortiPortal:

1. Go to *System > Settings > Authentication*.
2. In *Authentication Access*, select *Remote*.
3. In *Remote Server*, select *FortiAuthenticator*.
4. In *Remote Server Port*, enter 443.
5. In *Remote Server IP Address*, enter the IP address of the authentication server.
6. In *Remote Server Key*, paste the FortiAuthenticator REST API key you received by email.
7. In *Domains*, add the domain for the administrator user. For example, if the administrator user is `abc@test.com`, add `test.com` in *Domains*.
8. In *Remote Server User* field, enter the name of the FortiAuthenticator administrator user.
9. Click *Save*.

## Remote authentication: RADIUS

### Configure the following in the RADIUS server:

1. Add the following vendor-specific attributes to the Fortinet dictionary file:

Fortinet-Fpc-User-Role

Fortinet-Fpc-Tenant-Identification

For example, if you are using FreeRADIUS:

```
#  
#  
#
```

```
VENDOR      Fortinet      12356
```

```
BEGIN-VENDOR Fortinet
```

```
ATTRIBUTE    Fortinet-Group-Name      1  string
```

```
ATTRIBUTE    Fortinet-Client-IP-Address  2  ipaddr
```

ATTRIBUTE	Fortinet-Vdom-Name	3	string
ATTRIBUTE	Fortinet-Client-IPv6-Address	4	octets
ATTRIBUTE	Fortinet-Interface-Name	5	string
ATTRIBUTE	Fortinet-Access-Profile	6	string
ATTRIBUTE	Fortinet-Fpc-User-Role	40	string ###add this
ATTRIBUTE	Fortinet-Fpc-Tenant-Identification	41	string ###add this

```
#
# Integer Translations
#
```

END-VENDOR Fortinet

2. To configure FortiPortal roles in the RADIUS server, use the following vendor-specific attribute. You can specify multiple roles by using comma-separated values:

VENDORATTR 12356 Fortinet-Fpc-User-Role 40 string



A user will not be able to login to FortiPortal if the roles are not configured on the RADIUS server.

3. To configure which sites will use RADIUS authentication, use the following vendor-specific attribute. You can specify multiple sites by using comma-separated values. If no sites are specified, users have access to all sites.  
VENDORATTR 12356 Fortinet-Fpc-Tenant-User-Sites 42 string
4. Specify the customer identification, which is used to map a particular user to a customer profile. The RADIUS server will send one of the domain names specified in the *Domains* field of the customer settings, in the value of the new VSA.  
VENDORATTR Fortinet-Fpc-Tenant-Identification 41 string

## Remote authentication: SSO

For single sign-on (SSO), FortiPortal supports both service provider (SP) initiated and identity provider (IDP) initiated SAML authentication.

## To configure your SAML IDP server:

1. Set custom attributes to identify what fields in the SAML assertion will hold the needed values:

FortiPortal field	Example attribute name	Example attribute value	Description
Role Attribute	FPC_Role	user.jobtitle	Used to map the IDP server roles to FortiPortal profiles. Required.
Site Attribute	FPC_Site	user.officelocation	Used to restrict an account to a specific site or location. Optional.
Tenant Identification Attribute	FPC_Tenant	user.companyname	Defines the field in the SAML assertion that holds the user's domain name, which is then used to map to an organization or administration domain. Optional. See <a href="#">Tenant identification and domains on page 62</a> for more information.
Email Attribute	FPC_Email	user.mail	Defines the field in the SAML assertion that holds the user's email address, which is then used to map to a organization or administration domain if <i>Tenant Identification Attribute</i> is not set and the username is not in email format. Optional.

2. Configure other options as needed.
3. Consult the documentation for your IDP provider for more information.



FortiPortal requires that all SAML responses and assertions are signed.

In Azure AD, edit *Token signing certificate* and set *Signing Option* to *Sign SAML response and assertion*.

## To configure FortiPortal:

1. In the *Authentication Access* field, select *Remote*.
2. In the *Remote Server* field, select *SSO*.
3. Enter the *SSO IDP Entity URL*. The name of this field on your provider may vary. For example, in Azure AD, this value is found in the *Identifier* field.
4. Enter the *IDP Sign On Service Endpoint URL*. For example, in Azure AD, this value is found in the *Login URL* field.
5. Enter the *IDP Sign on Service Redirect Endpoint URL*. This value is usually the same as the *IDP Sign On Service Endpoint URL*.
6. Enter the *SSO Application ID* as set in your IDP configuration.
7. Enter the *SSO Audience URL* value from the sign on URL as set in your IDP configuration. This is usually `https://<portal>/fpc/saml/SSO`.
8. Enter the *Role Attribute* as set in your IDP configuration.
9. Enter the *Tenant Identification Attribute* as set in your IDP configuration. If set, this value is used to match the user with an organization. For more information, see [Tenant identification and domains on page 62](#).

10. Enter the *IDP Logout Service Endpoint*. In Azure AD, this value is found in the *Logout URL* field.
11. Enter the *SSO Certificate* from your IDP server. Strip out any carriage returns and the `BEGIN CERTIFICATE` and `END CERTIFICATE` sections.
12. Enter the *Site Attribute* as set in your IDP configuration.
13. Optionally:
  - a. Enter the *Email Attribute*.
  - b. Enter the *Self Service Portal*, if provided by your IDP provider.
  - c. Enable or disable *Support Idp Initiated SSO*. This should be enabled when *IDP-initiated SSO* is enabled on your SAML server.
14. Select the domains to be used for administration access. For more information about how domain matching works, see [Tenant identification and domains on page 62](#).
15. Click **Save**.



To use two-factor authentication, select the *Remote* authentication access and SSO and configure two-factor authentication on the SAML IDP server.



When troubleshooting single sign-on, use the following URL for the `spuser` account to authenticate locally, bypassing remote authentication:

`https://<Portal>/fpc/app/admin`

---

## Mapping IDP server roles user to FortiPortal profiles

The site administrator can create profiles on FortiPortal to restrict access to UI pages or actions. These profiles can be mapped to existing roles on the IDP server.

When users are authenticated, the user role noted in the SAML assertion from the IDP server is mapped to a profile in FortiPortal and the appropriate permissions are provided to the user.

Site administrators do not need to change or add permissions on the IDP server exclusively for FortiPortal.

FortiPortal profiles can be mapped to IDP server roles prior to setting up an SSO provider. The IDP role name will be matched to any IDP servers that are added.

### To map IDP roles to FortiPortal profiles:

1. Go to *System > Settings > Authentication*.
2. In *Authentication Access*, select *Remote*.
3. In the *Remote Server* dropdown, select *SSO*.
4. Select *View SSO Roles*.  
The *SSO Roles* window opens.
5. Select *Create*.
6. In the *Create Role* window, enter the *Role Name* (this name must be an SSO role). Select the *Role Type*.
7. Select a FortiPortal profile to associate with this SSO role. See [Profiles on page 68](#) for more information about creating profiles.
8. Click **Save**.

---

## Tenant identification and domains

During authentication, FortiPortal identifies whether the user is an administrator or an organization and loads the correct user interface. FortiPortal uses the domain name to identify which interface should be loaded.

If the *Tenant Identification Attribute* is configured and is provided in the SAML assertion, the value in the *Tenant Identification Attribute* is used to match a domain name provided in the SSO settings or in an organization's [General on page 32](#) settings. If the domain in the SAML assertion does not match any of these domains, an error message is displayed.

If the *Tenant Identification Attribute* is not configured or is not provided in the SAML assertion, the domain name is taken from the username attribute, which must be formatted as an email address.

If the username is not provided as an email address, then the SSO *Email Attribute* can be used to configure which SAML assertion field holds the user's email address. This field will be used to match the domain name.

If the username is not in email format and neither *Tenant Identification Attribute* nor *Email Attribute* are set, then the domain cannot be matched, login fails, and FortiPortal displays an error.

### How can the tenant ID attribute help maintain the appropriate privileged access to the system?

The *Tenant Identification Attribute* value is taken from the IDP response and that value is mapped with the domain name field in FortiPortal. For example, if the *Tenant Identification Attribute* is `map_id`, FortiPortal gets the value for the `map_id` attribute from the SAML response and maps that value with a domain name listed in an organization's [General on page 32](#) settings or the *System > Settings > Authentication* settings. If the value matches with an organization domain name, the user is granted access to that organization. If the value matches with a domain name in the SSO settings, the administrative interface loads.

### How can I add a domain name to an organization?

A unique domain name identifies the organization. You can add domain names to an organization in that organization's [General on page 32](#) settings.

In the [General on page 32](#) tab in [Create or edit an organization on page 31](#), enter the domain name in the *Domains* field and press *Enter* to add the name to the domain list.

You can add more than one domain to an organization.

See [General on page 32](#) for more information.

### How can I add a domain name for a service provider?

After you select `Remote` as the *Authentication Access* in the [Authentication on page 51](#) tab, you will see the *Domains* field.

See [Authentication on page 51](#) for more information.

## Two-factor authentication in FortiPortal - example

### To enable 2FA for a user:

1. Go to *System > Settings > Authentication* and enable two-factor authentication.



Two-factor authentication can be enabled for a local or a remote user.

---



Email information is mandatory for 2FA users.

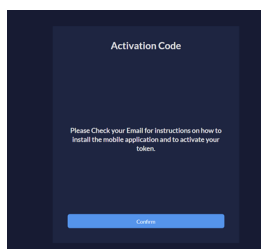
---



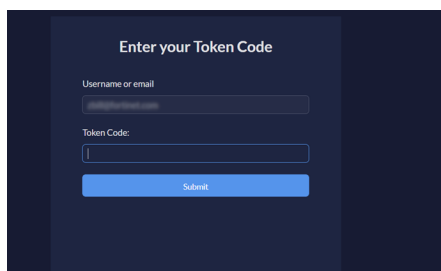
If the username is the email and no *Tenant Identification Attribute* is set, the domain part of the email will be used for tenant identification.

---

2. Ensure that two-factor authentication is enabled when creating or editing an admin in *System > Admins*. For organizational users, you can enable two-factor authentication when creating a new user or editing an existing user for the organization.
3. Log in to FortiPortal as the user with two-factor authentication enabled. The *Activation Code* window appears and an activation email is sent to the user.



4. Click *Confirm*.
5. In the *Enter your Token Code* window, enter token code from the email and click *Submit* to log in to FortiPortal. Alternatively, scan the QR code image in the activation email with the FortiToken mobile application to activate it. Click *Submit* to log in to FortiPortal.



### SSO 2FA users

If the email cannot be used as the username:

- In the SAML server, SAML user-defined email attribute can be used to set the user email.
- In FortiPortal, user-defined email attribute name needs to be configured in *Email Attribute*. See [Authentication on page 51](#).

## RADIUS 2FA users

Fortinet-Access-Profile attribute can be used to set email if the email cannot be used as the username in the RADIUS server.

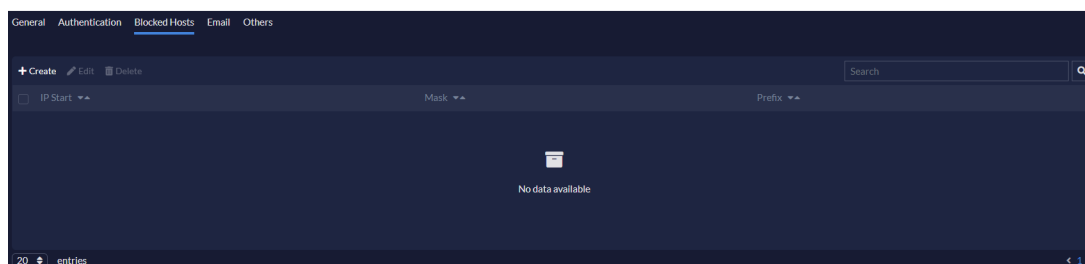
## FortiAuthenticator users

In FortiAuthenticator, if email cannot be used as the username, you can set the email in the *User Information* pane when creating or editing a user in *Authentication > User Management > Local Users* or *Authentication > User Management > Remote Users*.

## Blocked hosts

If you enable blocked hosts as a global setting in [General on page 49](#), the system enforces a configurable blocklist for all admin and users.

