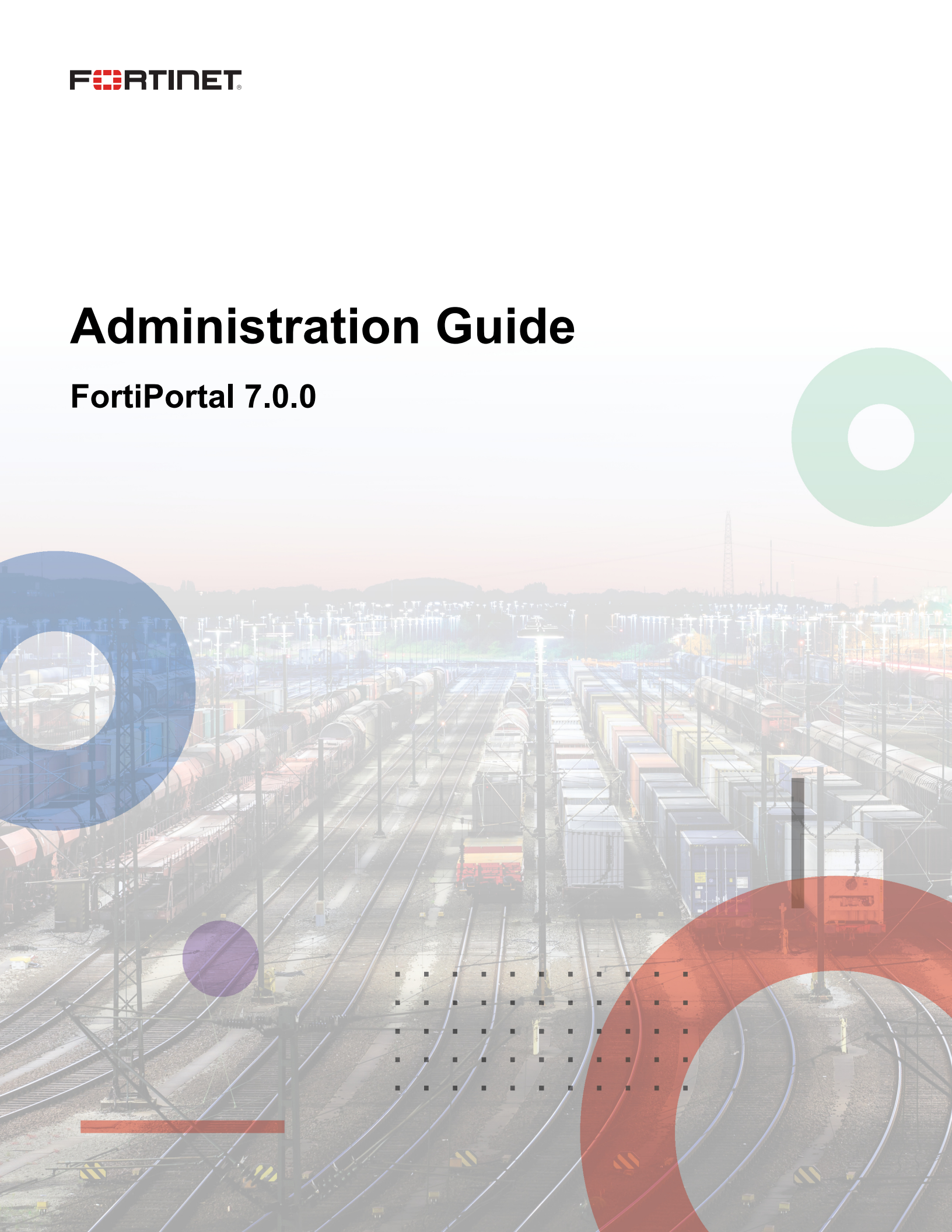


Administration Guide

FortiPortal 7.0.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



August 30, 2022

FortiPortal 7.0.0 Administration Guide

37-700-735199-20220830

TABLE OF CONTENTS

Change Log	5
FortiPortal overview	6
Key features	6
Language support	6
Components	6
Organization devices	7
FortiPortal concepts	8
Sites	8
Storage limits	8
Remote authentication	9
Trusted Hosts	9
Frequently asked questions	9
FortiPortal installation	11
Installation on VMware	11
Downloading virtual machine image files	11
Installing FortiPortal VMs	11
Starting the VM	12
Basic setup	13
Sizing	13
Default login credentials	13
Configuring FortiPortal	14
FortiManager configuration	16
FortiAnalyzer configuration	17
Additional setup tasks	17
Alerts	18
Page actions	18
Dashboard	19
Initial data-aggregation delay	21
Organizations	22
Page actions	22
Create or edit an organization	23
General	23
Contact	25
Adoms	25
Sites	26
Users	27
User roles	30
Authentication	31
Reports	32
FortiAnalyzer reports	32
Page actions	32
Devices	33
FortiManager devices	34

Page actions	34
Add a FortiManager	34
Edit a FortiManager	34
Manage FortiGate, FortiSwitch, and FortiAP devices	35
FortiAnalyzer devices	37
Prerequisites	37
Page actions	37
Edit a FortiAnalyzer	38
View FortiAnalyzer reports	38
System	40
Settings	41
General	41
Authentication	43
Blocked Hosts	55
Configuring a scalable cluster	56
Email	58
Profiles	58
Page actions	58
Create a profile	59
Admins	59
Page actions	60
Create an admin	60
Admin user roles	62
Theme	62
Customer theme options	62
Select a predefined color scheme	63
Editing a custom color scheme	63
Custom URLs and text	83
Disclaimers	85
Custom images	86
Resizing images	87
Details of the theme configuration fields	88
Additional Resources	90
Page actions	90
Notifications	91
Page actions	91
Create notifications	91
Audit	93
Page actions	93
Appendix A - Sizing	94

Change Log

Date	Change Description
2022-07-04	Initial release.
2022-07-08	Updated Remote authentication - SSO on page 51 . Updated Configuring a scalable cluster on page 56 . Removed SNMP.
2022-07-12	Updated Installation on VMware on page 11 .
2022-07-14	Updated Appendix A - Sizing on page 94 . Updated Configuring a scalable cluster on page 56 .
2022-08-30	Removed Appendix C - Installation using Nutanix and Appendix B - Installation using KVM.

FortiPortal overview

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

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

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

Language support

FortiPortal supports the following languages:

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

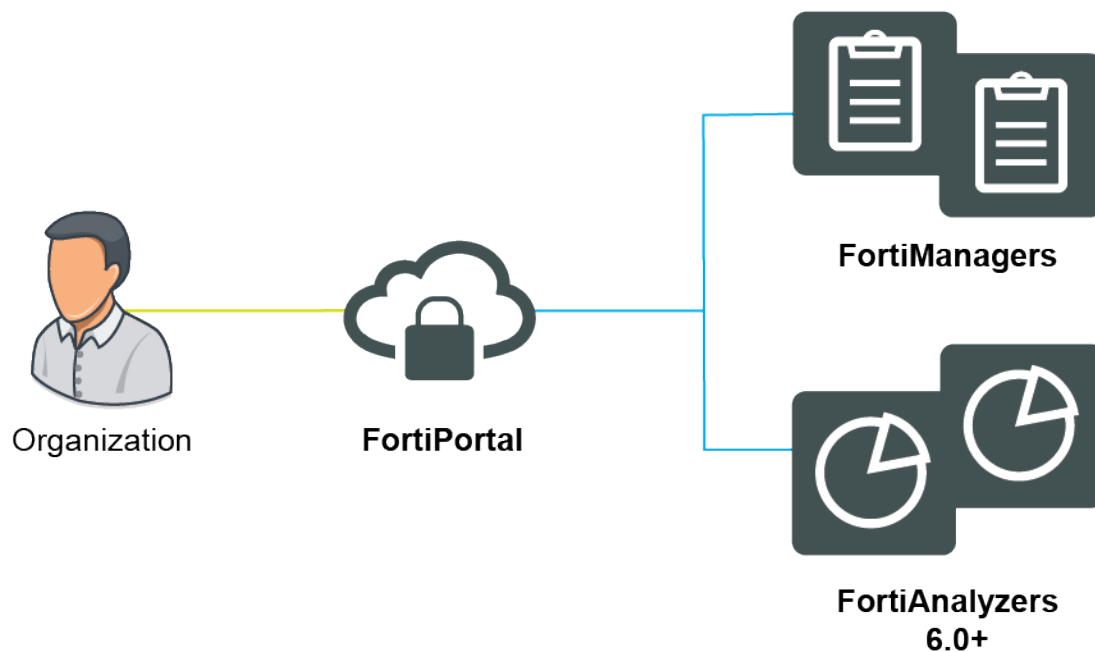
Components

The organization's FortiGate devices are managed by one or more FortiManagers. Optionally, logs from the FortiGate devices can be gathered by one or more FortiAnalyzers. The portal aggregates the FortiAnalyzer logs into a central database and performs security analytics on the logs.

The portal provides an administrative web interface (for the administrative staff) and an organization web interface (for the organizations).

FortiAnalyzer mode

The following figure shows the FortiPortal components in FortiAnalyzer mode and a typical organization network.



The FortiPortal solution includes the following components in FortiAnalyzer mode:

- Portal: virtual appliance:
 - Provides the administrator web interface and the organization web interface.
 - Uses the FortiManager API to manage devices, objects, and policies
 - FortiPortal includes only one portal (however, the portal can consist of multiple VM instances for redundancy and/or scalability)

The organization web interface enables each organization to access/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).

The administrative web service allows the administrator to configure the services for each organization, and to manage the overall cloud service.

Organization devices

FortiPortal requires that the organization FortiGate devices must be managed by FortiManager.

FortiManagers may reside in the organization network or in the cloud.

1. FortiGate: security devices in the organization environment:

- Generates the security logs
- Also fulfills the AP Wireless Controller role

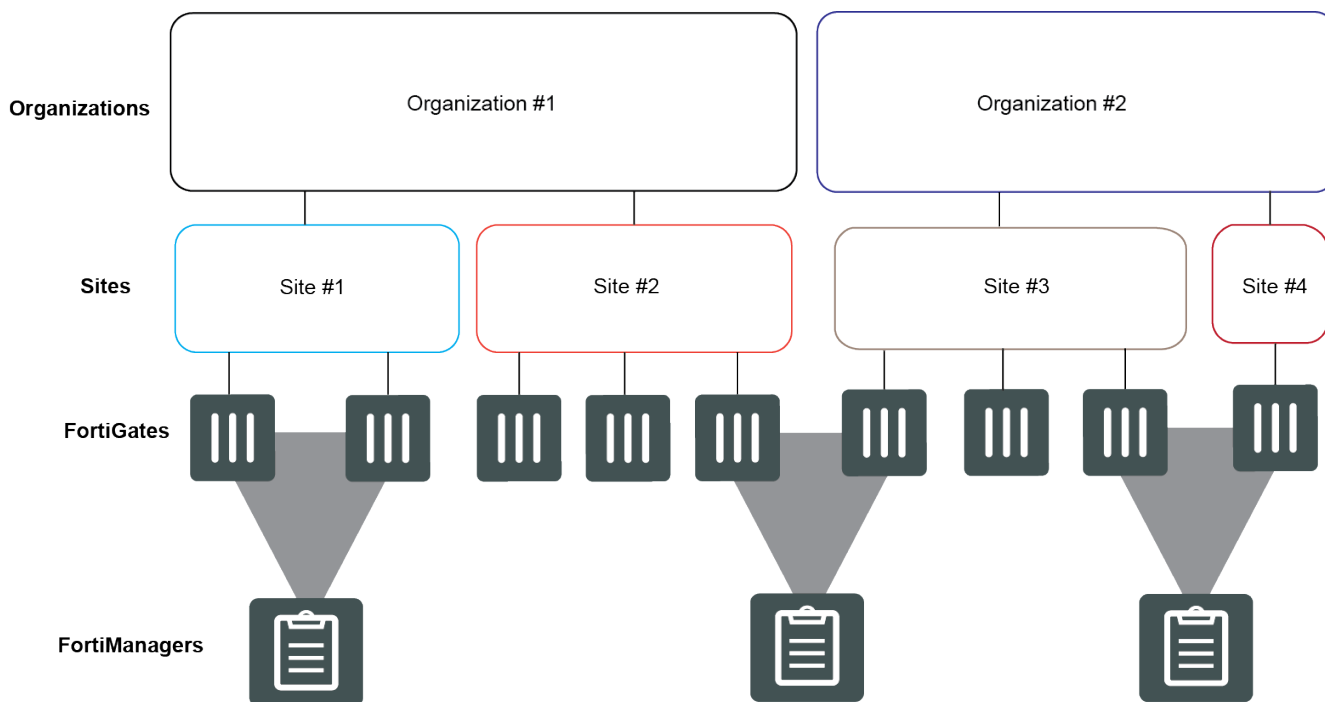
2. **FortiManager:** manages a set of FortiGate devices:
 - All FortiGate devices in the FortiPortal must be managed by FortiManager
 - FortiManager provides device information to the FortiPortal
 - May reside in the organization network or in the cloud
3. (Optional) **FortiAnalyzer:** receives logs from the devices:
 - May reside in the organization network or in the cloud

FortiPortal concepts

FortiPortal introduces the following 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 devices or AP wireless devices.



Storage limits

Each organization has a storage capacity maximum amount, which is expressed as a number of GB of database storage.

If an organization exceeds their storage limit, one of the following strategies is applied (this is configurable for each organization):

- Overwrite the oldest logs
- Stop logging

Remote authentication

You have the choice of local or remote user authentication of the admin and organization portal users. Local authentication works by defining the users in the local user databases. Remote authentication provides a choice of Radius authentication or FortiAuthenticator. The choice of authentication method is global to the whole FortiPortal.

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 Hosts

If you are using local user authentication, you can add the Trusted Hosts capability as an added level of security. You can apply the Trusted Hosts capability as a global feature. Optionally, you can add per-organization allowlists.

If you enable blocked hosts as a global setting, the system enforces a configurable blocklist for all admin and users.

You can also enable Trusted Hosts as an organization setting. The system creates an allowlist of trusted hosts for the users. The default entry in the allowlist is to allow all users, so you need to delete this entry to create a real allowlist.

For an organization with Trusted Hosts enabled, the system also enforces the global blocklist and allowlist for the users.

Frequently asked questions

What should I do when I upgrade or replace a FortiGate or FortiGate VM under 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.



If you create a new ADOM with the latest version, move the device to the new ADOM, and delete the old ADOM, there will be polling issues. 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?

Select the *Users* tab when editing an *Organization* and then select a user and select *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.

FortiPortal installation

This chapter covers the following tasks:

- [Installation on VMware on page 11](#)
- [Basic setup on page 13](#)
- [Additional setup tasks on page 17](#)

FortiPortal software provides a self-service management interface for organizations (or any organization that uses FortiManager to manage security instances) to monitor and configure security instances without direct FortiManager access. FortiPortal is a web application and runs on virtual machines.



Remember to protect FortiPortal with an external firewall. External users should only connect to the portal VM. They should not make direct connections to the FortiManager.

Installation on VMware

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

All VM instances run on VMware ESXi Server versions 5.5, 6.0, 6.5, 6.7, and 7.0.

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

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. Extract the 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 12](#).
2. Configure VM hardware settings. See [Configuring VM hardware settings on page 12](#).
3. Power on the VM. See [Starting the VM on page 12](#).
4. Configure the portal parameters. See [Basic setup on page 13](#).