The *Blocked Hosts* tab displays the blocklist, which is a list of IP addresses that are blocked.



The blocklist is a system level feature, and it applies to SSO and SAML users.

### To create blocked hosts:

1. Go to *System > Settings > Blocked Hosts*.



Select a blocked host and then click *Edit* to edit the blocked host.

When editing a blocked host, the fields are the same as those that appear when creating a blocked host.

2. In the *Blocked Hosts* tab, click *Create*.  
The *Create Blocked Hosts* window opens.



3. Enter the following information:

4.

Field	Required	Description
Type	Y	Select <i>IPv4</i> or <i>IPv6</i> .
IP Start	Y	Enter the start address for the range covered by this entry.
Mask	Y	If <i>Type</i> is set to <i>IPv4</i> , define the range of IP addresses covered by this entry.
Prefix	Y	If <i>Type</i> is set to <i>IPv6</i> , define the range of IP addresses covered by this entry.

5. Click **Save**.



To delete one or more blocked hosts, select the hosts and click *Delete*.

## Scalable cluster



Use this feature only if you are certain that a scalable cluster is required. Once a cluster has been set up it cannot be deleted.

When a FortiPortal instance is used to set up a new cluster or a FortiPortal instance joins an existing cluster, the FortiPortal instance can no longer be a standalone FortiPortal.

**All existing data from the secondary instances is deleted.**

In the *Scalable Cluster* tab, you can configure a FortiPortal cluster.

A cluster consists of a primary unit and two or more standby secondary units. A minimum of three units is required to set up a cluster. If the primary unit becomes unavailable, one of the standby secondaries will become the new primary.

In a FortiPortal cluster, the license limit is the combined license limit of all the FortiPortal instances in a cluster.

Scalable clusters have the following benefits:

- All the instances are active in a cluster and can serve requests in parallel.
- Data can be synchronized across all cluster members in real-time. When options are updated in a primary unit, the changes are applied to all the secondary units in the cluster.
- The cluster can be scaled horizontally by adding new FortiPortal instances.
- The built-in load balancer is available to distribute loads across all instances in a cluster.

The following roles are available:

- *Primary*: The FortiPortal is the primary in a high-availability cluster.
- *Secondary*: The FortiPortal is a secondary in a high-availability cluster.
- *Standalone*: The FortiPortal is independent of a high-availability cluster. This is the default setting. Use it if you intend to keep the FortiPortal instance independent of a cluster.

---

## To set up a FortiPortal cluster:

1. Prepare your system for the cluster.
  - a. If the *Certificate Information* and *Upload License* related options in *System > Settings* need to be updated, they should be updated in the primary unit before setting up the cluster.
  - b. If the firmware, restore, and backup options in the *Dashboard* need to be updated, they should be updated in the primary unit before setting up a cluster.



Make sure all cluster nodes have the same system configuration (number of CPUs, size of memory, etc.), otherwise the cluster may fail to form.

---



The following ports must be open between the FortiPortal instances:

- 2379
  - 2380
  - 6443
  - 7472
  - 7946
  - 10250
- 

2. Set up the primary instance.
  - a. Log in to the primary FortiPortal instance.
  - b. Go to *System > Settings > Scalable Cluster*.
  - c. In the *Operational Mode* field, select *Primary*.
  - d. In the *Cluster Password* field, set a password for the cluster. This password cannot be retrieved or changed once it is set.
  - e. Click *Create Cluster*.
3. Set up two or more secondary units.
  - a. Log in to another FortiPortal instance.
  - b. Go to *System > Settings > Scalable Cluster*.
  - c. In the *Operational Mode* field, select *Secondary*.
  - d. In the *Cluster Password* field, enter the cluster password you set on the primary instance.
  - e. In the *Primary FPC IP* field, enter the IP address of the primary instance.
  - f. In the *Serial Number* field, enter the serial number of the primary instance.
  - g. Click *Join*.
  - h. Repeat step 3 to add additional secondary instances to the cluster.
4. Configure the load balancer (optional).
  - a. Log in to one of the FortiPortal instances in the cluster.
  - b. Go to *System > Settings > Scalable Cluster*.
  - c. In the *Load Balancer IP Range* field, enter an IP address in the same subnet as the cluster instances. This IP should be one that is not assigned to any devices.
  - d. Click *Update*.

The load balancer IP configuration is automatically applied across all instances of the cluster.



After upgrading a FortiPortal instance, you must set the load balancer IP address again.

## Email

Use the *Email* tab to configure the email related settings.

### To configure email related settings:

1. Go to *System > Settings > Email*.
2. Enter the following information:

Field	Required	Description
SMTP Server	Y	Enter the URL of the SMTP server FortiPortal sends emails through.
Port	Y	Enter the email server port. The default value is 25.
Email From	Y	Enter the sender email address. Emails will originate from this address.
Enable Authentication	N	Enable or disable authentication. If you enable authentication, enter a user name and password. You can use special characters in the user name.
Enable Validate Mail Server Certificate	N	Enable or disable validating the mail server certificate. This option is enabled by default.

3. Click *Save*.

## Others

FortiPortal can send audit logs to a remote syslog server.

Use the *Others* tab to configure the remote log server settings.

### To configure a remote log server:

1. Go to *System > Settings > Others*.
2. Enter the following information:

Field	Required	Description
Primary Server	N	Enter the primary log server IP address.
Primary Port	N	Enter the primary log server port number (mandatory if the server address is supplied).
Secondary Server	N	Enter the secondary log server IP address.

Field	Required	Description
Secondary Port	N	Enter the secondary log server port number (mandatory if server address supplied).

3. Click **Save**.

## Profiles

Use *System > Profiles* to view and edit the permissions for each profile.

Role Name	Role Type	Type
Admin	Service Provider	Default
Customer Admin	Customer	Default
Customer Monitor	Customer	Default



In previous versions, profiles were referred to as "roles". In the GUI, "roles" is still occasionally used, and is synonymous with "profiles".

## Page actions

The *Profile* tab contains the following actions:

- **Create:** Create a new profile.
- **Edit:** Edit the selected profile.
- **Delete:** Delete one or more selected profiles.
- **Search:** Search for profiles by name.
- **Show x entries:** Limit number of entries that are displayed at once (20 or 50).
- **Sort:** Sort columns in ascending or descending order.

## Create or edit a profile


**To create or edit a profile:**

1. In *System > Profiles*:
  - a. Click **Create** to create a new profile.
  - b. Select a profile and click **Edit** to edit the profile.



When editing a profile, the fields are same as those that appear when creating a profile, except that *Profile Type* cannot be changed.

2. Enter or update the following information:

Field	Required	Description
Name	Y	Enter a unique name for the role.
Profile Type	Y	<i>Provider</i> or <i>Customer</i> . <i>Customer</i> is synonymous with "organization".
Access Permissions	N	Select <i>None</i> , <i>Read</i> , <i>Read/Write</i> , or <i>Custom</i> permissions for this profile. Not all components offer custom permissions. If <i>Custom</i> is selected, sub-component permissions display.
		 For customer profiles, you may specify per-widget access permissions for the widgets that appear in <i>Insights</i> > <i>Dashboard</i> .

3. Click **Save**.

## Admins

Use *System* > *Admins* to configure FortiPortal administrators.

These are local users and the related commands are available only when *Authentication Access* is set as *Local* in *System* > *Settings* > *Authentication*.

## Page actions

The *Admins* tab contains the following actions:

- *Create*: Create a new administrator.
- *Edit*: Edit the selected administrator.
- *Delete*: Delete one or more selected administrators.
- *Trusted Hosts*: Edit trusted hosts for the selected administrator. Only available if *Blocked Hosts* is enabled in *System* > *Settings* > *General*.
- *Search*: Search for administrators by name.
- *Show x entries*: Limit the number of entries that are displayed at once (20 or 50).
- *Sort*: Sort columns in ascending or descending order.



You cannot delete the default admin user.

---

## Create or edit an admin

### To create or edit an administrator:


1. In the *Admins* tab:
  - a. Click *Create* to create a new administrator.
  - b. Select an administrator and click *Edit* to edit the administrator.



When editing an administrator, the fields are same as those that appear when creating an administrator.

---

2. Enter or update the following information:

Field	Required	Description
First Name	Y	Enter the first name of the administrator.
Last Name	Y	Enter the last name of the administrator.
Email	Y	Enter the email address of the administrator.
Password	Y	Enter the password of the administrator.
 The password must meet the requirements set by the password policy.		
Confirm Password	Y	Confirm the entered password.
Enable Password Policy	N	Enable or disable a password policy for this administrator. If enabled: <ul style="list-style-type: none"> <li>In <i>Must Contain</i>, select the following types of characters that the password must contain:               <ul style="list-style-type: none"> <li><i>Uppercase Letters</i></li> <li><i>Lowercase Letters</i></li> <li><i>Numbers (0-9)</i></li> <li><i>Special Characters</i></li> </ul> </li> <li>In <i>Minimum Length</i>, enter the minimum number of characters a password must contain.</li> </ul> This field is only available when creating a new administrator.
Contact Information		
Address 1	N	Enter the address of the user.
Address 2	N	Use this field to continue the address.
City	N	Enter the city name.
State	N	Enter the state or province name.
Country	N	Enter the country name.
Zip	N	Enter the postal code.
Phone	N	Enter the phone number.
Fax	N	Enter the fax number.
Profile		From the dropdown, select a profile. See <a href="#">Admin profiles on page 72</a> .
Active		Set the administrator status to active or inactive.
Enable Two-factor Authentication		Enable or disable two-factor authentication.

3. Click **Save**.

---

## Admin profiles

Use profiles to authorize an administrator to view and modify only the content that is required for that administrator. For example, a system administrator may require write access to FortiPortal configuration, but does not need write access to organization information.

Each profile defines the access rights of the user to specific FortiPortal components. The user may have read/write access to the content, or it may be hidden or read-only.

The system provides a default administrative profile. You can also create new profiles or customize the default profile.

The following table describes the default profile for administrators:

Profile	Description
Admin	The <i>Admin</i> profile provides full read/write access to all of the FortiPortal. The <i>Admin</i> profile also provides read-write access to the organization portal.



In previous versions, profiles were referred to as "roles". In the GUI, "roles" is still occasionally used, and is synonymous with "profiles".

---

## Theme

FortiPortal provides a default UI theme that is applied to the administrative web interface and the organization portal interface.

Use the *Theme* tab to configure and customize this theme. Configuration changes apply to both user interfaces (administrative and organization portal).

## Theme options

You can configure the theme as follows:

- Define custom URLs and text fields.
  - Custom text for your company name, service name, and service description.
  - URLs such as contact information and privacy policy.
- Select a color scheme:
  - *Dark*: A predefined dark theme.
  - *Light*: A predefined light theme.
  - *Custom*: Create a custom color scheme using *Color Picker*.
- Override organization top-level menu item text.
- Set up legal disclaimers.
- Upload custom images for the favicon, header logo, and service logo.





All of the custom fields are optional. Blank fields are ignored.

## Details of the theme configuration fields

The following table describes the configuration fields:

Settings	Guidelines	Default value
<b>URL Settings</b>		
Customize text and urls that appear in the header and footer. URL values must be specified with the full URL, including protocol (such as "https://").		
Company Name	The company name is displayed in the header of each page.	n/a
Service Name	Service name to display on the login page	
Service Login Footer	Footer text to display on the login page	
Header URL	Link for the company logo in the header.	blank
Contact URL	If specified, the footer contains a link to this URL with the text <i>Contact Us</i> .	blank
Legal URL	If specified the footer contains a link to this URL with the text <i>Legal</i> .	blank
Privacy URL	If specified. the footer contains a link to this URL with the text <i>Privacy</i> .	blank
Acceptable Use Policy URL	If specified, the footer contains a link to this URL with the text <i>Acceptable Use</i> .	blank
<b>Menu Options</b>		
Menu Options	Enable or disable menu text overrides. For each top-level menu item in the organization portal, specify custom text as needed.	
<b>Color Scheme</b>		
Color Scheme	Select a color scheme for the Admin pages. Select either the preconfigured color schemes ( <i>Dark</i> or <i>Light</i> ). To edit a custom color scheme, select <i>Custom</i> and then select <i>Edit Custom Color Scheme</i> .	Light

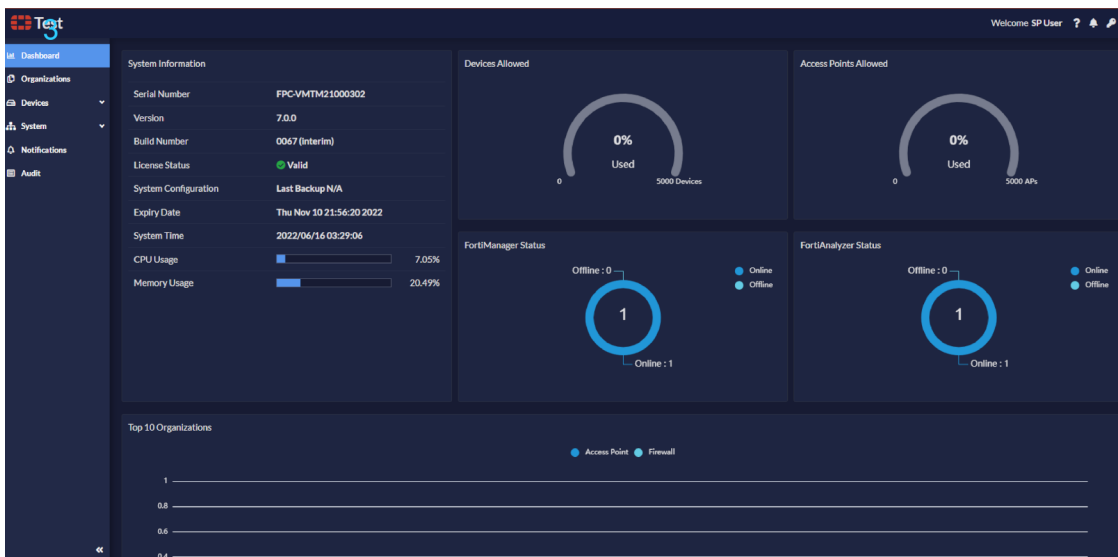
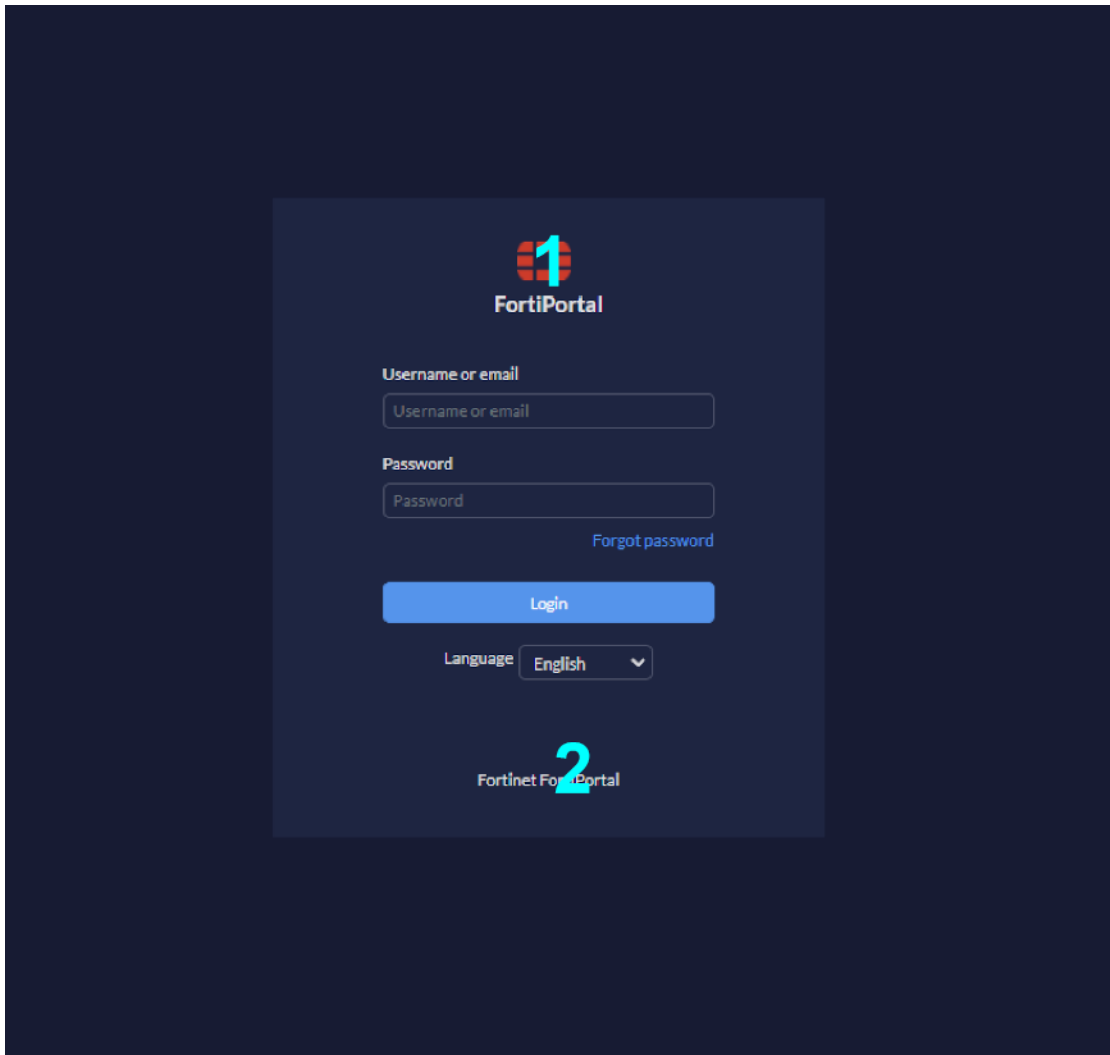
Settings	Guidelines	Default value
Color Picker	Visible only when you select <i>Custom</i> as the <i>Color Scheme</i> . Opens the <i>Edit Custom Color Scheme</i> window. See <a href="#">Editing a custom color scheme on page 76</a> .	n/a
<b>Disclaimers</b>		
Pre Login Disclaimer	Select the checkbox to enter content for the pre-login legal disclaimer.	blank
Post Login Disclaimer	Select the checkbox to enter content for the post-login legal disclaimer. Customer must accept the post-login disclaimer to be successfully logged in.	blank
<b>Image files</b>		
	Unless otherwise stated, the supported file types for images are jpg, png, and gif.	
Favicon Image	(Uploaded) Image file that FortiPortal will use as a Favorites icon. Supported file types include ico, jpg, png, and gif. The recommended file type is .ico and the maximum image size is 20x20 pixels.	blank
Header Logo Image	Image file that FortiPortal will use for the header logo. The recommended image size is 144x48 pixels.	blank
Service Logo Image	Image file that FortiPortal will use as the logo on the login page. The recommended image size is 104x80 pixels.	

## Custom URLs and text


The following figure displays the *URL Settings* pane.

The *URL Settings* pane sets URL and text fields for the login page. The maximum length of each custom text field is 100 characters.

The locations of the fields are shown in the following figure (see the table below for descriptions of the callout labels):



The following table describes the callout labels in the preceding figure:

Settings	Callout	What does it display?
Service Name	1	Service name and service logo image at the top of the login page.
Service Login Footer	2	Text at the bottom of the login page.
		 The login page does not include a separate footer color.
Company Name	3	Company name and header logo on the header of every page.

## Select a predefined color scheme

From the *Color Scheme* pane in the *Theme* tab, select one of the two predefined schemes; *Dark* or *Light*.

This scheme takes effect when you select *Save*.

## Editing a custom color scheme

**To edit a custom color scheme:**

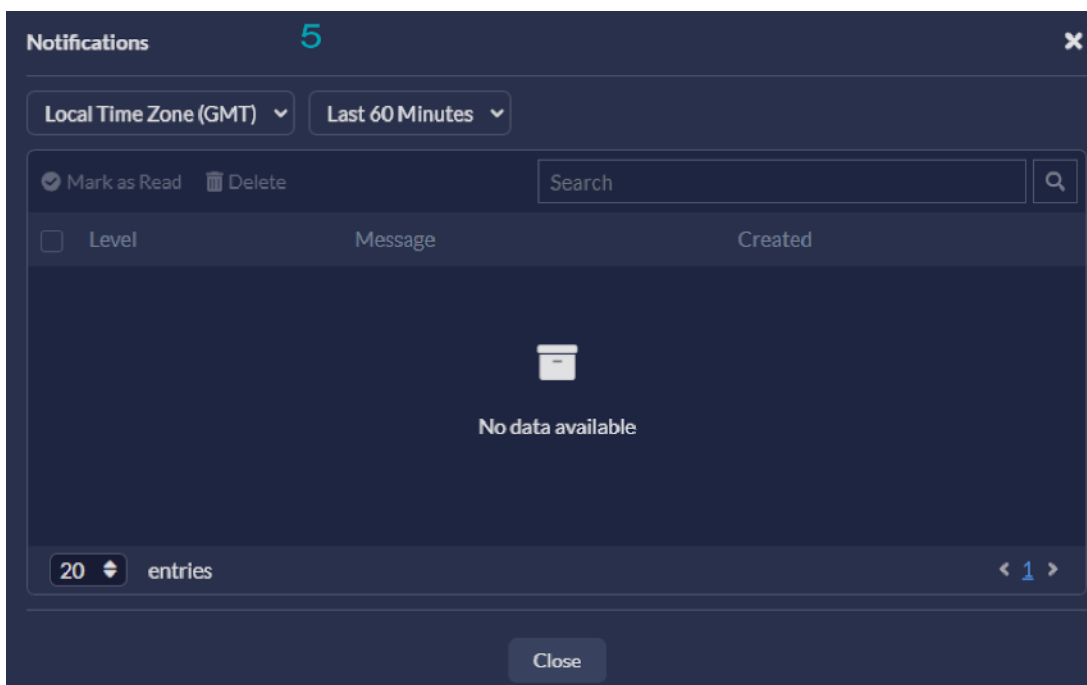
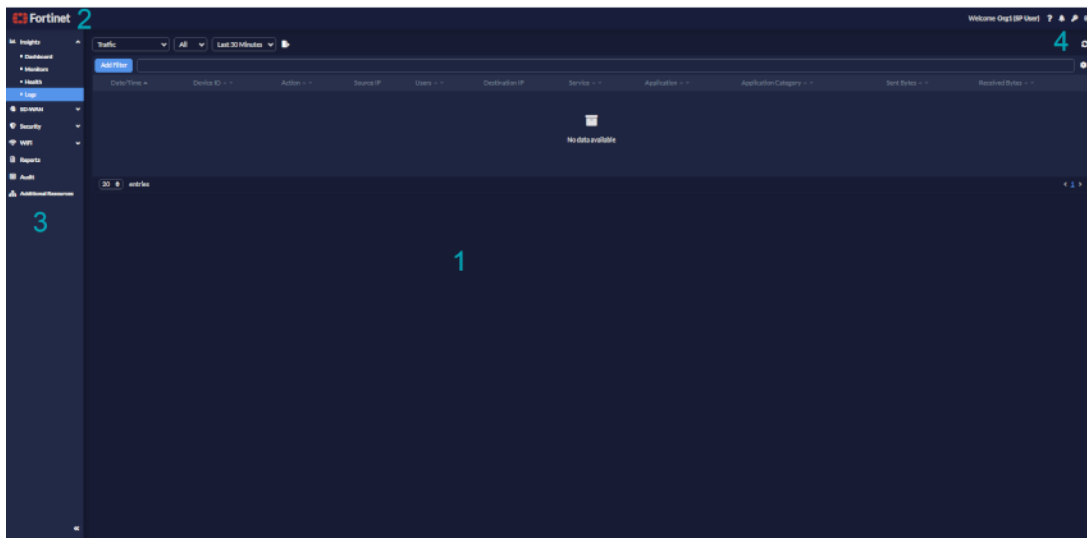
1. Go to *System > Theme*.
2. In the *Color Scheme* pane, select *Custom*.
3. Select *Edit Custom Color Scheme*.  
The *Edit Custom Color Scheme* window opens.