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 VM CPU, memory, and storage settings and click *Save*. The following are the **minimum** requirements:
 - CPU: 4
 - Memory: 16 GB
 - Hard drive: 12 GB

See [Appendix A - Sizing on page 94](#) for more information.

The portal interacts with FortiManager. To avoid the portal becoming a bottleneck, you can 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 13](#)
- [Default login credentials on page 13](#)
- [Configuring FortiPortal on page 14](#)
- [Basic setup on page 13](#)
- [FortiManager configuration on page 16](#)
- [FortiAnalyzer configuration on page 17](#)

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. (The 2-GB disk in the VM is the flash memory; the 12-GB disk is storage.) If you have many organization logins and many devices, increase the memory and disk sizes for improved performance.

See [Appendix A - Sizing on page 94](#) for more information.



FortiPortal requires at least 16 GB of memory.

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:

1. Before you can access the portal GUI, you must configure the VM port1 with an IP address and administrative access using the CLI console.

- a. Log in to the console using the default console/SSH credentials.

- b. To change the admin password using the CLI:

```
config system admin user
  edit admin
    set password
    Old password: xxxxxx
    New password: yyyyyy
    Retype password: yyyyyy
  end
```

- c. 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/x.x.x.x
  end
```

- d. 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
```

- e. 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
```

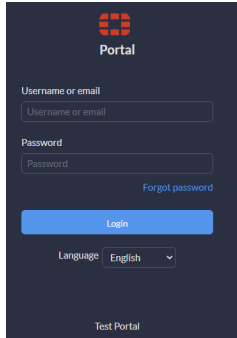
- f. Optionally, in the CLI console, enter the following commands to configure the NTP server for the instance:

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



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 may change the login credentials.



The left pane is common for all of the pages (*Dashboard, Organizations, Devices, System, Notifications, and Audit*).

3. Upload the license file. Go to *System > Settings > General*, and click *Upload* in *Upload License*. After the license is uploaded, check that the license status is valid and the number of devices allowed is correct. See [Dashboard on page 19](#).



The individual portal VM does not have serial numbers.

Updating the SSL certificate file

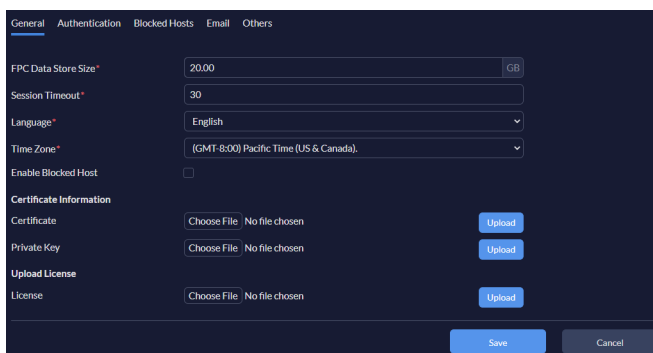
If you are setting up a demo server, you can skip this procedure.



You must upload the license first.

Use the following steps to import an SSL certificate for the FortiPortal VM.

From 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 for the FortiPortal in the PKCS#8 format.



Do not use certificate import and export commands from the portal VMs because they apply to the administration interface and not the FortiPortal application. The certificate signing request must be done on an external host and the signed certificate imported. For example:

```
openssl genrsa -des3 -out server.key 1024
cp server.key server.key.org
openssl rsa -in server.key.org -out server.key
openssl req -new -key server.key -out server.csr
openssl pkcs8 -topk8 -nocrypt -in server.key -out portal.key
openssl x509 -req -days 365 -in server.csr -signkey portal.key -out
server.crt
```

After these steps are done, you need to upload the certificate file (*.crt file) and portal.key file from the FortiPortal UI (as instructed in the administration guide). After uploading the certificate file, restart your portal VM.

FortiManager configuration

You need to configure FortiManager to work with FortiPortal.

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

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

2. Create a portal user with read-and-write permission:

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

3. *The workspace mode must be enabled for FortiManager to work with FortiPortal.*

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

4. Add your FortiManager device using the JSON port. You must poll FortiManager to see the device list. For more information about adding FortiManagers to the portal, see [FortiManager devices on page 34](#).

Name	IP Address/Domain Name	Mode	Status	Version
FortiManager				
FMG-demo	192.168.1.100	Standalone	Up	v7.0.3-build0254.220202 (GA)
FMG-120	192.168.1.101	HA	Up	v7.0.3-build0251.220131 (Interim)
FMG-234	192.168.1.102	Standalone	Up	v6.4.7-build0412.210902 (GA)
FMG-121	192.168.1.103	Standalone	Up	v7.2.0-build1074.220310 (Interim)

FortiAnalyzer configuration

You need to configure FortiAnalyzer to work with FortiPortal.

1. The ADOM mode must be enabled for FortiAnalyzer to work with FortiPortal. You must enable the interface permission `webservice` on FortiAnalyzer for the portal-facing interface.
2. You must allow remote procedure calls. Create an admin user for portal:

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



To add a FortiAnalyzer, see [FortiAnalyzer devices on page 37](#).

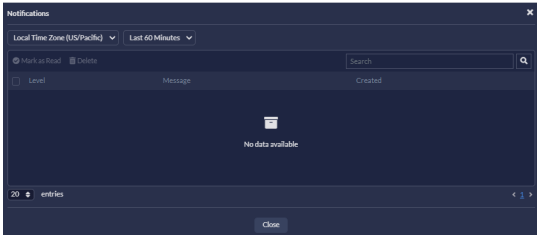
Additional setup tasks

After performing the basic installation, there are additional setup tasks to fully complete your configuration:

- To add additional FortiManager devices, see [FortiManager devices on page 34](#).
- To add wireless controllers, see [Manage FortiGate, FortiSwitch, and FortiAP devices on page 35](#).
- To add FortiAnalyzer devices, see [FortiAnalyzer devices on page 37](#).
- To create an organization, see [Create or edit an organization on page 23](#).
- To create sites, see [Sites on page 26](#).
- To create site administrators, see [Users on page 27](#).

Alerts

Selecting the *Alerts* icon displays a list of unread alerts:



For each alert, the window displays the following:

- *Level*—severity of the alert (*Informational* or *Warning*)
- *Message*—text summary of the alert
- *Created*—time the alert was raised (displayed for GMT time zone).

Page actions

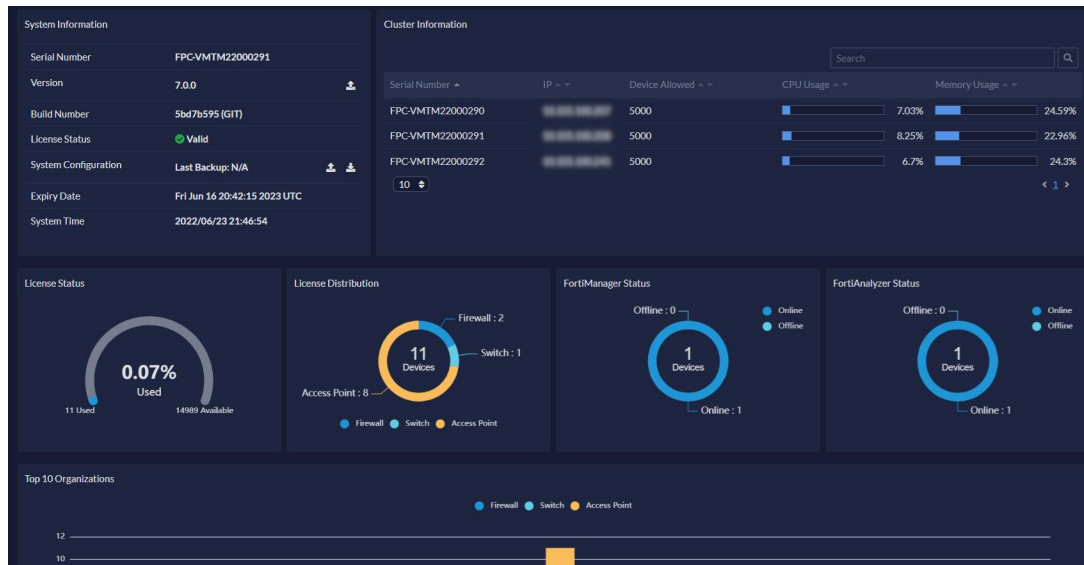
The *Alerts* window contains the following actions:

- *Time zone*—use the dropdown to set the time zone to *Local Time Zone (US/Pacific)* or *GMT Time Zone*
- *Filter*—filter the data (Last 60 Minutes, Last 1 day, Last 1 week, or Specify)
- *Mark as Read*—mark selected alerts as read
- *Delete*—delete selected alerts
- *Search*—enter text to search for alerts containing that text
- *Select*—select individual alerts, or select all alerts (select box in the column header)
- *Show x Entries*—use the dropdown selector to set the number of entries to display

Dashboard

The dashboard displays information about the FortiPortal and is organized as a set of widgets.

The dashboard also includes information about the system.



The dashboard includes the following default widgets:

- **System Information**

The *System Information* widget includes the following information:

Fields	Description
Serial Number	FortiPortal serial number.
Version	FortiPortal version.
Firmware Management (🔍)	Select the icon to open the <i>Firmware Management</i> dialog. See Firmware Management .
Build Number	FortiPortal build number.
License Status	FortiPortal license status. To upload a license, see Upload a license on page 42 .
System Configuration	Last backup and restore activity. See Backup and Restore .
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 General on page 41 .

- *Cluster Information*

FortiPortal cluster related information including instance serial numbers, IP address, devices allowed, CPU and memory usage.



- 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*

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*

Firmware Management

To upgrade FortiPortal firmware:

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

Backup and restore

To create a backup of the FortiPortal configuration:

1. Go to *Dashboard*.
2. In the *System Information* pane:
 - a. In *System Configuration*, select the *Backup* (📄) icon to save a backup file onto the local computer.

To restore a backed-up FortiPortal configuration:

1. Go to *Dashboard*.
2. In the *System Information* pane:
 - a. In *System Configuration*, select the *Restore* (📄) .
 - b. In the dialog that appears, select *Choose File* and locate the backup file on your local computer.
 - c. Select *Upload*.



FortiPortal reboots to complete restoring a backup.

Initial data-aggregation delay

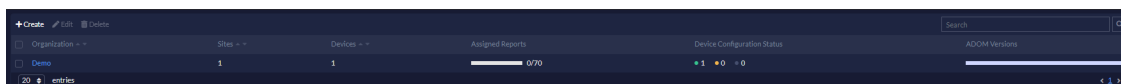
After FortiPortal begins to receive logs from the devices, you might experience a delay of up to 15 minutes before the aggregated data appears on the dashboard.

Organizations

The *Organizations* tab shows summary information for each organization.

The content pane lists the organization name and displays the following information per organization:

- Number of sites
- Number of devices
- Assigned reports
- Device configuration status
- ADOM versions



Organization	Sites	Devices	Assigned Reports	Device Configuration Status	ADOM Versions
Demo	1	1	0/70	1	0

Page actions

On the *Organizations* tab, the following actions are available:

- *Create*—open a dialog to add an organization. See [Create or edit an organization on page 23](#).
- *Edit*—edit selected organization.
- *Delete*—delete selected organizations.
- *Search*—enter text to search for organization names containing that text.
- *Sort*—allows you to sort data in ascending or descending order.
- *Show N entries*—filter the maximum number of organizations to display in the page.

Create or edit an organization

To create an organization:

1. Go to *Organizations* and select *Create*.
The *Create New Organization* window opens.



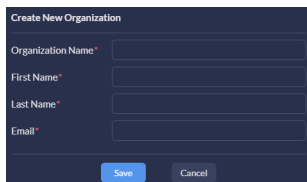
Select an organization and then select *Edit* to edit the organization.

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

2. In the *Create New Organization* window, enter the following information:

Settings	Guidelines
Organization Name	Organization business name, which must be unique within this FortiPortal
First Name	First name of the organization
Last Name	Last name of the organization
Email	Email of the organization

3. Click *Save*.



A new window opens with the following tabs:


- [General on page 23](#)
- [Contact on page 25](#)
- [Adoms on page 25](#)
- [Sites on page 26](#)
- [Users on page 27](#)
- [Authentication on page 31](#)
- [Reports on page 32](#)

General

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

To configure general settings for an organization:

1. When creating or editing an *Organization*, go to the *General* tab.
2. In the *General* tab, enter the following information:

Settings	Guidelines
Organization Name	Required. Organization business name, which must be unique within this FortiPortal.
Email	Required. Email of the organization.
First Name	Required. First name of the organization.
Last Name	Required. Last name of the organization.
Locale	<p>If you deselect <i>Use MSSP Locale</i>, you can select a language for this organization.</p> <p>When an organization user logs in to the GUI, pages will display in this language.</p> <p>For Administrative users, the system will continue to use the language set in the <i>System > Settings > General</i>.</p>
Domains	<p>Enter a domain and then hit <i>enter</i>. The new domain appears in the field.</p> <p>Use this field for the organization domain. To specify a domain for the administrator, see Authentication on page 43.</p>
 <p>When using remote authentication, a customer may have users defined in more than one domain.</p>	
Use MSSP Locale	Uses the MSSP locale (the language configured in General on page 41).
Require Pattern Validation	Select to require pattern validation.
Enable Trusted Hosts	Enable trusted hosts for this organization.
Attach Logo	<p><i>Upload</i> an image file for this organization's logo. The maximum file size is 1 MB.</p> <p>The format can be jpg, gif, bmp, or png. The maximum file dimension is 144 pixels wide by 48 pixels tall.</p>
Policy Installation Scheduler	<p>Enables you to schedule automatic policy installation at a particular time (daily or weekly).</p> <p>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.</p>

3. Click *Save*.



Use *Reset* to reset entries and selections in the tab.

Contact

The *Contact* tab contains contact related information about the organization.

To configure contact settings for an organization:

1. When creating or editing an *Organization*, go to the *Contact* tab.
2. In the *Contact* tab, enter the following information:

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

3. Click **Save**.



Use **Reset** to reset entries and selections in the tab.

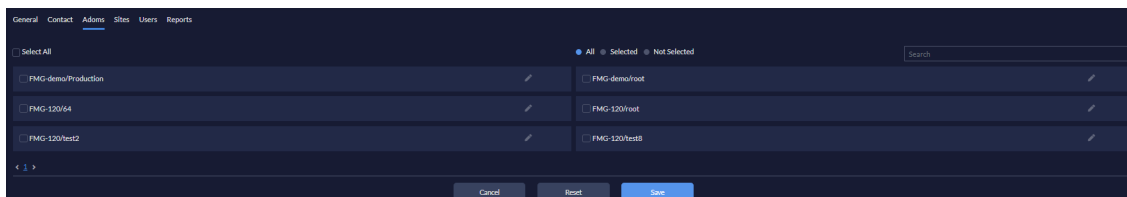
Adoms

The *Adoms* tab allows you to select the devices that are then listed for an organization in dropdown menus of devices.

See [Devices on page 33](#).

To configure ADOM settings for an organization:

1. When creating or editing an *Organization*, go to the *Adoms* tab.
2. Select the pen icon to give the device an alias for ADOM/Device/VDOM to prevent customers from knowing the MSSP configuration.
3. Click **Save**.





Use *Reset* to reset selections in the tab.

Sites

The *Sites* tab displays information about the organization sites.

For each site you can see the name, email, vdom, and APs of the site administrator.

To configure sites for an organization:

1. When creating or editing an *Organization*, go to the *Sites* tab.







Select a site and then select *Edit* to edit the site.

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

2. In the *Sites* tab, select *Create* to create a new site.
The *Create New Site* window opens.

3. In the *Create New Site* window, enter the following information:

Settings	Guidelines
Name	Required. Name for the site, which must be unique across this organization's sites.
Contact Name	Required. Name of the organization contact for this site.
Email	Required. Email of the organization contact for this site.
Phone	Required. Phone number of the organization contact for this site.
Sandbox	<p>Enable sandbox capability for all the selected devices.</p> <hr/> <div style="display: flex; align-items: center;">  <p>An extra license is required for each device that you enable with sandbox.</p> </div> <hr/>
Managed FortiGates	<p>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.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Select a device and then select the pen icon to give the device an alias for ADOM/Device/VDOM to prevent customers from knowing the configuration.</p> </div> <hr/>
Managed FortiSwitches	<p>Select the FortiSwitch devices to associate with this site. Use the search box to filter the choices available.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Select a device and then select the pen icon to give the device an alias.</p> </div> <hr/>
Managed FortiAPs	<p>Select the FortiAP devices to associate with this site. Use the search box to filter the choices available.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Select a device and then select the pen icon to give the device an alias.</p> </div> <hr/>

4. Click **Save**.



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

Users

The *Users* tab displays information about the local administrative users configured for this organization.



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

To configure users for an organization:

1. When creating or editing an *Organization*, go to the *Users* tab.
-





Select a user and then select *Edit* to edit the user.

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

2. In the *Users* tab, select *Create* to create a new user.
The *Create User* window opens.

3. In the *Create User* window, enter the following information:

Settings	Guidelines
First Name	First name of the user.
Last Name	Last name of the user.
Email	Email of the user.
Password	Password of the user. <hr/>  The password must meet the requirements set by the password policy.
Confirm Password	Confirm the entered password.
Enable Password Policy	If enabled, you can set one or more of the following types of character that the password must contain in <i>Must Contain</i> : <ul style="list-style-type: none"> • Uppercase Letters • Lowercase Letters • Numbers (0-9) • Special Characters
Minimum Length	Select the minimum number of characters that a password must contain. Note: This option is available only when the password policy option is enabled.
Contact Information	
Address 1	Enter the address of the user.
Address 2	Use this field to continue the address.
City	Enter the city name.
State	Enter the state name.
Country	Enter the country name.
Zip	Enter the ZIP code.
Phone	Enter the phone number.
Fax	Enter the fax number.
Profiles	From the dropdown, select a role. See User roles on page 30 .
Sites	From the dropdown, select sites. <hr/>  You can specify multiple sites for a user. If no site is selected, the user has access to all sites.

Settings	Guidelines
Active	Select to set the user status as active.
Enable Two-factor Authentication	Select to enable two-factor authentication.

4. Click **Save**.



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

User roles

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

Each role defines the access rights of the user to specific organization portal pages and components. Content may be hidden from the user, read-only, or read-write access.

You can assign one or more roles to a user. For example, a user with Schedule Report Write and RunNow Report Execute roles will have read-write access to the Reports page and the RunNow page, and read-only access to the remaining pages and components for that organization.

The system provides a set of default user roles. You can also create new roles or customize the default roles using the *Profiles* tab. See [Profiles on page 58](#).

There are numerous default roles, but note the following common points:

- The Customer Monitor role provides read-write access to the pages that a user requires to administer the organization portal for that organization. Because this role is far-reaching, we recommend that you assign this role to a limited number of users.
- All of the roles provide read-write access to the dashboard.
- All of the "Read" roles provide read access to all of the organization pages (except that the Run Now Report page is hidden). In addition, the role allows read-only access to the resource that the role name specifies (such as Policy, Address Object, Schedule Object).
- Each of the "Write" roles provide read-only access to the same resources as the "Read" role, except that it also allows write access to the resource that the role name specifies (such as Policy, Address Object, Schedule Object).
- The RunNow Report Execute role allows access to the RunNow page, so that the user can run reports. On the report page, the *Run Now* button is hidden for users without this role.

The following table describes the default role types that are available:

Role	Description
Customer Admin	Read-write access to the pages that an user requires to administer the organization portal for that organization
Schedule Report Read	Read access to the Report Definitions page

Role	Description
Schedule Report Write	Read access to the Report Definitions page and allows the user to add or edit an organization-defined report
Run Now Report Execute	Makes the Run Now button visible on the Reports page and enables the user to select a report and run it
Policy Read	Provides the user with read-only access to the policies
Policy Write	Provides the user with read-write access to the policies
Object Read	Provides the user with read-only access to the specified object type. Object types include: Address Object, Schedule Object, Anti Virus Object, Application Sensor Object , DLP Object, Email Filter Object, IPS Sensor Object, Web Filter Object.
Object Write	Provides the user with read-write access to the specified object type

Authentication

The *Authentication* tab allows organizations to use separate SSO authentication servers for improved security.

To configure authentication settings for an organization:

1. When creating or editing an *Organization*, go to *Authentication*.
2. In the *Authentication* tab, enter the following information:

Settings	Guidelines
Override Authentication Settings	Enable to override authentication settings set up in Authentication on page 43 . Note: This option is disabled by default.
Enable Two-factor Authentication	Enable two-factor authentication for the organization. See Enable Two-factor Authentication on page 43 .
SSO IDP Entity URL	Required. IDP Entity URL (ID) or URN for SAML provided by IDP server.
IDP Sign On Service Endpoint URL	Required. Endpoint URL for IDP (Post) provided by IDP server.
IDP Sign On Service Redirect Endpoint URL	Required. Endpoint URL for IDP (Redirect) provided by IDP server.
IDP Logout Service Endpoint	Required. IDP logout URL provided by IDP.
SSO Certificate	Required. Certificate provided by IDP used by SP to decrypt the signed response.
View/Change SSO Roles	Select to map the SSO roles with the local roles. See SSO Roles .

3. Click **Save**.



Click the *Reset* button to reset entries in the table.

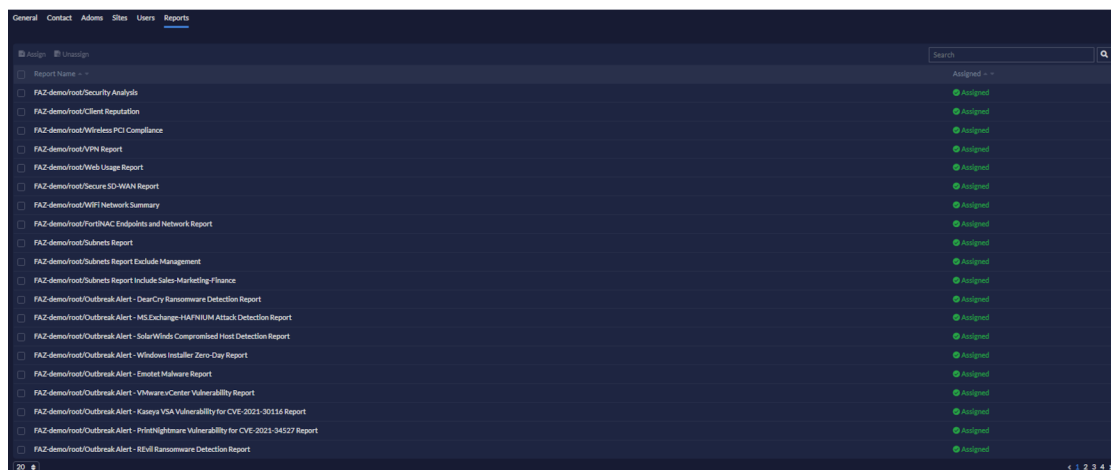
Reports

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 roles assigned to that user. For additional information, refer to [Users on page 27](#).

When you select the *Reports* tab when creating or editing an organization, the *Reports* tab displays information about the reports that are available to this organization.

FortiAnalyzer reports

The following figure shows the *Reports* tab in *Organizations*, which lists the reports that are available to download.



Page actions

The *Reports* tab contains the following actions:

- **Assign**—assigns the selected report templates to this customer who can download a PDF file of the content
- **Unassign**—unassigns the selected report templates from this customer
- **Search**—enter text to find within the list of report names
- **Select**—select one or more report (boxes) to assign or unassign to a customer
- **Show x entries**—sets the 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.

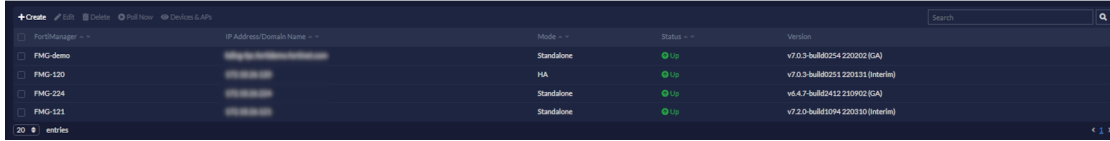
Devices

Go to *Devices* to see a list of FortiManager and FortiAnalyzer devices.

See [FortiManager devices on page 34](#) and [FortiAnalyzer devices on page 37](#).

FortiManager devices

Go to *Devices > FortiManager* to see a list of FortiManager devices and the devices that they are managing:



FortiManager	IP Address/Domain Name	Mode	Status	Version
FMG-demo	192.168.1.100	Standalone	Up	v7.0.3-build80254.220202 (GA)
FMG-120	192.168.1.101	HA	Up	v7.0.3-build80251.220131 (Interim)
FMG-224	192.168.1.102	Standalone	Up	v6.4.7-build82412.210902 (GA)
FMG-121	192.168.1.103	Standalone	Up	v7.2.0-build2094.220210 (Interim)

Page actions

In this tab, the following actions are available:

- *Create*—opens a dialog to add a FortiManager
- *Edit*—opens a dialog to edit the selected FortiManager
- *Delete*—delete selected FortiManager devices
- *Poll Now*—select to poll the FortiManager
- *Device Repo*—select to see a list of FortiGates, FortiSwitches, and FortiAPs managed by the FortiManager
- *Search*—enter text to search for FortiManager names containing that text. You can also search by IP address
- *Show x entries*—sets the number of entries that are displayed at once (20 or 50)
- *Sort*—allows you to sort columns in ascending or descending order.

Add a FortiManager

Assuming that you have already acquired the credentials for an admin user on the FortiManager (create a dedicated admin user for FortiPortal), do the following to add a FortiManager:

1. In *Devices > FortiManager*, select *Create*.
2. Input the fields, as described in the table in the next section.
See [Edit a FortiManager on page 34](#).
3. Select *Add*.

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


Edit a FortiManager

To edit the FortiManager:

1. Go to *Devices > FortiManager*.
2. Select a FortiManager device and then select *Edit*.
3. Input the fields, as described in the table below.
4. Select *Save*.

The following table contains descriptions of the fields:

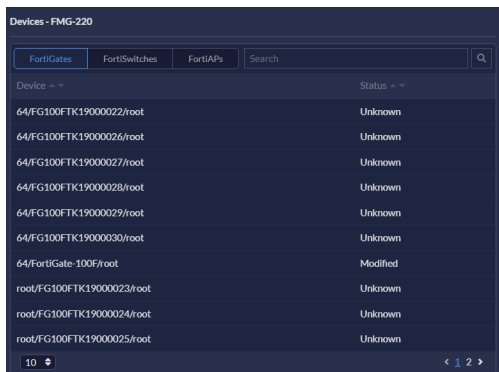
Field	Description
Name	A name for the FortiManager. The name must be unique within this FortiPortal.
Host	Enter the IP address or domain name of the FortiManager
Username	User name for a valid FortiManager administrative user
Password	Enter a password for a valid FortiManager administrative user
Confirm Password	Confirm password for the FortiManager administrative user
Port	Port number to use to connect with the FortiManager. The default for is 443.
XML Port	Port number to use to connect with the FortiManager. The default for XML is 8080.
Polling Frequency	How frequent the FortiPortal will poll the FortiManager to update the devices information.



If you set the frequency to **No Polling**, the FortiPortal will never poll the FortiManager. Valid values include *Daily*, *Weekly*, or *Monthly*.

Manage FortiGate, FortiSwitch, and FortiAP devices

Selecting a *FortiManager* device and then selecting *Device Repo* displays a list of the FortiGate, FortiSwitch, and FortiAP devices managed by the FortiManager.



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

For each FortiManager device, the system displays the following:

- *Device*—name of the managed FortiGate device
Note: This option is only available when *FortiGates* is selected.
- *Switch*—name of the managed FortiSwitch device
Note: This option is only available when *FortiSwitches* is selected.
- *Access Point*—name of the managed FortiAP device
Note: This option is only available when *FortiAPs* is selected.
- *Status*—status of the FortiGate device
Note: This option is only available when *FortiGates* is selected.

-
- *From Devices*—FortiAP and FortiSwitch devices from the FortiGate device

Note: This option is only available when *FortiAPs* or *FortiSwitches* is selected.



FortiPortal can add FortiGate devices configured in the Fortinet Security Fabric.

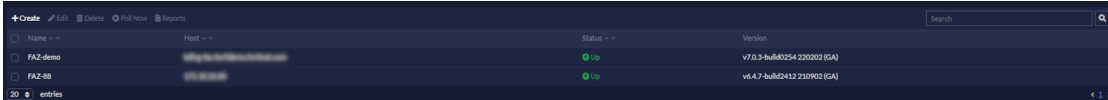
FortiGate devices added from the Security Fabric can be identified by the * sign next to the Security Fabric root, and the name of the Security Fabric it belongs to is also displayed.

FortiAnalyzer devices

Go to *Devices > FortiAnalyzer* to see a list of FortiAnalyzer devices.

When you add a FortiAnalyzer device to the FortiPortal, you make the reports on that FortiAnalyzer available to organizations. Refer to [Reports on page 32](#).

The list displays the FortiAnalyzer name, the IP address, the status, and the version for each FortiAnalyzer:



Name	Host	Status	Version
FAZ-demo	192.168.1.100	Up	v7.0.2-build0254.220202 (GA)
FAZ-08	192.168.1.101	Up	v6.4.7-build02412.210902 (GA)

Prerequisites

Before you add a FortiAnalyzer device, use the FortiAnalyzer CLI to set the following configuration values:

1. 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 the FortiPortal>
    set rpc-permit read-write
```

2. Set port1 (assuming it is connected to the FortiPortal) to allow web service access.

- Go to *System Settings > Network*. The System Network Management Interface pane displays.
- For *Administrative Access*, select the *Web Service* check box.

```
config system interface
  edit port1
    set allowaccess https http ping telnet snmp webservice
      aggregator fortimanager
```

Page actions

In this tab, the following actions are available:

- *Create*—opens a dialog to add a FortiAnalyzer device.



To use FortiAnalyzer mode, you must be running FortiAnalyzer 6.0 or later

-
- *Edit*—opens a dialog to edit the selected FortiAnalyzer
 - *Delete*—delete selected FortiAnalyzer devices
 - *Poll Now*—polls the selected FortiAnalyzer to obtain the most recent data
 - *Reports*—displays a list of FortiAnalyzer reports for the selected FortiAnalyzer device
 - *Search*—enter text to search with FortiAnalyzer names


- *Show x entries*—sets the number of entries that are displayed at once (20 or 50)
- *Sort*—allows you to sort columns in ascending or descending order.