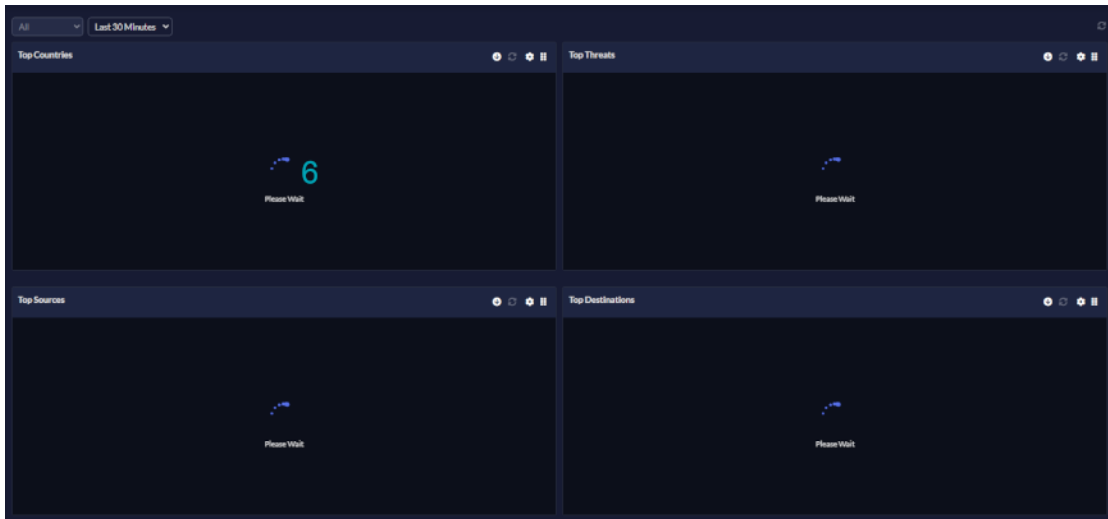
4. Edit the color scheme as needed. See [Color scheme options on page 79](#).
5. Click Save.



Changes take effect when the theme is saved successfully.

The following three figures show the page elements that have background colors and text colors that can be customized (see the table for descriptions of the callouts):





Callout	Label	Description
1	Page	Background and text color for the overall page, excluding the header and footer
2	Page Header	Background and text color for the top portion of the page.
3	Menu	Background and text color for the menu.
4	Button	Background and text color for the buttons on the page
5	Widget header	Background and text color for the widgets (and dialog boxes) on the dashboard and for some content on other pages.
6	Progress Bar	Background and text color for the progress indicator.

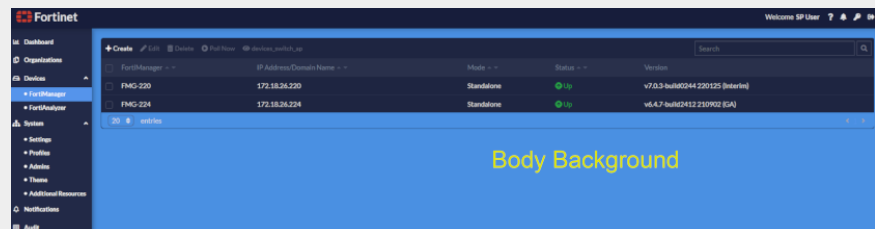
## Color scheme options

The *Edit Custom Color Scheme* window has the following panes:

1. **Reset to:** From the dropdown, select either *Dark* or *Light* theme to reset to.
2. **Global Settings:** From the *Font Family* dropdown, select a font style.
3. **General Colors:** Colors for the general GUI features.

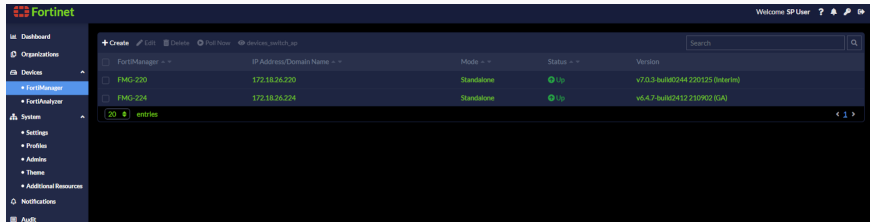
Body Background

The body background color of FortiPortal.



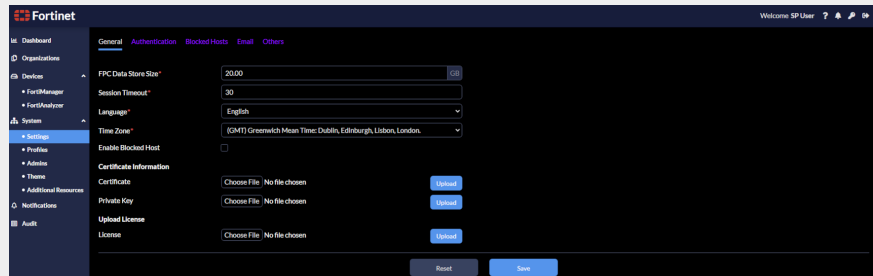
Font Color

Font color for the content pane and the page header.



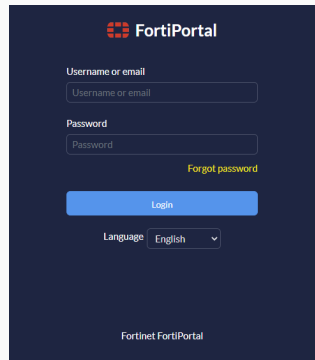
Font Link Color

Font color for sub-menus.



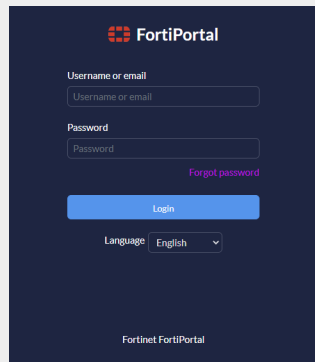
Link

The link color, e.g., the *Forgot password* link in the image below.



Link Hover

The link color when hovering.



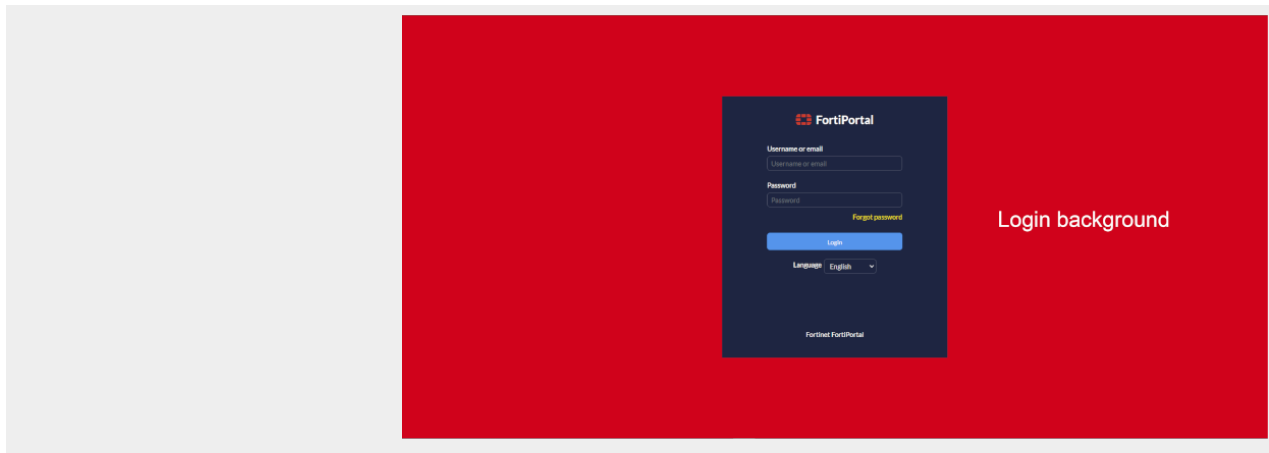
Link Disabled

Disabled link color.

Login Background

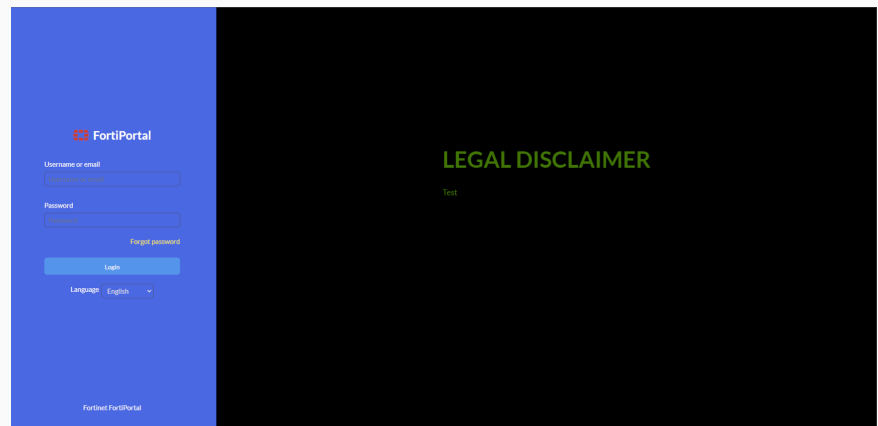
Login screen background color.





Disclaimer Text

The legal disclaimer text color.



Dividers Line

The color of the lines marking out the entire window.

Create New FortiManager

Name\*

Host\*

Username\*

Password\*

Confirm Password\*

Port\*443

XML Port\*8080

Polling FrequencyNo Polling

Cancel

Save

Notification Unread Background

The background color of unread messages.

Summary Background

The background color of the column names.

test8/FQVM08TM21001075fwactFirewall Policy

+ Create Edit Delete Action Column Settings

Search

#	Name	From	To	Source	Destination	Schedule	Service	Action	Security Profile	NAT
1	test79	any	any	all	all	always	ALL	Deny		
2	win test 0227 from fpc	any	any	all	all	always	ALL	Deny		
3	win test from fpc 0227 2	any	any	all	all	always	ALL	Accept	<div><div>g-default</div><div>g-default</div><div>g-default</div><div>g-default</div><div>default</div><div>no-inspection</div></div>	Disabled
4	win test 356	any	any	all	all	always	ALL	Accept	default	Disabled
5	wintestfpc2	any	any	all	all	always	ALL	Accept	no-inspection	Enabled
6	win policy with 06 022	win 0602++ SASE	any	all	all	always	ALL	Accept	<div><div>g-with-default</div><div>default</div><div>no-inspection</div></div>	Enabled
7	win test 0602222 2 updated!!	H52 fortillink	any	all	all	always	ALL	Accept	no-inspection	Disabled
8	win test 063	win 0603	any	all	all	always	ALL	Deny		
9	win test 123	any	any	all	all	always	ALL	Deny		
10	win test 12317770	any	any	all	all	always	ALL	Deny		

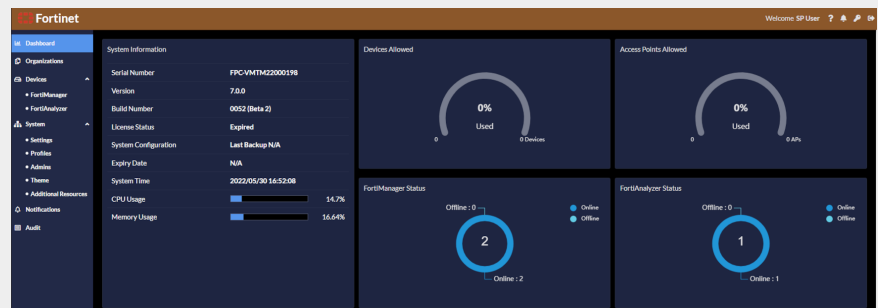
06/11

4. **Modal:** The background color of the dialog that displays.

5. **Header & Footer:** Header and footer colors.