Edit a FortiAnalyzer

To edit the FortiAnalyzer:

1. Go to *Devices > FortiAnalyzer*.
2. Select a FortiAnalyzer device and then select *Edit*.
3. Change the fields as needed; see the field descriptions in the table.
4. Select *Save*.

The following table contains descriptions of the fields:

Settings	Guidelines
Name	Name for the FortiAnalyzer. The combination of FortiAnalyzer name and VDOM must be unique within this FortiPortal.
Host	Enter the IP address or domain name of the FortiAnalyzer.
Username	User name for the FortiAnalyzer user assigned to this FortiPortal.
Password	Password for the FortiAnalyzer user assigned to this FortiPortal.
Confirm Password	Confirm password for the FortiAnalyzer user assigned to this FortiPortal.
Port	Port number to use to connect with the FortiAnalyzer. The default port is 443.
polling	How often the FortiPortal will poll FortiAnalyzer to update the device information.
	 <p>The default value is daily. The polling frequency is not configurable.</p>

View FortiAnalyzer reports

When you select the *Reports* for a selected FortiAnalyzer in the list, FortiPortal opens a new pane with the reports.

The pane displays reports listed by ADOM.

Reports - FAZ-demo

Search

adom	Name
FortiCache	FortiCache Default Report
FortiCache	FortiCache Web Usage Report
FortiCache	FortiCache Security Analysis
FortiCarrier	Security Analysis
FortiCarrier	Client Reputation
FortiCarrier	Wireless PCI Compliance
FortiCarrier	VPN Report
FortiCarrier	Web Usage Report
FortiCarrier	WiFi Network Summary
FortiCarrier	User Security Analysis

10 < 1 2 3 4 5 6 ... 13 14 >

System

Go to *System* to access the following:

- [Settings on page 41](#)
- [Profiles on page 58](#)
- [Admins on page 59](#)
- [Theme on page 62](#)
- [Additional Resources on page 90](#)

Settings

Go to *System > Settings* to change the administrative settings for FortiPortal.

Settings contains the following tabs:

- [General on page 41](#)
- [Authentication on page 43](#)
- [Blocked Hosts on page 55](#)
- [Configuring a scalable cluster on page 56](#)
- [Email on page 58](#)




General

In the *General* tab, you can configure the general administrative settings for FortiPortal.

To configure general settings:

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

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

Settings	Guidelines
Session Timeout	Required. Timeout for user sessions on the Administrative or Organizational web interfaces, in minutes (15 - 3240, default = 30).
Language	Desired language (default = English).
	 <p>If you change the language, save the settings and log out. The change takes effect upon subsequent logins.</p>
Time Zone	Select the appropriate time zone to use.
Enable Blocked Host	Select to enable blocked hosts. When enabled, the system provides a blocklist, for blocking rogue log-in attempts. See Blocked Hosts on page 55 .
Certificate Information	
Certificate	Upload a new certificate for FortiPortal.
Private Key	Upload a new private key for FortiPortal.
	 <p>The <i>Private Key</i> is in PKCS#8 format.</p>
Upload License	
License	See Upload a license on page 42 .
	 <p>The system automatically restarts the FortiPortal VM to apply the license.</p>
System	
System Logs	Select 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, 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 as “used” 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.

In case you have no license, three free devices are allowed. Once the grace period expires, the service provider and the end-customer interfaces are not accessible anymore.






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 related settings for FortiPortal.

To configure authentication settings:

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

Settings	Guidelines
Authentication Access	<p>Select <i>Local</i> or <i>Remote</i>.</p> <hr/> <p> By default, <i>Authentication Access</i> is set as <i>Local</i>.</p> <hr/> <p> When you change the authentication configuration from local to remote or from remote to local, you must restart FortiPortal.</p> <hr/> <p>See Authentication Access on page 47.</p>
Enable Two-factor Authentication	<p>Enable two-factor authentication for local or remote users.</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>

Settings

Guidelines



Email information is mandatory for 2FA users.
It is recommended that 2FA users use email as the user name.



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

See [2FA in FortiPortal example on page 54](#).

Allow Service Provider
Usernames without Domain

Enable allowing SP usernames without a domain.
If you enable this field, the user can enter their user ID without a domain qualifier, and the system will try to authenticate the user credentials in each of the domains until a match is found.

Note: This option is available only when *Authentication Access* is set as *Remote*.

Remote Server

Required. Select *FortiAuthenticator*, *RADIUS*, or *SSO* as the remote server.

Note: This option is available only when *Authentication Access* is set as *Remote*.

Remote Server Port

Required.

Port for the authentication server (default is 443)

Note: This option is available only when *Authentication Access* is set as *Remote* and *Remote Server* is *FortiAuthenticator* or *RADIUS*.

Remote Server IP Address

Required. Enter the IP address of the authentication server.

Note: This option is available only when *Authentication Access* is set as *Remote* and *Remote Server* is *FortiAuthenticator* or *RADIUS*.

Remote Server Key

Required. Secret key for REST API requests.

Note: This option is available only when *Authentication Access* is set as *Remote* and *Remote Server* is *FortiAuthenticator* or *RADIUS*.

Domains

Enter a domain, URL, or URN attribute and then hit *enter*. The new domain appears in the list below the entry box. If you do not want to provide a domain for the site administrator, enable *Allow Service Provider Usernames without Domain*.

Use this field to specify the domain, URL, or URN for the site administrator. To specify the domain for an organization, see [General on page 23](#).



The site administrator may allow administrative users to be defined in more than one authentication domain.

Settings	Guidelines
	Note: This option is available only when <i>Authentication Access</i> is set as <i>Remote</i> .
Remote Server User	Required. Administrator user name for the authentication server. This user must have sufficient permission to initiate REST API requests. Note: 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	Required. Select <i>CHAP</i> or <i>PAP</i> authentication protocols. Note: 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	Select to map the RADIUS roles with local roles. See Radius Roles on page 47 . Note: 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	Required. IDP Entity URL (ID) or URN for SAML provided by IDP server. Note: 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	Required. Endpoint URL for IDP (Post) provided by IDP server. Note: 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	Required. Endpoint URL for IDP (Redirect) provided by IDP server. Note: 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	Required. SSO application provided by IDP. Note: 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	Required. URL used for audience within assertion (format: <code>https://<FPC_PORTAL> /fpc/saml/SSO</code>). Note: 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	Required. Attribute parameter name that maps to the corresponding role in FortiPortal. Note: 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	Introduced with FortiPortal Version 3.2.1, this attribute specifies a 'string' value that FortiPortal uses under SSO to map a user to a specific customer. This feature works similar to the Tenant Identification Attribute in RADIUS, except that in SSO, FortiPortal allows you to configure the name of the attribute on the Administration Settings page.

Settings

Guidelines

If you configure "My Customer Id" as the attribute value, FortiPortal expects the following in the authentication response from the SSO server:

```
<My Customer Id>Fortinet</My Customer Id>
```

where Fortinet is the value returned by the SSO server.

This value must have been supplied to *Domains* in the [General on page 23](#).

For a RADIUS server, the Tenant Identification Attribute value is a Fortinet Vendor Attribute value. The server will send "Fortinet" in the authentication response.



FortiPortal treats the attribute values from either RADIUS or SSO server equally.

Note: This option is available only when *Authentication Access* is set as *Remote* and *Remote Server* is *SSO*.

SSO Error URL

(Optional) Error URL provided by IDP.

Note: This option is available only when *Authentication Access* is set as *Remote* and *Remote Server* is *SSO*.

IDP Logout Service Endpoint

Required. IDP logout URL provided by IDP.

Note: This option is available only when *Authentication Access* is set as *Remote* and *Remote Server* is *SSO*.

SSO Certificate

Required. Certificate provided by IDP used by SP to decrypt the signed response.

Note: This option is available only when *Authentication Access* is set as *Remote* and *Remote Server* is *SSO*.

Site Attribute

Attribute parameter name that specifies which sites the customer user can access.

When the *Remote Server* is *SSO*, enter the site attribute.

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".

```
<saml:Attribute Name="site"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">site1</saml:AttributeValue>
  <saml:AttributeValue xsi:type="xs:string">site2</saml:AttributeValue>
</saml:Attribute>
```

When the *Remote Server* is *FortiAuthenticator* or *Radius*, select a site attribute from the dropdown. By default, `Fortinet-Fpc-Tenant-user-sites` is available.

You can select a different value if you define an attribute for a site on the *FortiAuthenticator-side* or the *RADIUS* server.

Settings	Guidelines
	<p>Note: If the <i>Site Attribute</i> is empty, the customer user is assigned all the sites owned by the organization.</p> <p>Note: This option is available only when <i>Authentication Access</i> is set as <i>Remote</i>.</p>
Email Attribute	<p>The user-defined email attribute name.</p> <p>Note: 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>
View/Change SSO Roles	<p>Select to map the SSO roles with the local roles. See SSO Roles on page 48.</p> <p>Note: 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>

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 or FortiAuthenticator user database. Local customer users *cannot* be used when remote authentication is selected.

See [Remote authentication using FortiAuthenticator on page 49](#), [RADIUS server configuration on page 50](#), and [Remote authentication - SSO on page 51](#).

Radius Roles

Selecting *View Radius Roles* on the *Authentication* tab displays the *Radius Roles* window. Here, you can configure the mapping between FortiPortal roles and RADIUS roles. For each RADIUS role, 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.

The *Radius Roles* window contains the following options:

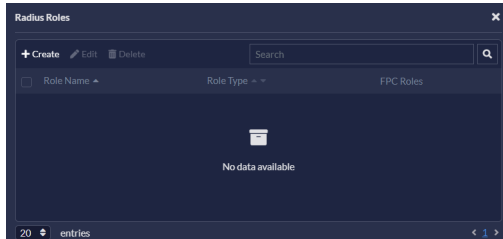
- *Create*—open a dialog to create a RADIUS role.
- *Edit*—edit a selected RADIUS role.
- *Delete*—delete a selected RADIUS role.
- *Search*—enter text to search for RADIUS role names containing that text.
- *Show x entries*—sets the number of entries that are displayed at once (20 or 50).
- *Sort*—allows you to sort columns in ascending or descending order.

To create a Radius Role:

1. Go to *System > Settings > Authentication*.
2. In *Authentication Access*, select *Remote*.
3. In the *Remote Server* dropdown, select *Radius*.

4. Select *View/Change Radius Roles*.

The *Radius Roles* window opens.



5. In the *Radius Roles* window, select *Create*.

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

Settings	Guidelines
Role Name	The RADIUS role name. The name must match a role name in the RADIUS server.
Role Type	<i>Service Provider</i> or <i>Customer</i> .
FPC Roles	Select the FortiPortal roles to associate with this RADIUS role.

7. Click *Save*.

SSO Roles

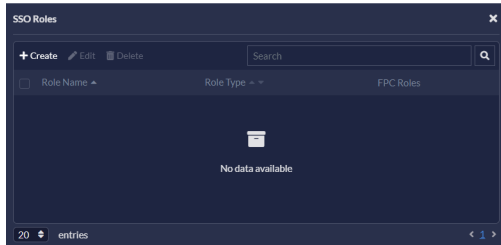
Selecting the *View SSO Roles* button on the *Authentication* tab displays the *SSO Roles* window. Here, you can configure the mapping between FortiPortal roles and SSO roles. For each SSO role, the window displays *Role Name*, *Role Type* (*Service Provider* or *Customer*) and a list of *FPC* (FortiPortal) roles that map to the SSO role.

The *SSO Roles* window contains the following actions:

- *Create*—open a dialog to add an SSO role.
- *Edit*—edit a selected SSO role.
- *Delete*—delete a selected SSO role.
- *Search*—enter text to search for SSO role names containing that text.
- *Show x entries*—sets the number of entries that are displayed at once (20 or 50).
- *Sort*—allows you to sort columns in ascending or descending order.

To create an SSO Role:

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

Settings	Guidelines
Role Name	The SSO role name. The name must match a role name in the SSO server.
Role Type	<i>Service Provider</i> or <i>Customer</i> .
FPC Roles	Select the FortiPortal roles to associate with this SSO role.

7. Click *Save*.

Remote authentication using 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*.

Change local user

Username: admin

Disabled
 Password-based authentication [\[Change Password\]](#)
 Token-based authentication
 Allow RADIUS authentication
 Force password change on next logon

User Role

Role:
 Administrator
 Sponsor
 User

Full permission
 Web service access
 Restrict admin login from trusted management subnets only

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

Configuring FortiPortal

When you select *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 REST API key you received in email. See step 3 in [To configure FortiAuthenticator](#).
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 admin user from step 1 in [To configure FortiAuthenticator](#).
9. Click *Save*.

RADIUS server configuration

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:

```
#
# Fortinet's VSAs
#

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



If you want to use two-factor authentication, select the *Remote* authentication access and SSO and configure two-factor authentication on the SAML IDP server.

For SSO, FortiPortal supports Service Provider-initiated or Identity Provider-initiated SAML authentication.

For troubleshooting SSO configuration, FortiPortal provides the following URL for the SPUSER to authenticate locally (even if the system is configured for SSO remote authentication):

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

SSO - example

Here is an example of setting up the *Tenant Identification Attribute* for a company named Local.com that will be using SSO remote authentication:

1. Set up the *Tenant Identification Attribute* on the SSO server. For example, set the Tenant Identification name to `FPC_Tenant` and set the *Tenant Identification Value* to `Local.com`
2. In FortiPortal, go to *System > Settings > Authentication*.
3. Select *Remote for Authentication Access* and *SSO for Remote Server*.
4. In *Tenant Identification Attribute*, enter `FPC_Tenant`.
5. Fill out the rest of the fields and select *Save*.
6. Go to *Organizations* and select *Create*.

7. In the *General* tab, for *Domains*, enter `Local.com` and press *enter*.
8. Fill out the rest of the fields as shown in [Create or edit an organization on page 23](#) and click *Save*.

Frequently asked questions (FAQs) about SSO configuration

How can I map the role (permission) for the IDP server user to the FortiPortal roles (permission)?

To map SSO roles to FortiPortal roles:

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 an FPC role to associate with this SSO role.
8. Click *Save*.

How can role mapping help maintain secure access to the system?

The site administrator can create different roles on FortiPortal by going to *System > Profiles* and selecting *Create*.

The administrator can create a read-only role or a read-write role for a specific UI page or for a specific action. After a role is created, the role can be associated with an existing role on the IDP server. When users are authenticated, the role coming from the IDP server is mapped to a role in FortiPortal and the appropriate permissions are provided to the user.

The advantage of using this mapping is that the site administrator does not need to change anything on the IDP server exclusively for FortiPortal.

How can I create custom roles (permission groups) on the FortiPortal unit?

The FortiPortal unit allows the administrative user to create different permission groups so that users can be mapped with appropriate permissions. For example, the administrative user (spuser) can create a read-only permission group and a read-write permission group for different UI objects. These permission groups are created for the administrator level, as well as the organization level.

These permission groups can be created from the UI by going to *System > Profiles*.

What is the Tenant Identification Attribute field for?

The FortiPortal unit has a multitenancy feature. This feature helps different types of users to access the system. Site administrators are typically administrators of the system; by using roles/permission groups, these users can have a different type of access. Other types of users are organization users.

During authentication, the FortiPortal unit needs to identify whether each user is an administrator or an organization so that the correct user interface is loaded. The FortiPortal uses the user domain name to identify which interface should be loaded. For example, if the user name in the IDP response is `abc@domain.com`, the system extracts `domain.com` from the user name field and checks if this domain is mapped to an organization or an administrator. Based on that mapping, the system displays the correct UI.

If the *Tenant Identification Attribute* is configured in *System > Settings > Authentication* and is provided in the SAML assertion, the value in the *Tenant Identification Attribute* is used to match the domain name provided in the MSSP settings or in [General on page 23](#). If the domain provided does not match any MSSP or organization domains, an error message is displayed.

If the *Tenant Identification Attribute* is not configured in *System > Settings > Authentication* or is not provided in the SAML assertion, the domain name is taken from the username attribute.

When there is no domain name in the uid attribute, the system requires a value in *Tenant Identification Attribute*.

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

The *Tenant ID Attribute* value is processed from the IDP response, and the value is mapped with the domain name field in the FortiPortal unit. For example, if tenant ID is `map_id`, FortiPortal gets the respective value for the `map_id` attribute from the SAML response and maps that value with the domain name listed in [General on page 23](#) or the *System > Settings > Authentication*. If the value matches with the organization domain name, the user is granted access to the organization. If the value matches with the domain name in the *System > Settings > Authentication*, FortiPortal loads the administrator UI.

How can I add a domain name to the organization?

A unique domain name identifies the organization. You can add the domain name to the organization when configuring [General on page 23](#).

In the [General on page 23](#) tab in [Create or edit an organization on page 23](#), there is the *Domains* field. Enter the domain name and hit *enter* to add the name to the domain list.

The administrator can add more than one domain to an organization.

How can I add a domain name for a server provider?

After you select *SSO/FortiAuthenticator/RADIUS* as a remote server in the [Authentication on page 43](#) tab, you will see an option for the domain field.

2FA 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.

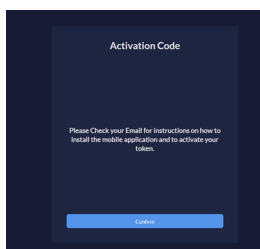


Email information is mandatory for 2FA users.
It is recommended that 2FA users use email as the username.

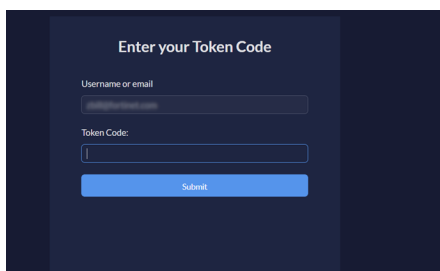


If the username is the email and no *Tenant Identification Attribute* is set, the domain part of the email can be used for tenant identification.

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 admin or 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 43](#).