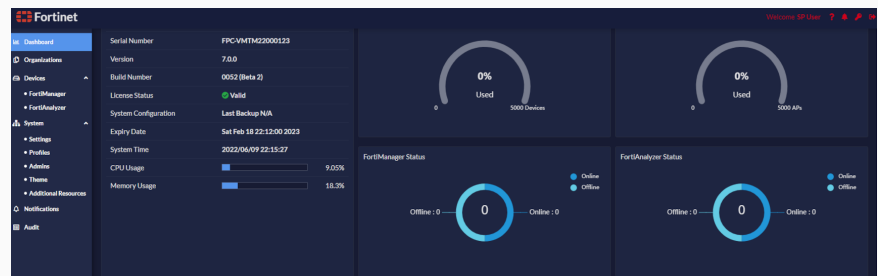
Header Background

The color of the header background.



Header Text

The color of the header icons and the message in the header.



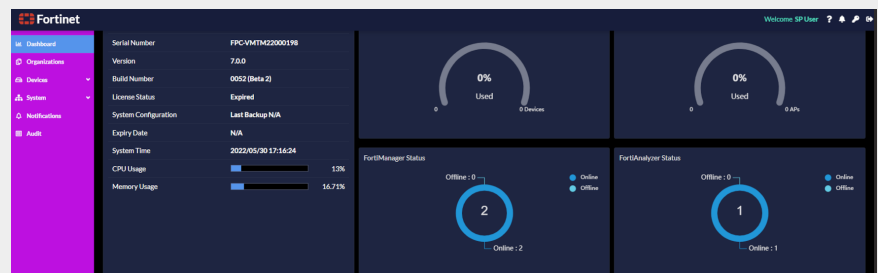
Footer Background

The color of the footer background.

6. **Menu:** Menu background and font colors.

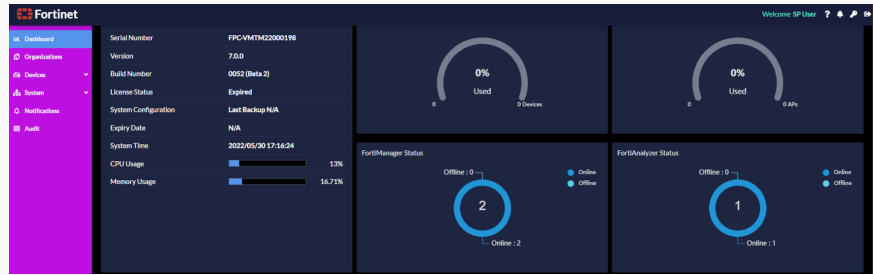
Background

The menu background color.



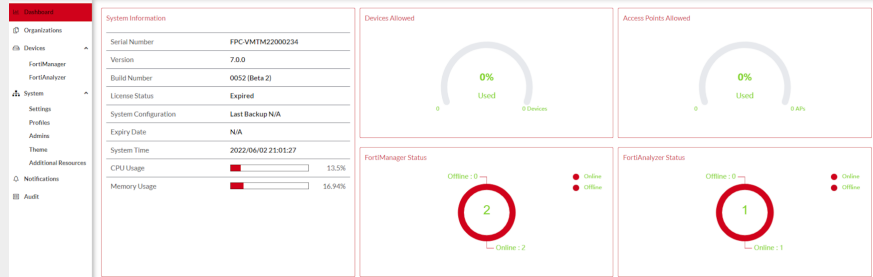
Active Background

The color of the selected menu item, e.g., *Dashboard* in the menu.



## Font Color

The color of the font for the menu items on the left.



## 7. Table: Table related colors.

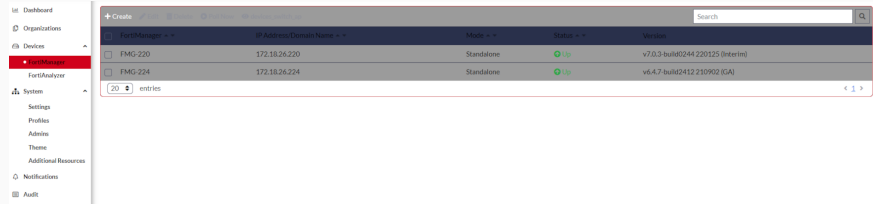
### Border

The color of the borders for a table.



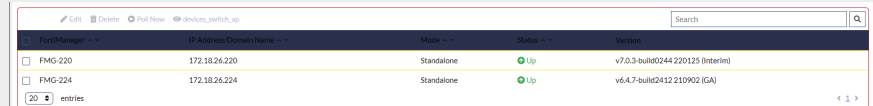
### Background

The color of the table background.



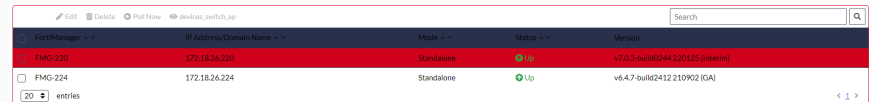
### Row Border

The color of the border separating rows in a table, e.g., the yellow line separating the two rows below.



### Row Hover

The color when you hover over a row in a table.

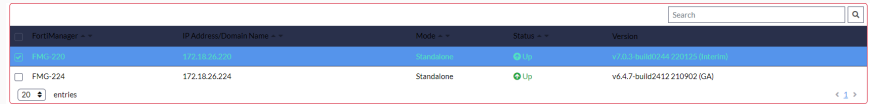


### Active Color

The color of the active contents in a table.

Row Checked Text

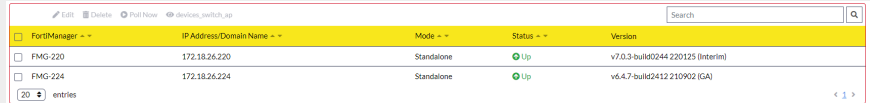
The font color when an item is selected in the table.



FortiManager	IP Address/Domain Name	Mode	Status	Version
<input checked="" type="checkbox"/> FMG-224	172.18.26.224	Standalone	Up	v6.4.7-build2412 210902 (GA)

Thead Background

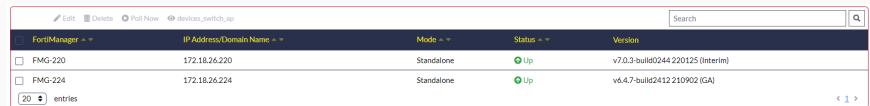
The background color of the table header.



FortiManager	IP Address/Domain Name	Mode	Status	Version
<input type="checkbox"/> FMG-220	172.18.26.220	Standalone	Up	v7.0.3-build0244 220125 (Interim)
<input type="checkbox"/> FMG-224	172.18.26.224	Standalone	Up	v6.4.7-build2412 210902 (GA)

Thead Text

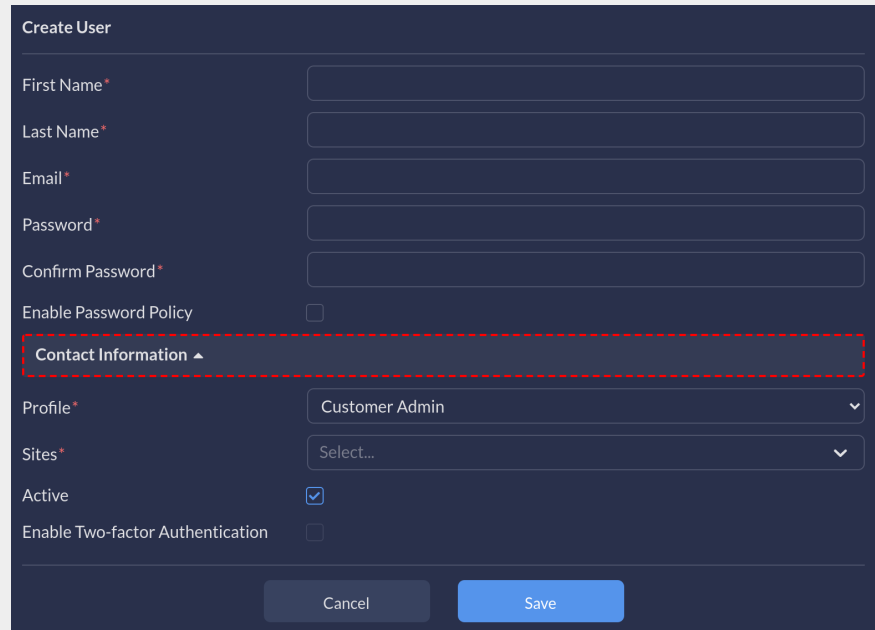
The font color of the table header.



FortiManager	IP Address/Domain Name	Mode	Status	Version
<input type="checkbox"/> FMG-220	172.18.26.220	Standalone	Up	v7.0.3-build0244 220125 (Interim)
<input type="checkbox"/> FMG-224	172.18.26.224	Standalone	Up	v6.4.7-build2412 210902 (GA)

Section Heading Background

The background color of the pane heading.



Create User

First Name \*

Last Name \*

Email \*

Password \*

Confirm Password \*

Enable Password Policy ☐

Contact Information ▲

Profile \* Customer Admin

Sites \* Select...

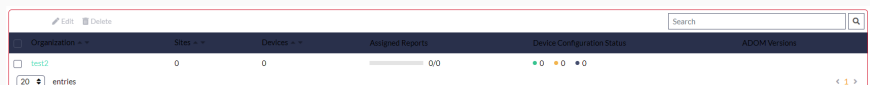
Active ☒

Enable Two-factor Authentication ☐

Cancel Save

Pagination Active Color

The color of the current page number, e.g., font color of page 1 in the image below.



Organization	Sites	Devices	Assigned Reports	Device Configuration Status	ADOM Versions
<input type="checkbox"/> test2	0	0	0/0	0 0 0	

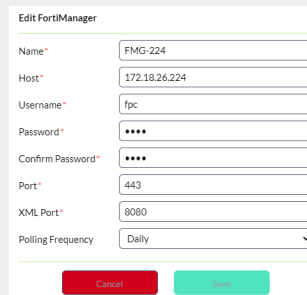
Pagination Color

The pagination color.

## 8. Buttons - Primary: Buttons related colors.

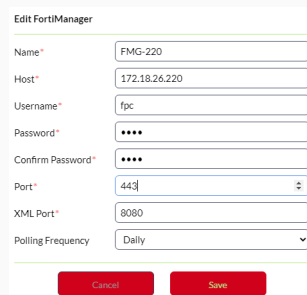
### Background

The primary button background color, e.g., the **Save** button background color in the image below.

A screenshot of the 'Edit FortiManager' form. It contains fields for Name (FMG-224), Host (172.18.26.224), Username (fpc), Password (masked with dots), Confirm Password (masked with dots), Port (443), XML Port (8080), and Polling Frequency (Daily). At the bottom, there are two buttons: 'Cancel' (red) and 'Save' (teal). The 'Save' button is the primary button.

### Text

The primary button font color, e.g., the color of the text in the **Save** button.

A screenshot of the 'Edit FortiManager' form, identical to the one above. The 'Save' button is highlighted with a blue border, and its text 'Save' is white, indicating the primary button's text color.

### Disabled Background

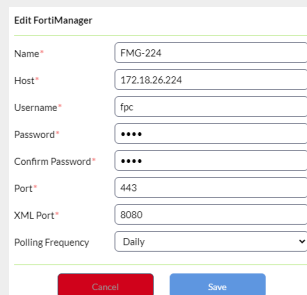
The disabled primary button background color.

### Disabled Text

The disabled primary button text color.

### Active Background

The active primary button background color, e.g., the color of the background of the **Save** button.

A screenshot of the 'Edit FortiManager' form, identical to the ones above. The 'Save' button is highlighted with a blue border and a blue background, indicating the active primary button's background color.

## 9. Buttons - Secondary:

### Background

The secondary button background color, e.g., the **Cancel** button background color.

The screenshot shows the 'Edit FortiManager' form with the following fields: Name (FMG-224), Host (172.18.26.224), Username (fpc), Password (masked with dots), Confirm Password (masked with dots), Port (443), XML Port (8080), and Polling Frequency (Daily). At the bottom, there are two buttons: 'Cancel' (red) and 'Save' (blue). The 'Cancel' button has a red border.

Border

The secondary button border color, e.g., the color of the border of the *Cancel* button.

This screenshot is identical to the one above, showing the 'Edit FortiManager' form with the 'Cancel' button having a red border.

Text

The secondary button font color, e.g., the color of the text in the *Cancel* button.

This screenshot is identical to the one above, showing the 'Edit FortiManager' form with the 'Cancel' button having a red border.

Active Background

The active secondary button background color, e.g., the color of the background of the *Cancel* button.

The screenshot shows the 'Edit FortiManager' form with the following fields: Name (FMG-220), Host (172.18.26.220), Username (fpc), Password (masked with dots), Confirm Password (masked with dots), Port (443), XML Port (8080), and Polling Frequency (Daily). At the bottom, there are two buttons: 'Cancel' (dark blue) and 'Save' (red). The 'Cancel' button has a dark blue background.

Active Border

The active secondary button border color, e.g., the color of the border of the *Cancel* button.

Disabled Background

The disabled secondary button background color.

Disabled Border

The disabled secondary button border color.

Disabled Text

The disabled secondary button text color.

## 10. Buttons - Light:

Text

The font color of the action buttons.

Active Text

The font color of the active action button.

Disabled Text

The font color of the disabled action buttons, e.g., *Edit*, *Delete*, *Poll Now*, and *devices\_switch\_ap* buttons in the image below.

## 11. Dropdown:

Background

The color of the dropdown background.

Border

The color of the dropdown border.



Text

The color of the text in a dropdown.

## 12. Forms Input: Forms related colors.

Input Border

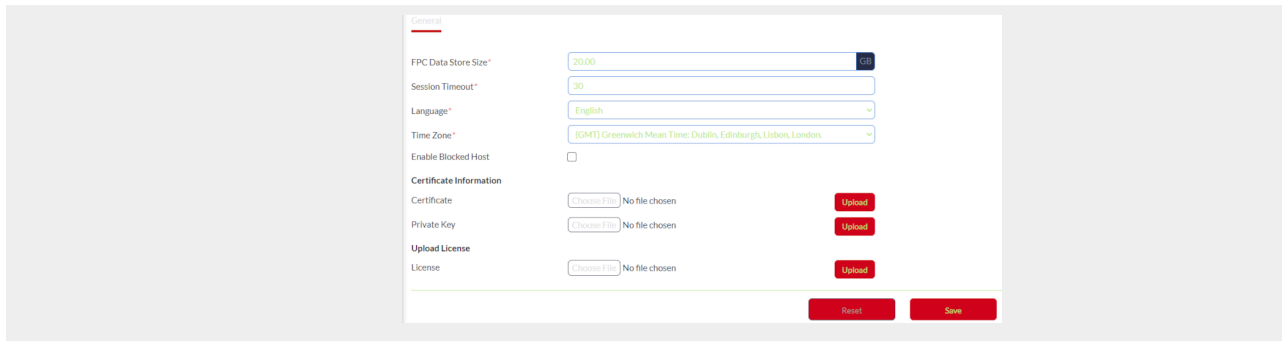
The borders colors of the input fields in a form.

Input Active Color

The color of the border of the active field in a form.

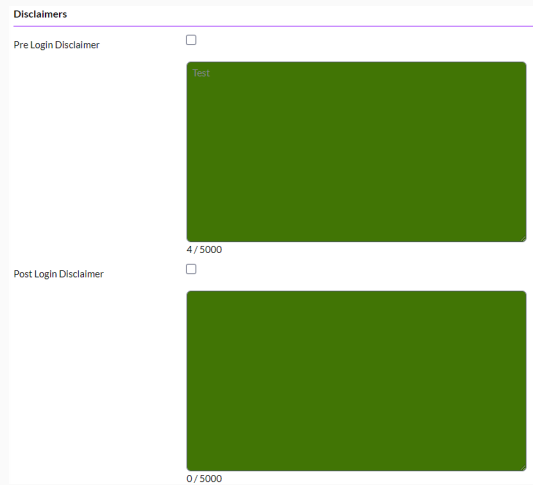
Input Text Color

The color of the text in a field.



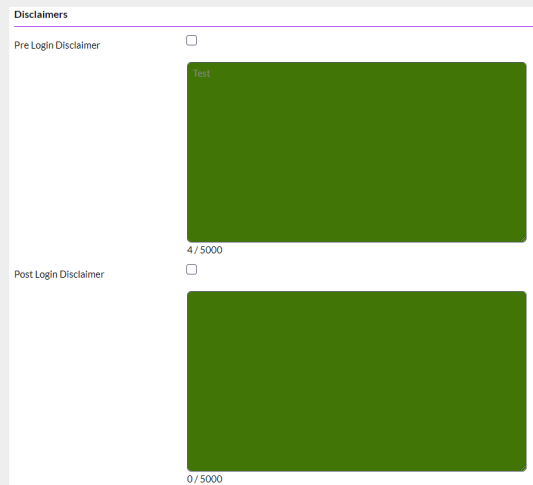
### Input Disabled Background

The color of the disabled input field.



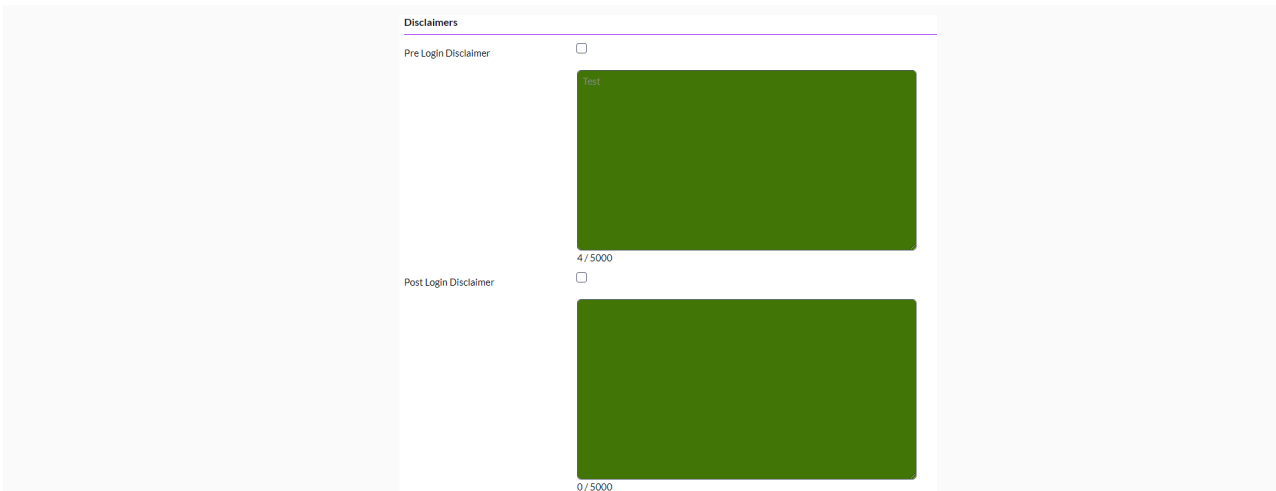
### Input Disabled Text

The font color in a disabled field, e.g., *Test* in the disabled fields below.



### Input Disabled Border

The color of the border of disabled fields in a form.

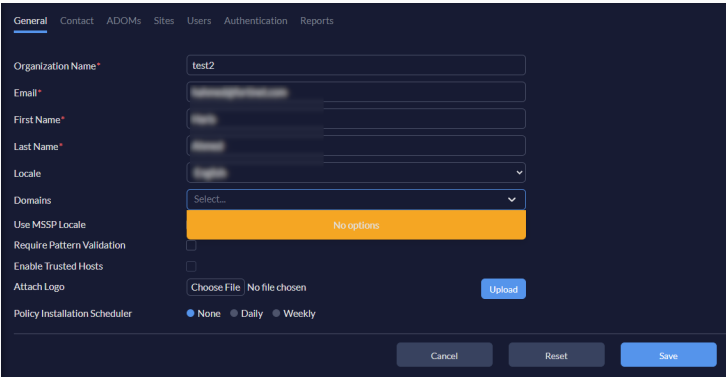


Input File Selected Text

The font color of the *Choose File* option when selected.

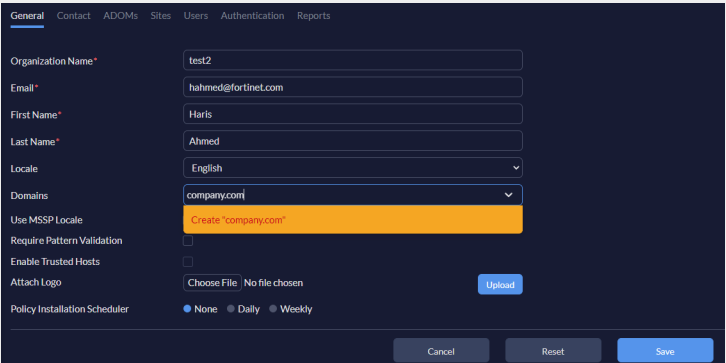
Select Option background

The background color when selecting an option.



Select Option Text

The font color when entering information in a *Select Option* field.



Select Option Active Text

The font color for options being selected in a *Select Option* field.

Select Disabled Border

The border color for the selected options where the options cannot be changed.

Select Disabled Text

The font color for the selected options where the options cannot be changed.

Select Disabled Background	The background color for the selected options where the options cannot be changed.
Select Disabled Tag Background	The background color for the selected options tags where the options cannot be changed.
Placeholder Font Color	The font color of the placeholder in a form, e.g., the text in the <i>Domains</i> option.



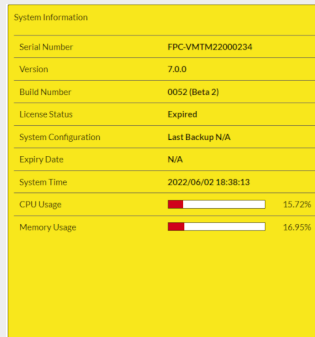
### 13. Forms - Checkbox & Radio Group: Checkbox and radio buttons related colors.

Radio & Checkbox Disabled	The color when a radio button or checkbox is disabled, e.g., the <i>Enable Trusted Hosts</i> checkbox
Radio & Checkbox Checked Disabled	The color when a radio or checkbox is selected and the setting is disabled.
Radio Group Text	The font color of the radio buttons group text.
Radio Group Checked Disabled Text	The font color of the radio group text when selected, but the options cannot be changed.
Radio Group Checked Disabled Background	The background color of the radio group when selected, but the options cannot be changed.
Radio Group Checked Disabled Border	The border color of the radio group when selected, but the options cannot be changed.

#### 14. Card: Card related colors.

##### Background

The background color of the widget.

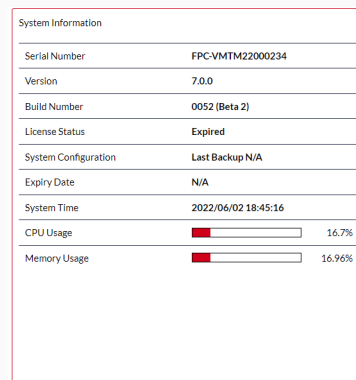


A yellow widget card with a title 'System Information' and a table of system details. The card has a solid yellow background.

System Information	
Serial Number	FPC-VM2M22000234
Version	7.0.0
Build Number	0052 (Beta 2)
License Status	Expired
System Configuration	Last Backup N/A
Expiry Date	N/A
System Time	2022/06/02 18:38:13
CPU Usage	<div><div></div></div> 15.72%
Memory Usage	<div><div></div></div> 16.93%

##### Border

The border color of a widget.

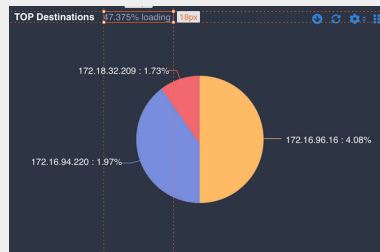


A white widget card with a red border. It contains the same system information table as the yellow card.