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.

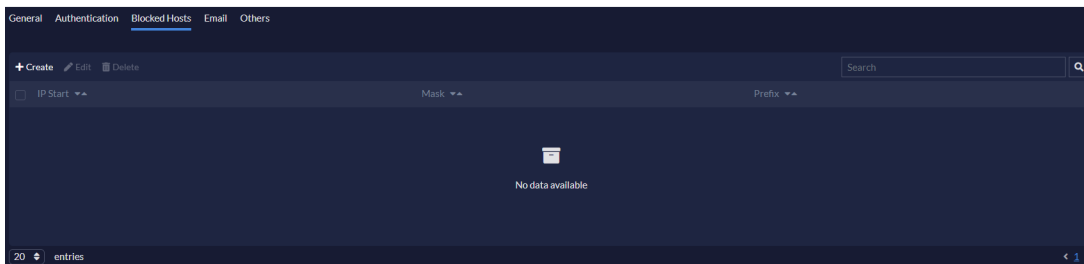
FortiAuthenticator users

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 41](#), 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 select *Edit* to edit the blocked host.
When editing a blocked host, the fields are same as those that appear when creating a blocked host.

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

3. In the *Create Blocked Hosts* window, enter the following:

Settings	Guidelines
IPv4	
IP Start	Enter the start address for the range covered by this entry.
Mask	Define the range of IP addresses covered by this entry.
IPv6	
IP Start	Enter the start address for the range covered by this entry.
Mask	Define the range of IP addresses covered by this entry.

4. Click *Save*.



To delete blocked hosts, select blocked hosts and then select *Delete*.

Configuring a scalable cluster



Use this feature only if you are certain that a FortiPortal 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.

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.

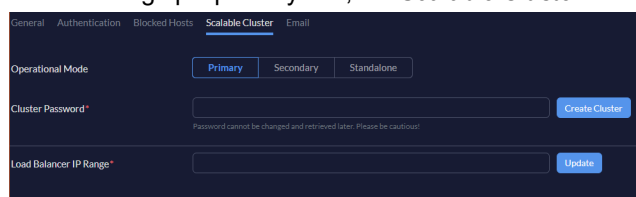
The following roles are available:

- *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.
- *Primary*: The FortiPortal is the primary in a high-availability cluster.
- *Secondary*: The FortiPortal is a secondary in a high-availability 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, the options 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, the options should be updated in the primary unit before setting up a cluster.
2. Set up the primary instance.
 - a. Log in to the primary FortiPortal instance.
 - b. Go to *System > Settings > Scalable Cluster*.

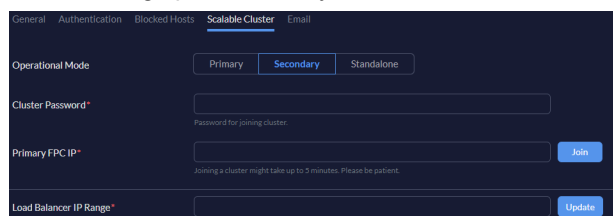
When setting up a primary unit, the *Scalable Cluster* tab looks like the following:



The screenshot shows the 'Scalable Cluster' configuration page for a primary unit. It features a dark blue background with white text. At the top, there are tabs for 'General', 'Authentication', 'Blocked Hosts', 'Scalable Cluster', and 'Email'. The 'Scalable Cluster' tab is active. Below the tabs, there are three radio buttons for 'Operational Mode': 'Primary' (selected), 'Secondary', and 'Standalone'. There is a 'Cluster Password*' field with a 'Create Cluster' button. A note below the password field states: 'Password cannot be changed and retrieved later. Please be cautious.' There is also a 'Load Balancer IP Range*' field with an 'Update' button.

- 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*.

When setting up a secondary unit, the *Scalable Cluster* tab looks like the following:



The screenshot shows the 'Scalable Cluster' configuration page for a secondary unit. It features a dark blue background with white text. At the top, there are tabs for 'General', 'Authentication', 'Blocked Hosts', 'Scalable Cluster', and 'Email'. The 'Scalable Cluster' tab is active. Below the tabs, there are three radio buttons for 'Operational Mode': 'Primary', 'Secondary' (selected), and 'Standalone'. There is a 'Cluster Password*' field. A note below the password field states: 'Password for joining cluster.' There is also a 'Primary FPC IP*' field with a 'Join' button. A note below the IP field states: 'Joining a cluster might take up to 5 minutes. Please be patient.' There is also a 'Load Balancer IP Range*' field with an 'Update' button.

- 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. Click *Join*.
 - g. 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

In the *Email* tab, you can configure the email related settings for FortiPortal.

To configure Email related settings:

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

Settings	Guidelines
SMTP Server	Required. URL of the SMTP server from which FortiPortal sends emails.
Port	Required. Email server port. The default value is 25.
Email From	Required. Email address. Emails sent from FortiPortal will originate from this address.
Enable Authentication	Enable 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	Enable validating the mail server certificate. This option is enabled by default.

3. Click **Save**.

Profiles

Go to *System > Profiles* to see the profile information (type and permissions) for each FortiPortal profile:

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

Page actions

The *Profile* tab contains the following actions:

- *Create*—open a dialog to add a profile
- *Edit*—edit the selected profile
- *Delete*—delete the selected profiles

- *Search*—enter text to search for profile names containing that text
- *Show x entries*—sets the number of entries that are displayed at once (20 or 50)
- *Sort*—allows you to sort columns in ascending or descending order.

Create a profile

To create a profile:

1. Go to *System > Profiles* and select *Create*. The *Create Profile* tab opens.

2. In the *Create Profile* window, enter the following information:

Settings	Guidelines
Name	Name for the role, which must be unique for this organization.
Profile Type	<i>Provider</i> or <i>Customer</i> .
Access Permissions	Select <i>None</i> , <i>Read</i> , <i>Read/Write</i> , or <i>Custom</i> FortiPortal permissions for this profile.

3. Click *Save*.

Admins

Go to *System > Admin* to see the list of FortiPortal administrators.

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

First Name	Last Name	Email	Status	Role
SP	User	spuser	Active	Admin
Tech	Doc	techdoc@fortinet.com	Active	Admin

Page actions

The *Admin* tab contains the following actions:

- *Create*—open a dialog to add an admin
- *Edit*—edit the selected admin
- *Delete*—delete the selected admin
- *Search*—enter text to search for admin names containing that text
- *Show x entries*—sets the number of entries that are displayed at once (20 or 50)
- *Sort*—allows you to sort columns in ascending or descending order.




You cannot delete the default admin user.

Create an admin

To create a user:

1. Go to *System > Admin* and select *Create* to create an admin.
The *Create Admin* dialog opens.

2. In the *Create Admin* window, enter the following information:

Settings	Guidelines
First Name	First name of the administrator.
Last Name	Last name of the administrator.
Email	Email of the administrator.
Password	<p>Password of the administrator.</p> <hr/> <div style="display: flex; align-items: center;">  <p>The password must meet the requirements set by the password policy.</p> </div> <hr/>
Confirm Password	Confirm the entered password.
Enable Password Policy	<p>If enabled, you can set one or more of the following types of character that the password must contain in <i>Must Contain</i>:</p> <ul style="list-style-type: none"> • Uppercase Letters • Lowercase Letters • Numbers (0-9) • Special Characters
Minimum Length	<p>Select the minimum number of characters that a password must contain.</p> <p>Note: This option is only available when <i>Enable Password Policy</i> is selected.</p>
Contact Information	
Address 1	Enter the address of the admin.
Address 2	Use this field to continue the address.
City	Enter the city name.
State	Enter the state name.
Country	From the dropdown, select a country.
Zip	Enter the ZIP code.
Phone	Enter the phone number.
Fax	Enter the fax number.
Profile	From the dropdown, select a profile. See Admin user roles on page 62 .
Active	Select to set the administrator user status as active.
Enable Two-factor Authentication	Select to enable two-factor authentication.

3. Click **Save**.

Admin user roles

The purpose of roles is to authorize each user to view and modify only the content that is required for that user. For example, a system administrator requires write access to the pages required for FortiPortal configuration, but does not need write access to the organization information.

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

You can assign one or more roles to a user. For example, a user with Sys Admin and FortiPortal Admin roles is a “Super Admin,” with read-write access to all administrator pages and all organization portal pages.

The system provides a set of default administrative roles. Using the FortiPortal Roles user interface, you can also create new roles or customize the default roles.

The following table describes the default roles for administrative users:

Settings	Guidelines
FPC Admin	The FortiPortal Admin role provides read-write access to all of the FortiPortal pages, but with read-only access to administrator settings, system log, and themes. The FortiPortal Admin role also provides read-write access to the organization portal.
System Admin	The System Admin role provides read-only access to all of the FortiPortal pages. In addition, this role provides read-write access to the administrator settings, system log, and themes. The organization portal is hidden for the Sys Admin role.
Admin Monitor	The System Admin role provides read-only access to all of the FortiPortal admin portal and the organization portal.

Theme

FortiPortal provides a default UI theme that is applied to the Administrative Web Interface and the Organization Portal Interface. The *Theme* tab provides configuration fields that allow you to customize this theme. Configuration changes apply to both user interfaces (Administrative and Organization portal).

Customer theme options

You can configure customizations such as:

- Select a predefined color scheme. There are two predefined color schemes: *Dark* and *Light*.
- Create a custom color scheme using *Color Picker*.
- Define custom URLs and text fields.
 - URLs such as contact information and privacy policy.
 - Custom text for your company name, service name, and service description.
- Set up legal disclaimers.
- Upload custom images.
 - Images for the login page and page banner.



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

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.

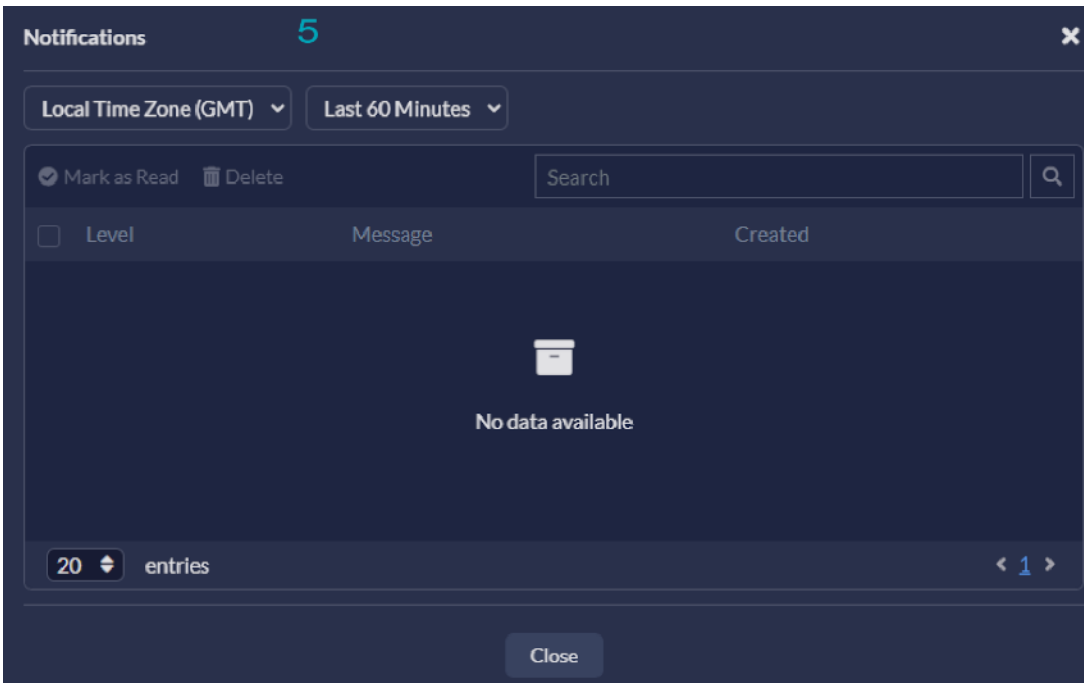
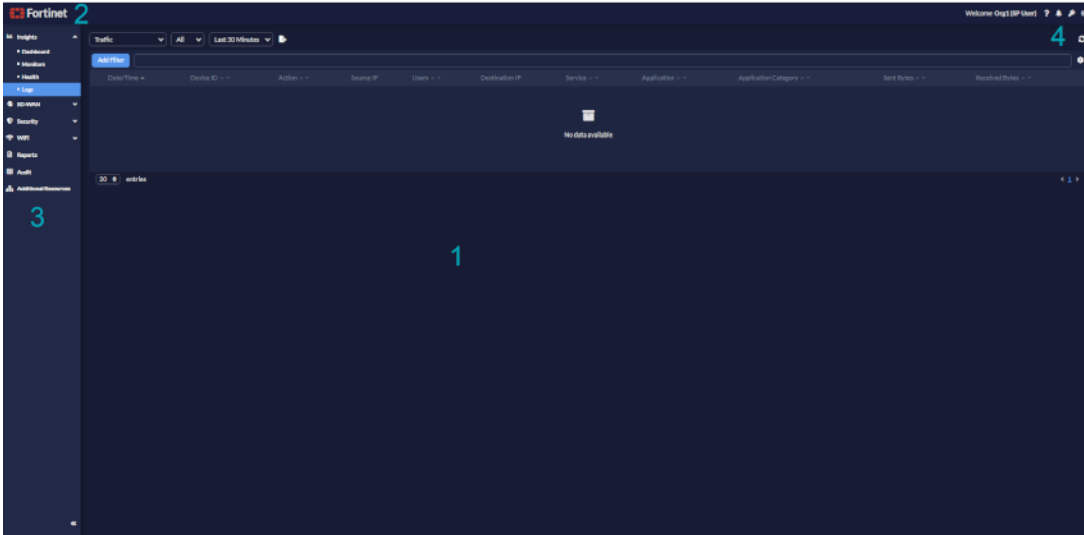


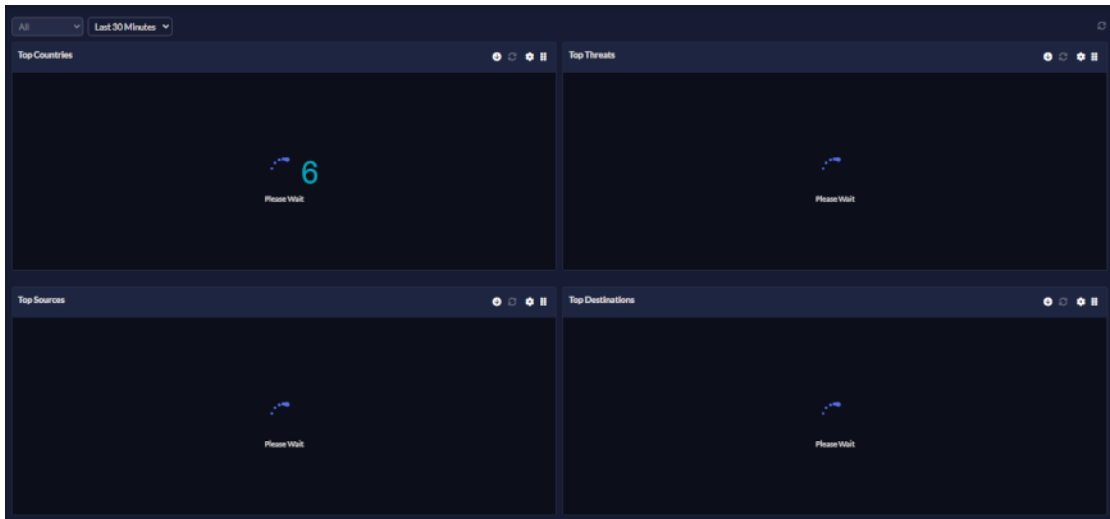
4. Edit the color scheme as needed. See [Color scheme options on page 67](#).
5. Click Save.



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.

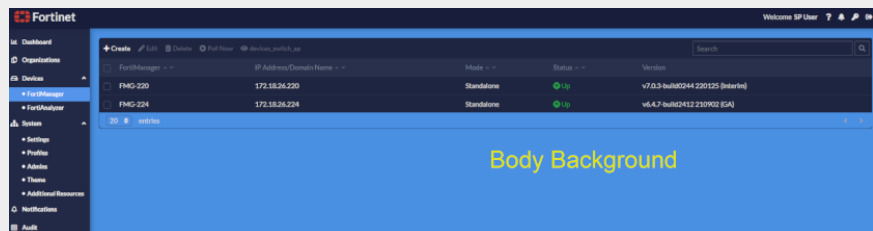
Color scheme options

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.

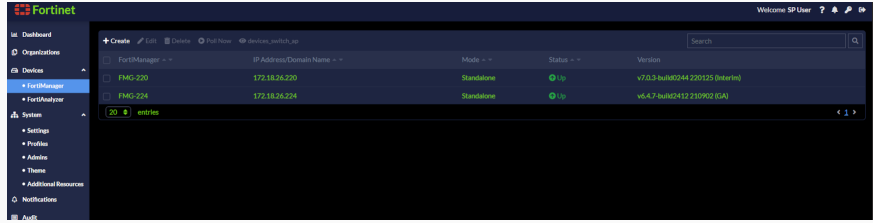
Body Background

The body background color of FortiPortal.



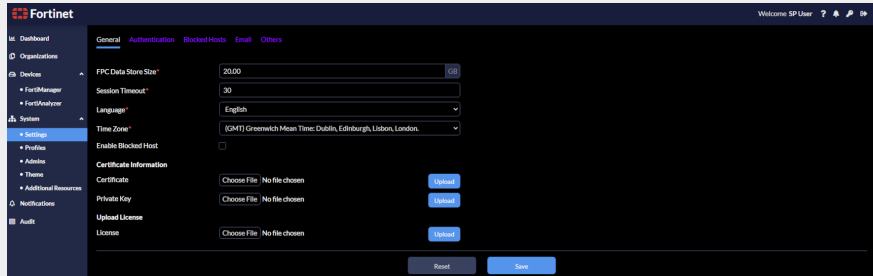
Font Color

Font color for the content pane and the page header.



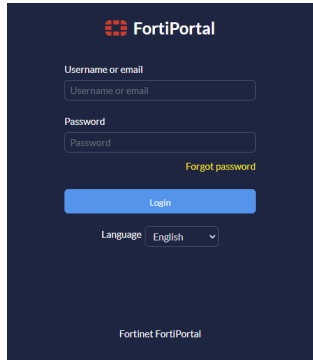
Font Link Color

Font color for sub-menus.



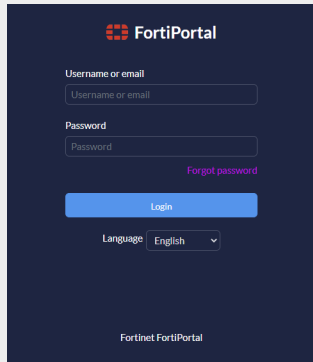
Link

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



Link Hover

The link color when hovering.

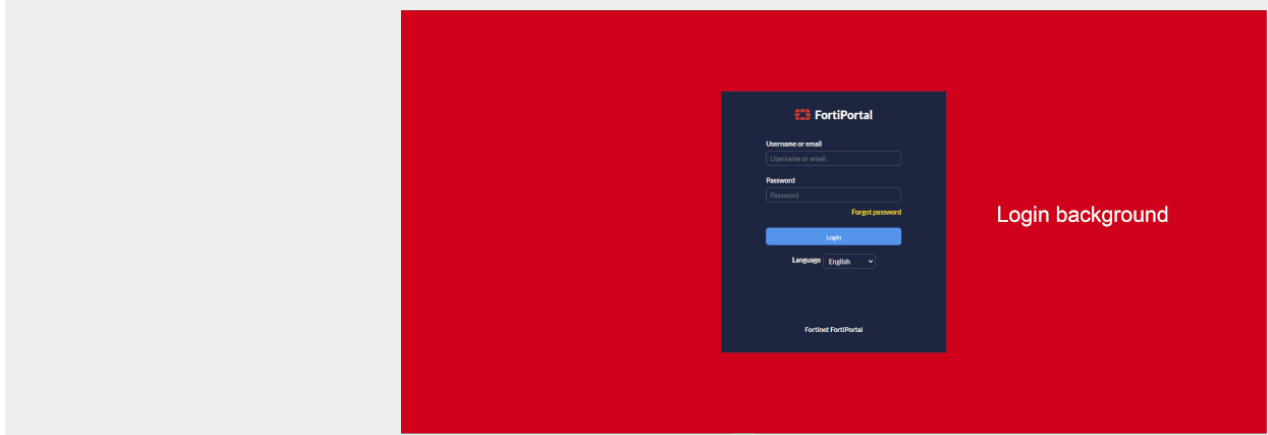


Link Disabled

Disabled link color.

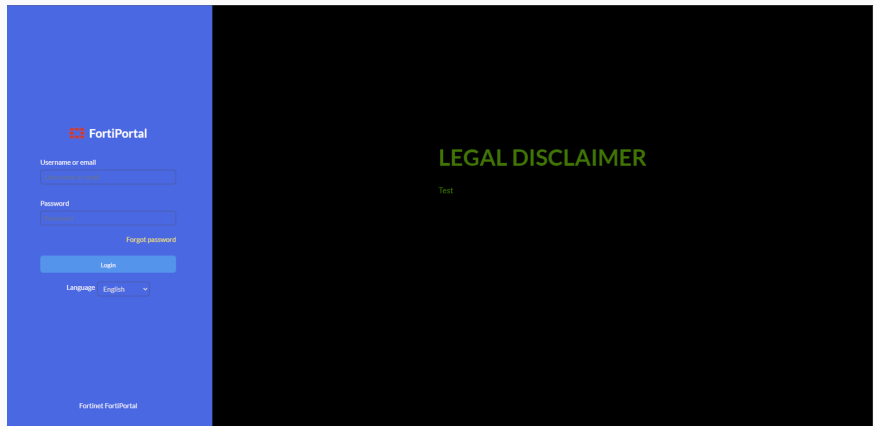
Login Background

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*

XML Port*

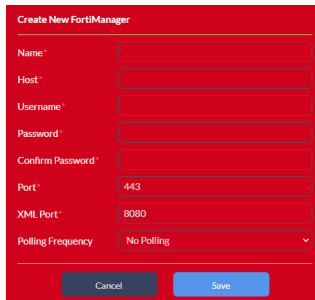
Polling Frequency

Notification Unread Background The background color of unread messages.

Summary Background The background color of the column names.

#	Name	From	To	Source	Destination	Schedule	Service	Action	Security Profile	NAT
1	test179	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	g-default	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	g-with-default	Enabled
7	win test 0602222 2 update!!!	H52 fortlink	any	all	all	always	ALL	Accept	no-inspection	Disabled
8	win test 063	win 0603	any	all	all	always	ALL	Deny		
9	win test123	any	any	all	all	always	ALL	Deny		
10	win test12317770	any	any	all	all	always	ALL	Deny		

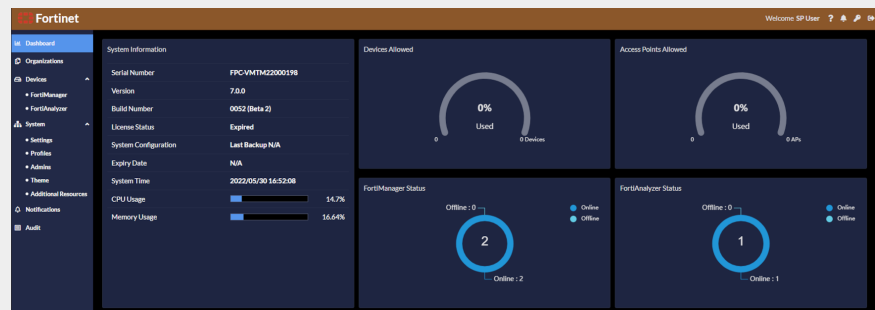
4. **Modal:** The background color of the dialog that displays.



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

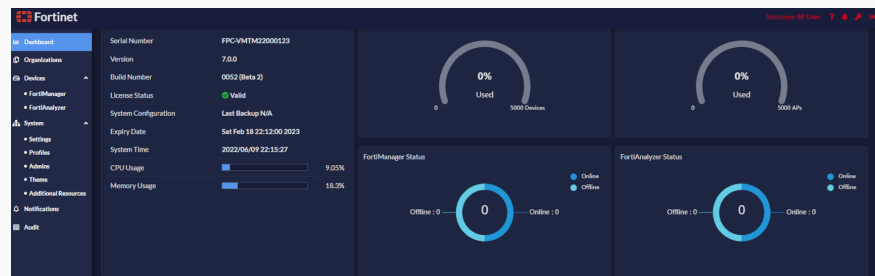
Header Background

The color of the header background.



Header Text

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



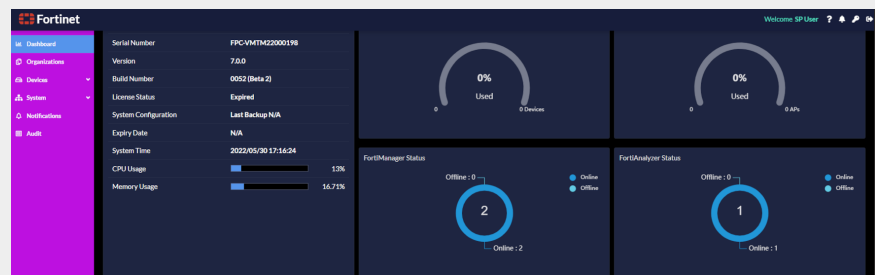
Footer Background

The color of the footer background.

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

Background

The menu background color.



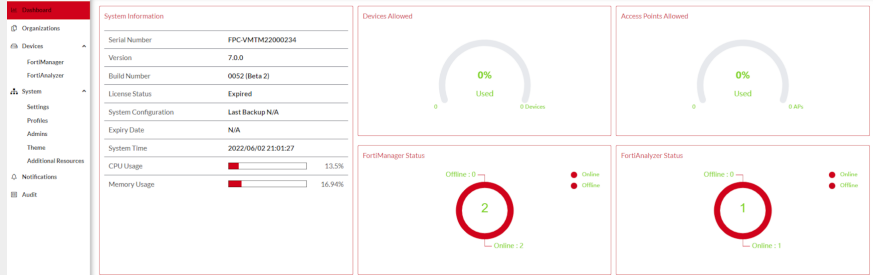
Active Background

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



Font Color

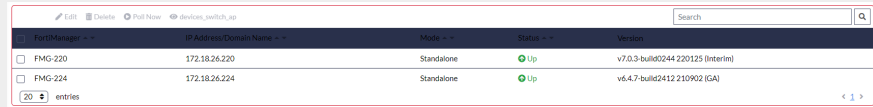
The color of the font for the menu items on the left.



7. Table: Table related colors.

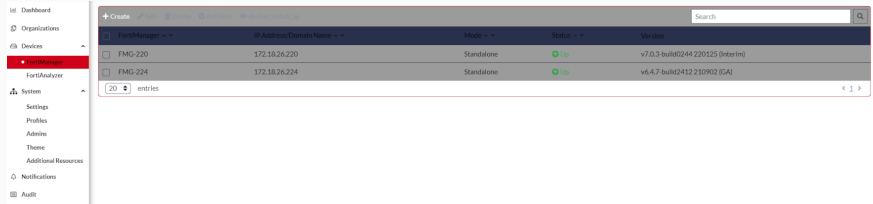
Border

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.

Organization	Sites	Devices	Assigned Reports	Device Configuration Status	ADOM Versions
test1	0	0	0/0	0 ● 0 ● 0	
test2	0	0	0/0	0 ● 0 ● 0	

Row Checked Text

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

FortiManager	IP Address/Domain Name	Mode	Status	Version
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
FMG-220	172.18.26.220	Standalone	Up	v7.0.3-build0244.220125 (Interim)
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
FMG-220	172.18.26.220	Standalone	Up	v7.0.3-build0244.220125 (Interim)
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