System Information	
Serial Number	FPC-VM2M22000234
Version	7.0.0
Build Number	0052 (Beta 2)
License Status	Expired
System Configuration	Last Backup N/A
Expiry Date	N/A
System Time	2022/06/02 18:45:16
CPU Usage	<div><div></div></div> 16.7%
Memory Usage	<div><div></div></div> 16.96%

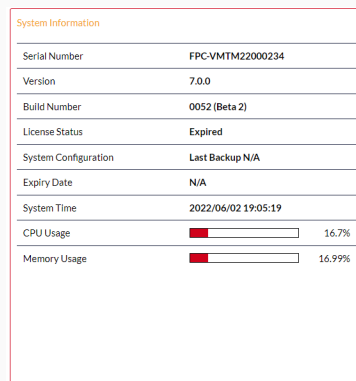
##### Percent Text

The color of the percent text.



##### Text

The font color of the heading in a widget.

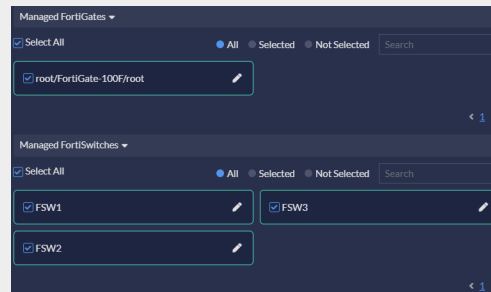


A white widget card with a red border. The heading 'System Information' is in orange. It contains the same system information table as the yellow card.

System Information	
Serial Number	FPC-VM2M22000234
Version	7.0.0
Build Number	0052 (Beta 2)
License Status	Expired
System Configuration	Last Backup N/A
Expiry Date	N/A
System Time	2022/06/02 19:05:19
CPU Usage	<div><div></div></div> 16.7%
Memory Usage	<div><div></div></div> 16.99%

### Device Selector Border

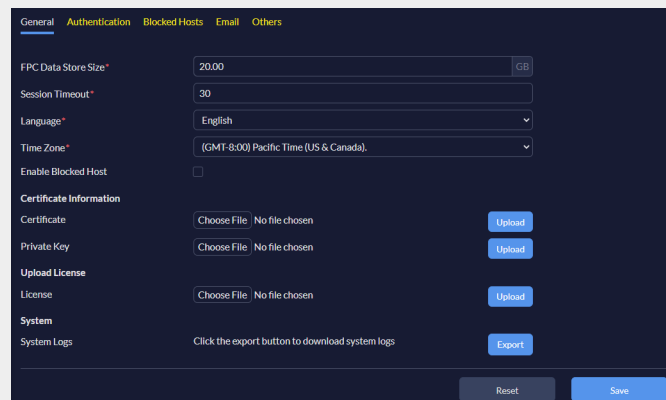
The border color for the device selector option.



- 15. **Chart:** Color settings related for charts in the dashboard.
- 16. **Loading:** The loading background and text related colors.
- 17. **Navbar:** Navigation bar related colors.

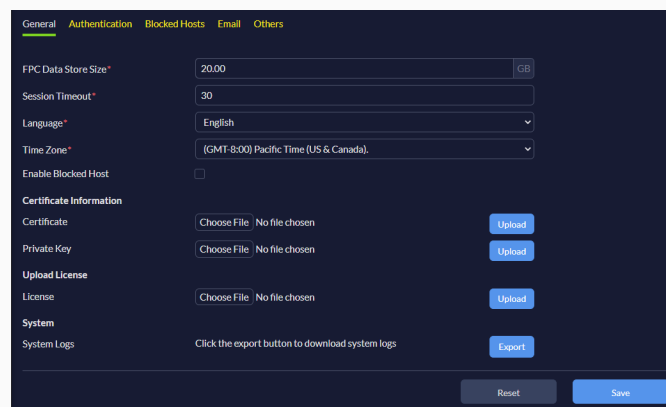
### Text Color

The font color for the navigation bar elements.



### Active Border

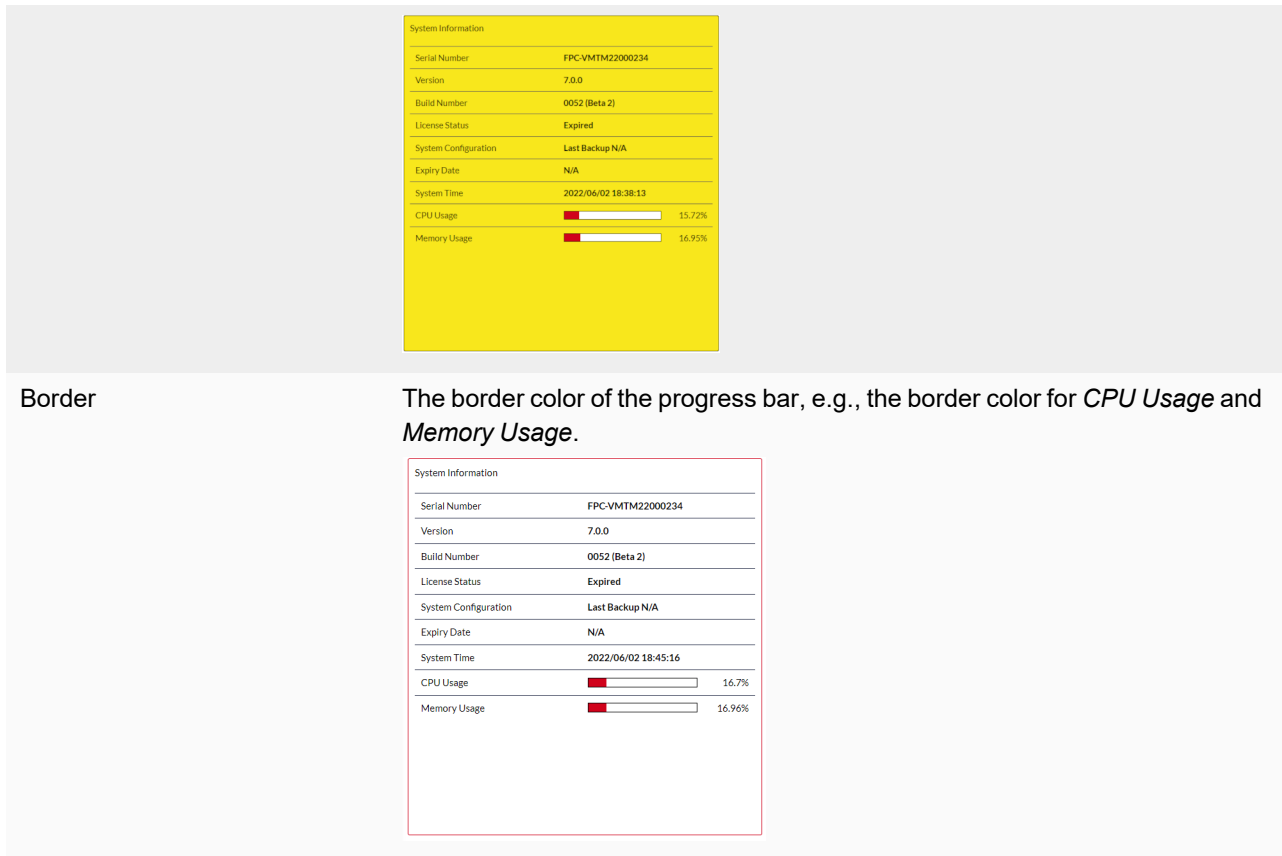
The border color of the active navigation bar element, e.g., the border color for the *General* tab.



- 18. **Progress Bar:** Progress bar related colors.

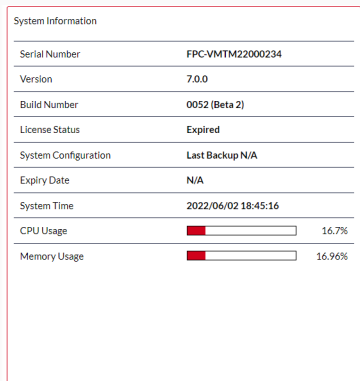
### Active

The color of the progress bar.



Border

The border color of the progress bar, e.g., the border color for *CPU Usage* and *Memory Usage*.



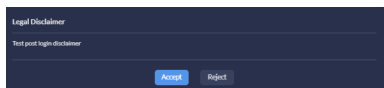
## Disclaimers

FortiPortal allows you to set up pre-login and post-login disclaimers.

A text area on the landing page presents a pre-login disclaimer to anyone attempting to log in. The following figure shows the pre-login disclaimer text area:



Once you are successfully authenticated, a post-login disclaimer banner appears only when the login attempt was made by a user. The user must click *Accept* to access FortiPortal. If the customer clicks *Reject*, they are logged out immediately.



When an administrative user attempts to log in, they only get the pre-login disclaimer. Post-login disclaimer appears only when a user attempts to log in to FortiPortal.

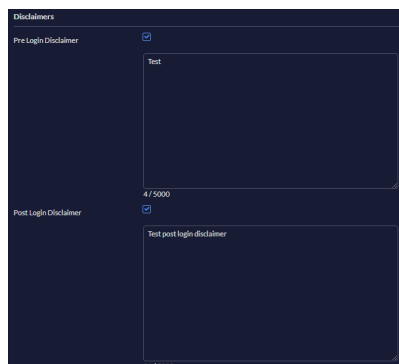


When a user logs in for the first time, a *Change Password* dialog appears asking the user to change the password.

### To set up disclaimers:

1. Go to *System > Theme*.
2. In the *Disclaimers* pane, select *Pre Login Disclaimer* and/or *Post Log in Disclaimer* checkboxes, and enter the disclaimer content.

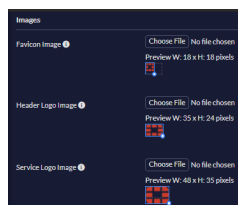
Both pre-login and post-login disclaimers are selected here.



3. Click *Save* to save the changes.  
At the next instance of login, and depending on whether you are an administrative user or a user, relevant disclaimers appear.

## Custom images

The following figure shows the *Images* pane:

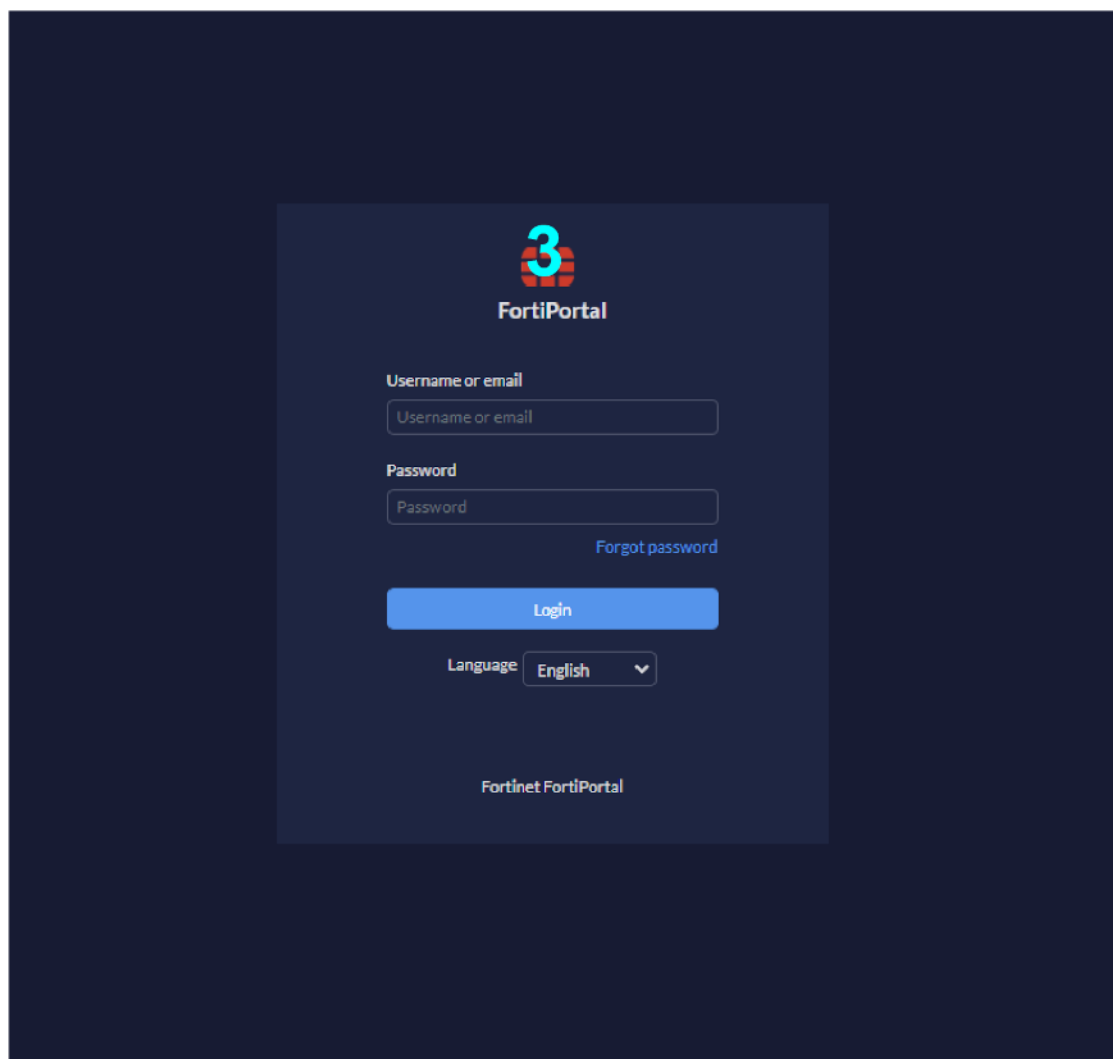






When the options in the *Images* pane are updated, the FortiPortal instance reboots.

Some of the custom image fields refer to the login page. The locations of the fields are shown in the following figure (see the table below for descriptions of the callout labels):



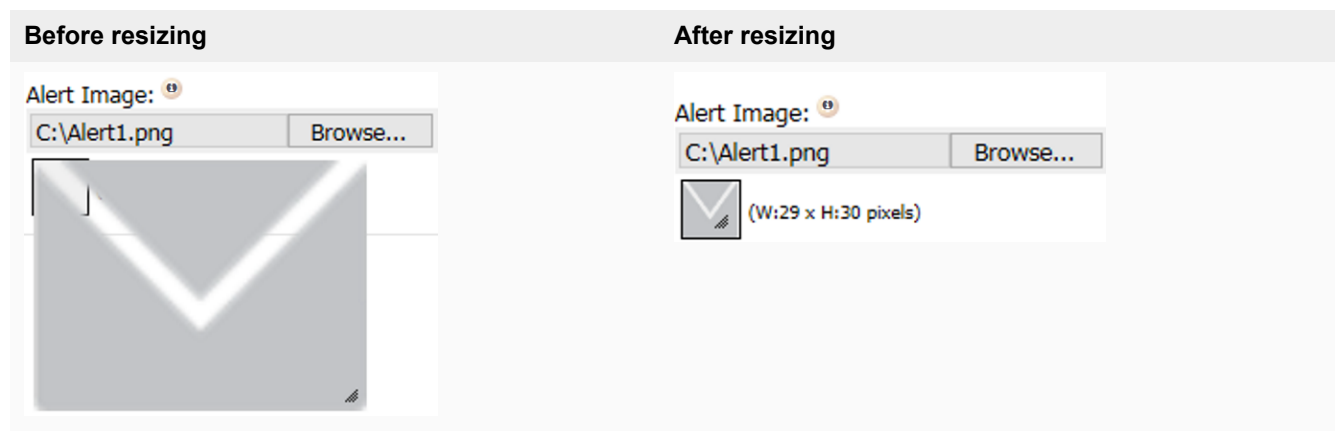
The following table describes the callout labels in the preceding figure:

Settings	Callout	What does it display?
Service Logo Image	3	Logo image for the service provider.

## Resizing images

When you upload an image for one of the custom fields, the system displays a thumbnail of the image. If the uploaded image is too large, you can drag from the right edge and bottom edge of the image to resize it. You can also drag from

the bottom right corner (or depress the shift key), to retain the current proportions of the image as it changes size. For assistance in resizing the image, the system provides a sizing box, and also provides the image height and width. The help (*i*) icon for each image field provides the minimum and maximum dimensions for each image. The following figure shows a downloaded alert icon image before resizing and after resizing:



## Additional Resources

Use *System > Additional Resources* to add, edit, delete, or view the displayed resources.

Additional resources display as buttons in the organization portal.

### Page actions

The *Additional Resources* tab contains the following actions:

- *Create*: Create a new resource.
- *Edit*: Edit the selected resource.
- *Delete*: Delete one or more selected resources.
- *Search*: Search for resources name or url.
- *Show x entries*: Limit the number of entries displayed (20 or 50)
- *Sort*: Sort columns in ascending or descending order.

#### To create or edit an additional resource:

1. In the *Additional Resources* tab:
  - a. Click *Create* to create a new resource.
  - b. Select a resource and click *Edit* to edit the resource.



When editing a resource, the fields are same as those that appear when creating a resource.

---

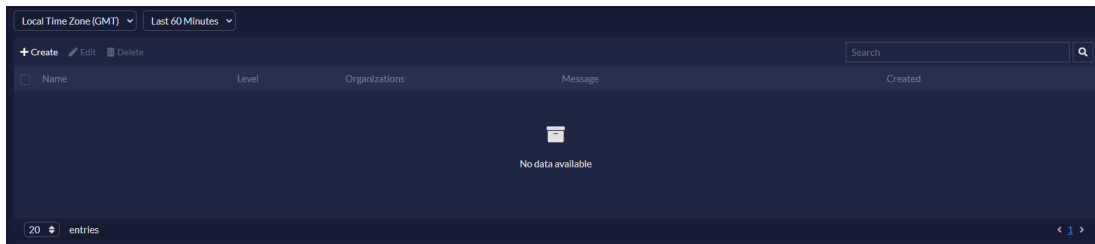
2. Enter or update the following information:

Field	Required	Description
Name	Y	Enter the resource name.
URL	Y	Enter the link to open when the button is clicked.
Status	N	Enable or disable the resource button. If set to <i>Disable</i> the button is visible but cannot be clicked.
Image	N	Upload a button image. The default image is pre-populated. You can change or resize the image with the <i>Choose File</i> button and resize icon.

3. Click *Save*.

# Notifications

Go to *System > Notifications* to view, create, edit, and delete system notifications.



## Page actions

The *Notifications* tab contains the following actions:

- *Time zone*: Set the time zone. The available options depend on the time zone selected in *System > Settings > General*.
- *Filter*: Filter the data by recency (*Last 60 Minutes*, *Last 1 Day*, *Last 1 Week*, or *Specify*).
- *Create*: Create a system notification.
- *Edit*: Edit the selected notification
- *Delete*: Delete one or more selected notifications.
- *Search*: Search for entries containing entered text.
- *Show x entries*: Limit the number of entries to display per page (20 or 50).

## Create or edit a notification

1. In *System > Notifications*:
  - a. Click *Create* to create a new notification.
  - b. Select a notification and click *Edit* to edit the notification.



When editing a notification, the fields are same as those that appear when creating a notification.

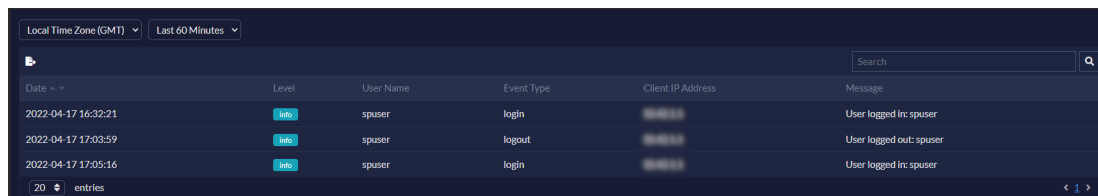
2. Enter or update the following information:

Field	Required	Description
Name	Y	Enter the name of the notification.
Level	Y	Select the level of importance of the notification.
Message	Y	Enter the text content of this notification. The maximum length of the message is 255 characters.
Organizations	Y	From the dropdown, select one or more organizations to receive the notification.

3. Click **Save**

# Audit

Use the *Audit* tab to view a log of administrator and user activity.



The screenshot shows the FortiGate Audit interface. At the top, there are two dropdown menus: 'Local Time Zone (GMT)' and 'Last 60 Minutes'. Below these is a search bar with a magnifying glass icon. The main area is a table with the following columns: Date, Level, User Name, Event Type, Client IP Address, and Message. The table contains three entries, all with a level of 'info' and user 'spuser'. The first entry is a login at 2022-04-17 16:32:21. The second entry is a logout at 2022-04-17 17:03:59. The third entry is a login at 2022-04-17 17:05:16. At the bottom left, there is a pagination control showing '20' and 'entries'. At the bottom right, there are navigation arrows and the number '1'.

Date	Level	User Name	Event Type	Client IP Address	Message
2022-04-17 16:32:21	info	spuser	login	192.168.1.1	User logged in: spuser
2022-04-17 17:03:59	info	spuser	logout	192.168.1.1	User logged out: spuser
2022-04-17 17:05:16	info	spuser	login	192.168.1.1	User logged in: spuser

## Page actions

- **Time zone:** Set the time zone. The available options depend on the time zone selected in *System > Settings > General*.
- **Filter:** Set the recency of the logs to display (*Last 60 Minutes*, *Last 1 Day*, *Last 1 Week*, or *Specify*).
- **Export to CSV:** Export the audit log list as a comma-separated value (CSV) file.
- **Search:** Search the audit log list by level, user name, event type, client IP address, or message.
- **Show x entries:** Limit the number of entries to display (20 or 50).
- **Sort:** Sort the *Date* column in ascending or descending order.

## Appendix A - Sizing recommendations

The table below shows sizing recommendations for the FortiPortal virtual machine and maximum values for numbers of organizations, FortiManager, and FortiAnalyzer.



The default memory size is 16 GB.

FortiPortal VM					
Number of organizations	Number of FortiManager	Number of FortiAnalyzer	Number of VMs	RAM (GB)	vCPU
250	25	25	1	16	4
500	50	50	1	16	8
1000	100	100	1	32	16
2500	250	250	1	64	16
5000	500	500	3(Cluster)	64	16
7500	500	500	3(Cluster)	64	24
10000	500	500	3(Cluster)	64	32

## Appendix B - Installation on KVM

FortiPortal software runs on virtual machines.

You can use KVM to create and manage the VM instances.

### Prerequisites

- KVM installed and running on the host server.
- Access to the KVM host server.

### Downloading virtual machine image files

**To download the VM files:**

1. Go to [FortiCloud](#) and log in to your account.
2. Go to *Support > Downloads > Firmware Download*.
3. Select FortiPortal from the product dropdown.
4. Click the *Download* tab.
5. Navigate to the appropriate directory.
6. Download the latest image file in QCOW2 format.

### Deploying the FortiPortal Virtual Machine

**To install the virtual machine:**

1. Launch *Virtual Machine Manager* on your KVM host server.
2. From the Virtual Machine Manager (VMM) home page, click *Create a new virtual machine*.
3. Select *Import existing disk image* and click *Forward*.
4. Click *Browse*.  
If you saved the image file to `/var/lib/libvirt/images`, it will be visible on the right. If you saved it somewhere else on your server, select *Browse Local*, find it, and click *Choose Volume*.
5. Select the *OS type* and *Version* you are running, and click *Forward*.
6. Specify the amount of memory and the number of CPUs to allocate to this virtual machine.  
Set the memory to a minimum of 16GB and the CPUs to a minimum of 4.  
See [Sizing recommendations on page 103](#) for more information.





FortiPortal interacts with FortiManager. To avoid the portal becoming a bottleneck, adjust the maximum CPU and memory sizes so that they equal the values for the FortiManager devices.

---

7. Click *Forward*.
8. Enter the name for the VM and click *Forward*.  
A new VM includes one network adapter by default.
9. Click *Finish*.

#### **To start the virtual machine:**

1. Launch *Virtual Machine Manager* on your KVM host server.
2. Select the VM from the list and click *Run*.
3. Right-click on the instance and click *Open* to see the login prompt.

#### **To configure the portal parameters**

The first time you start the portal, you will have access only through the console window of your VM server environment. After you configure the initial parameters, you can access FortiPortal through the web-based portal.

See [Basic setup on page 16](#) to continue the installation process.



[www.fortinet.com](http://www.fortinet.com)

---

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.