test1	0	0	0/0	0 ● 0 ● 0	

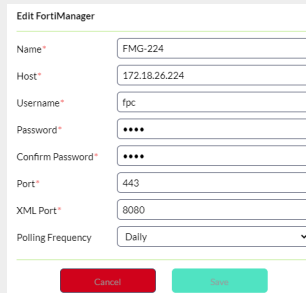
Pagination Color

The pagination color.

8. Buttons - Primary: Buttons related colors.

Background

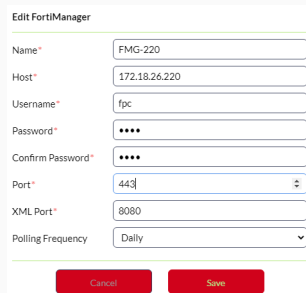
The primary button background color, e.g., the *Save* button background color in the image below.



The screenshot shows a form titled "Edit FortiManager" 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 (Dally). At the bottom, there are two buttons: "Cancel" (red) and "Save" (teal).

Text

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



The screenshot shows the same "Edit FortiManager" form as above, but with the "Save" button highlighted in red, demonstrating the primary button text color.

Disabled Background

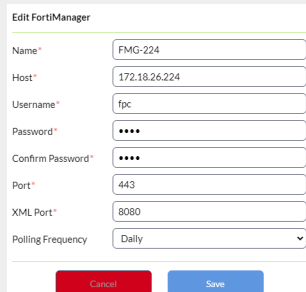
The disabled primary button background color.

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.

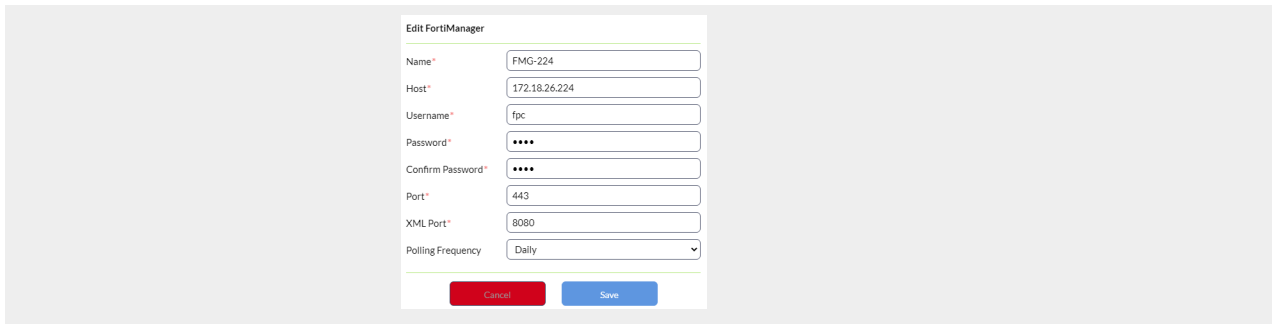


The screenshot shows the same "Edit FortiManager" form as above, but with the "Save" button highlighted in blue, demonstrating the active primary button background color.

9. Buttons - Secondary:

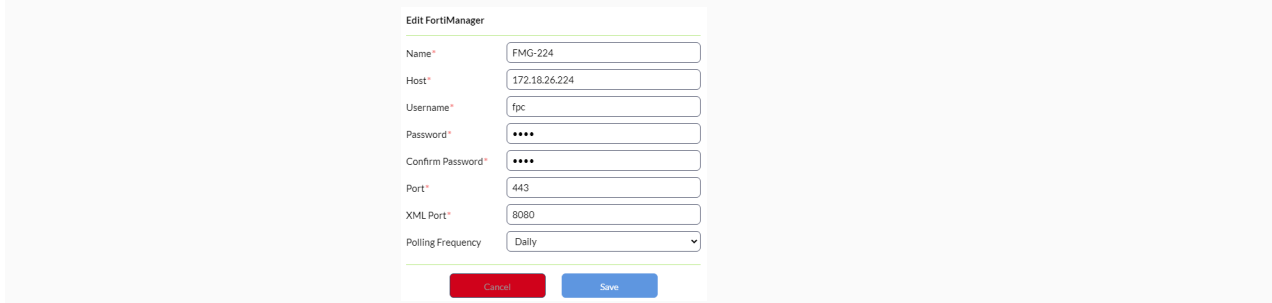
Background

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



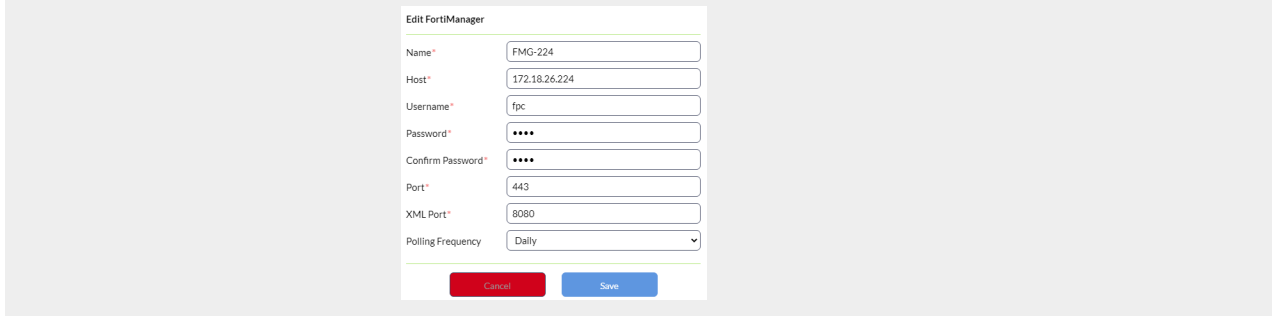
Border

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



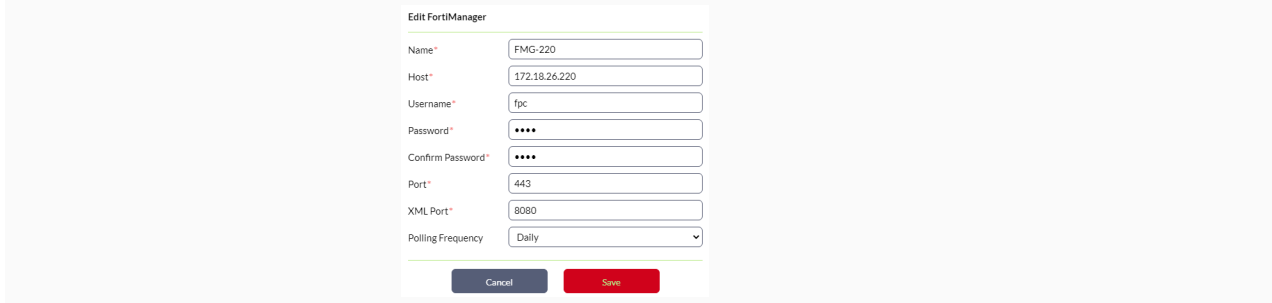
Text

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



Active Background

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



Active Border

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

Edit FortiManager

Name*

Host*

Username*

Password*

Confirm Password*

Port*

XML Port*

Polling Frequency

Disabled Background

The disabled secondary button background color.

Disabled Border

The disabled secondary button border color.

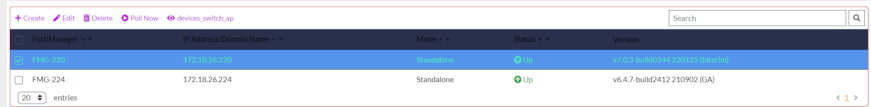
Disabled Text

The disabled secondary button text color.

10. Buttons - Light:

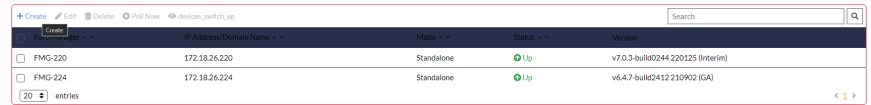
Text

The font color of the action buttons.



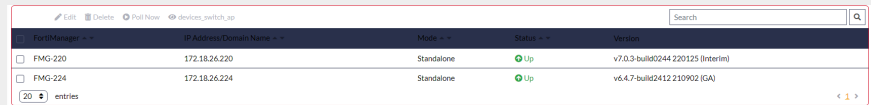
Active Text

The font color of the active action button.



Disabled Text

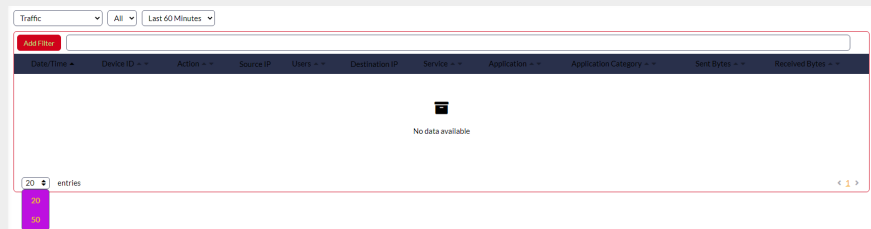
The font color of the disabled action buttons, e.g., *Edit*, *Delete*, *Poll Now*, and *devices_switch_ap* buttons in the image below.



11. Dropdown:

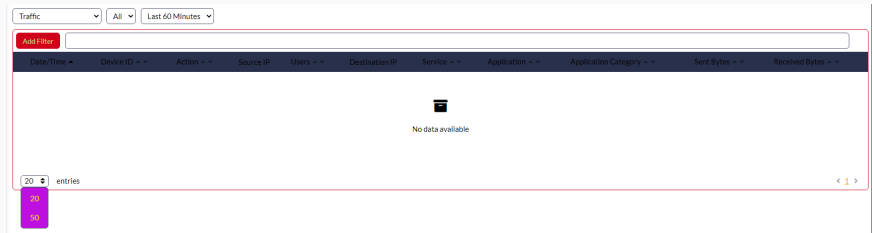
Background

The color of the dropdown background.



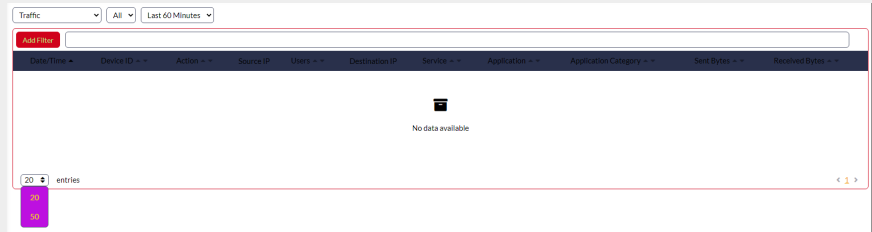
Border

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.

Edit FortiManager

Name*

Host*

Username*

Password*

Confirm Password*

Port*

XML Port*

Polling Frequency

Input Active Color

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

General

FPC Data Store Size* GB

Session Timeout*

Language*

Time Zone*

Enable Blocked Host

Certificate Information

Certificate

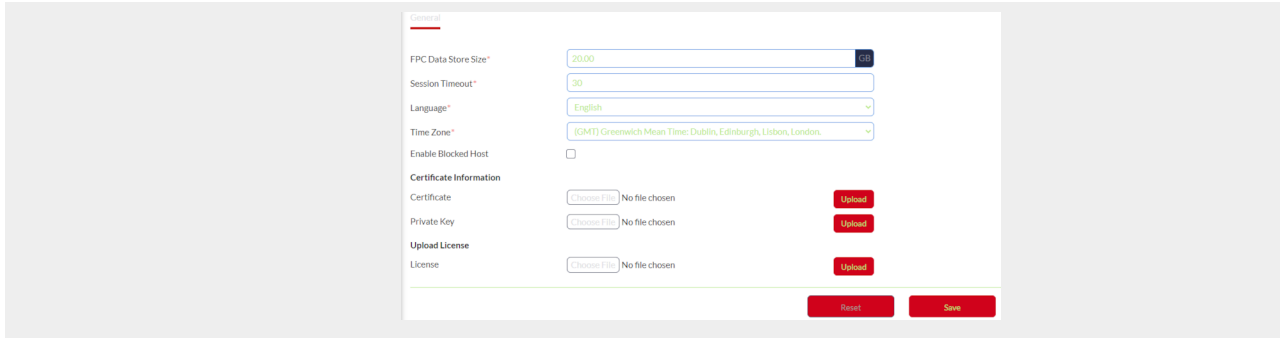
Private Key

Upload License

License

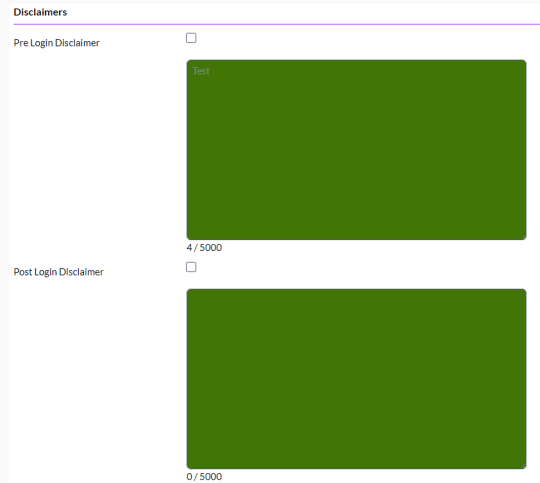
Input Text Color

The color of the text in a field.



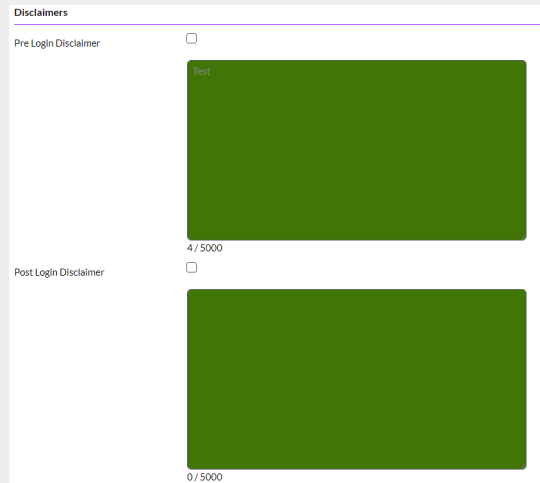
Input Disabled Background

The color of the disabled input field.



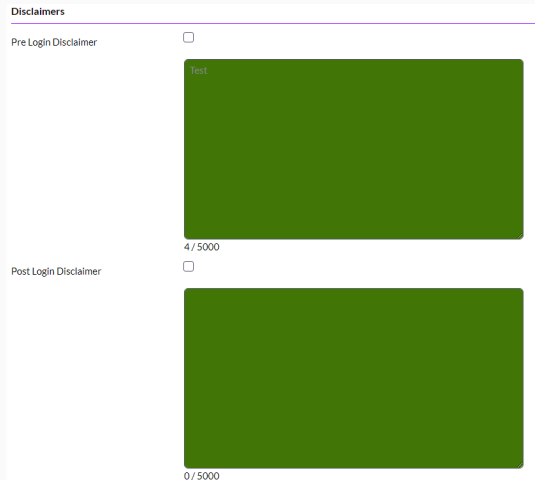
Input Disabled Text

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.

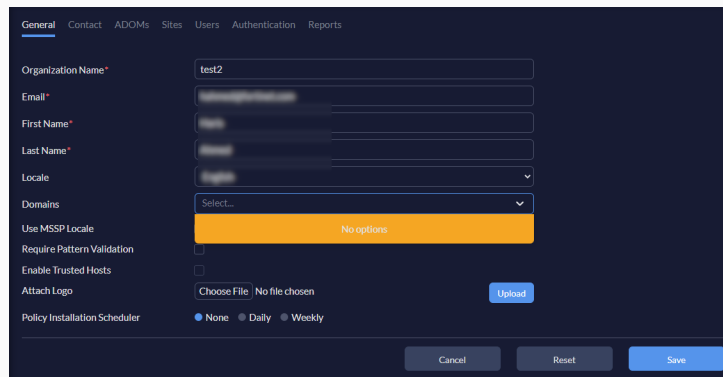


Input File Selected Text

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

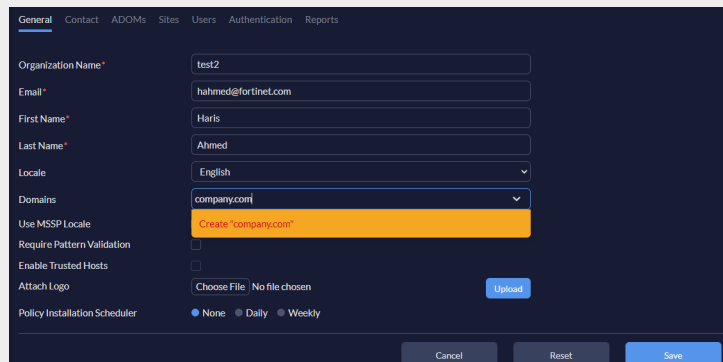
Select Option background

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 *Domains* 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 *Enable Trusted Hosts* 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.

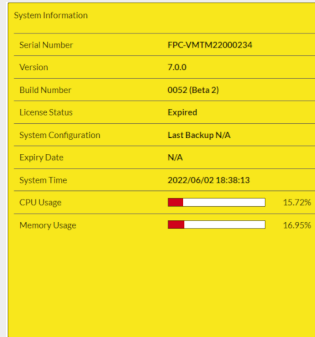
Radio Group Checked Disabled Border

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.

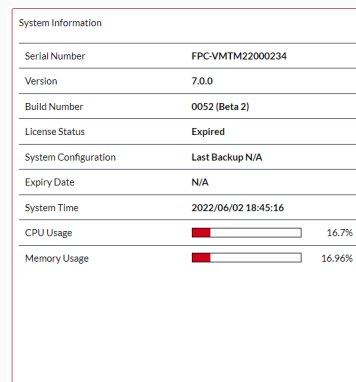


A screenshot of a 'System Information' widget with a yellow background. The widget contains a table of system details and two progress bars for CPU and Memory usage.

System Information	
Serial Number	FPC-VMTM22000234
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	15.72%
Memory Usage	16.95%

Border

The border color of a widget.

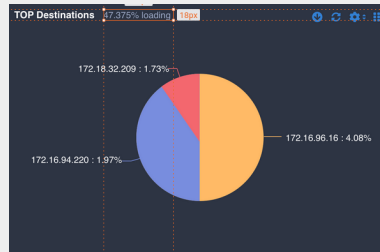


A screenshot of a 'System Information' widget with a red border. The widget contains a table of system details and two progress bars for CPU and Memory usage.

System Information	
Serial Number	FPC-VMTM22000234
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	16.7%
Memory Usage	16.96%

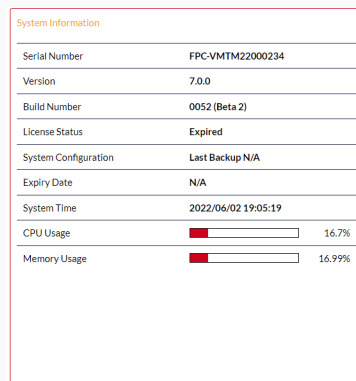
Percent Text

The color of the percent text.



Text

The font color of the heading in a widget.

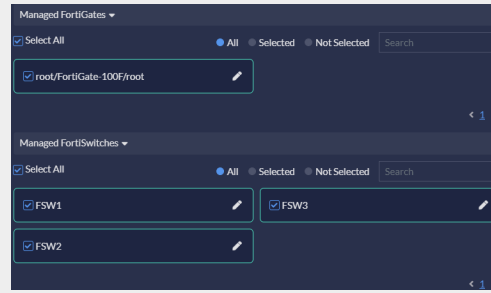


A screenshot of a 'System Information' widget with an orange heading. The widget contains a table of system details and two progress bars for CPU and Memory usage.

System Information	
Serial Number	FPC-VMTM22000234
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	16.7%
Memory Usage	16.99%

Device Selector Border

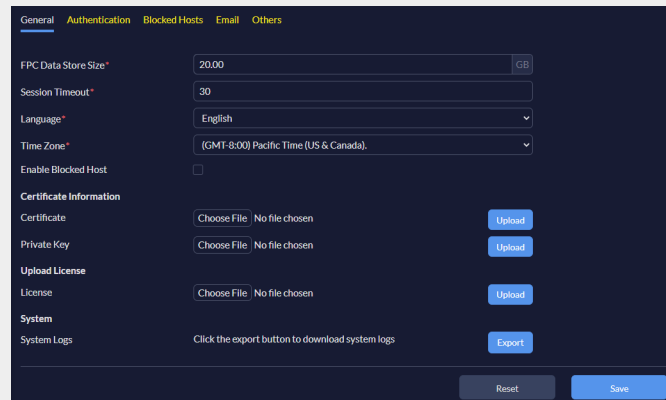
The border color for the device selector option.



- 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.

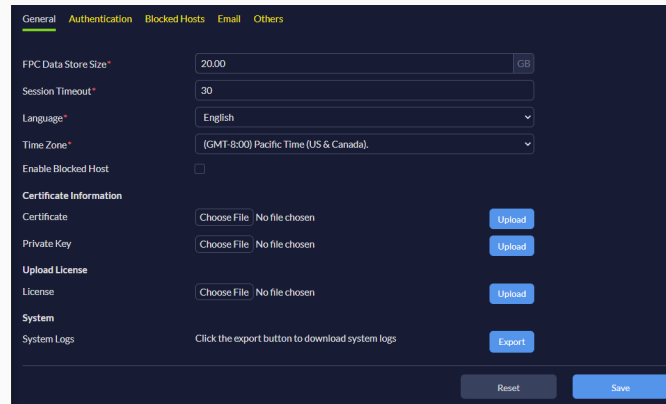
Text Color

The font color for the navigation bar elements.



Active Border

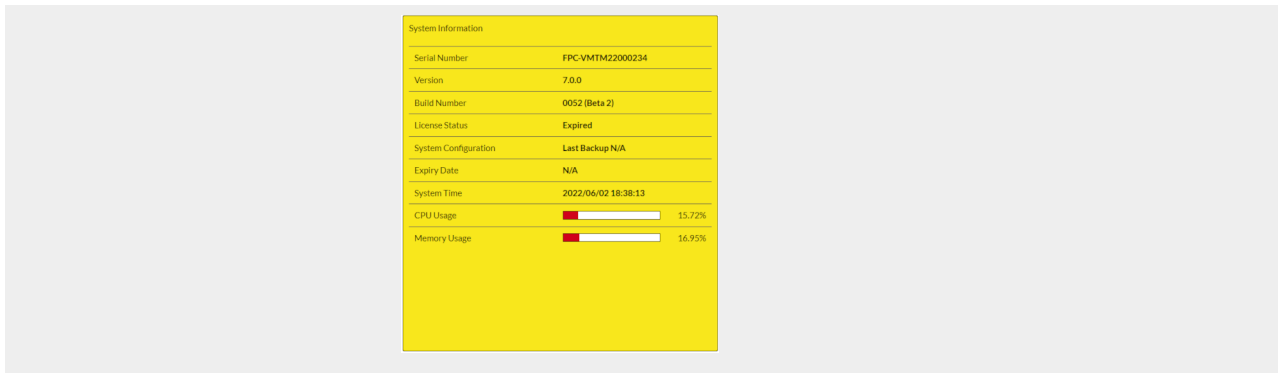
The border color of the active navigation bar element, e.g., the border color for the *General* tab.



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

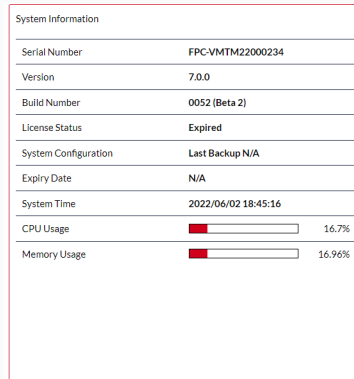
Active

The color of the progress bar.



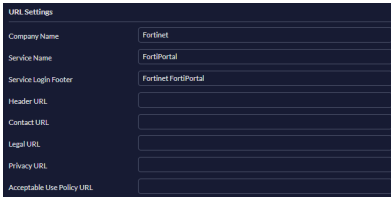
Border

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



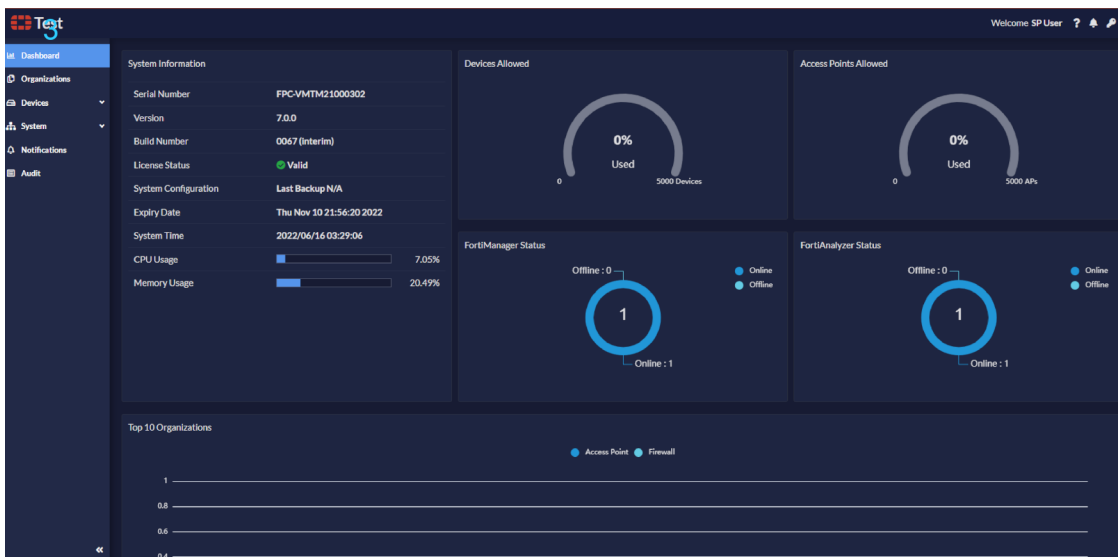
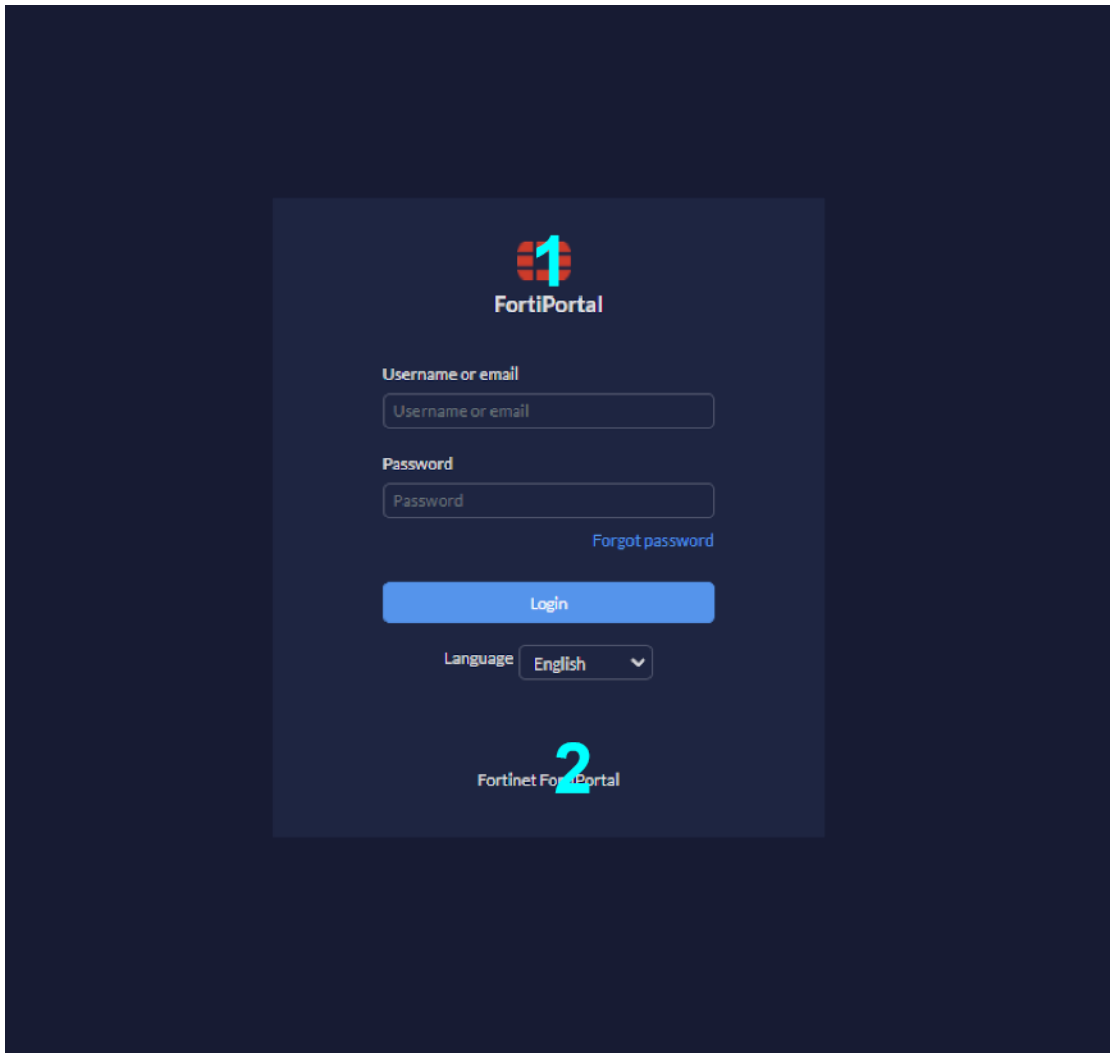
Custom URLs and text

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.
		 <p>The login page does not include a separate footer color.</p>
Company Name	3	Company name and header logo on the header of every page.

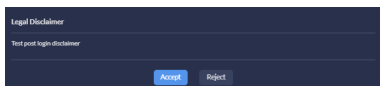
Disclaimers

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.

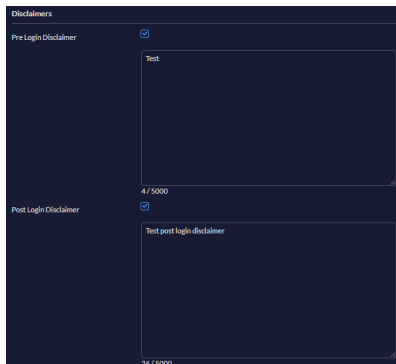


When a user logs in for the first time, a *Change Password* dialog appears asking the user to change the password.

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.

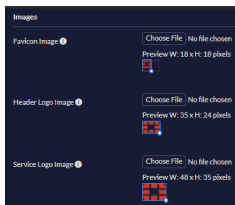


3. Click *Save* to save the changes.

At the next instance of login, and depending on whether you are an administrative user or a user, relevant disclaimers appear.

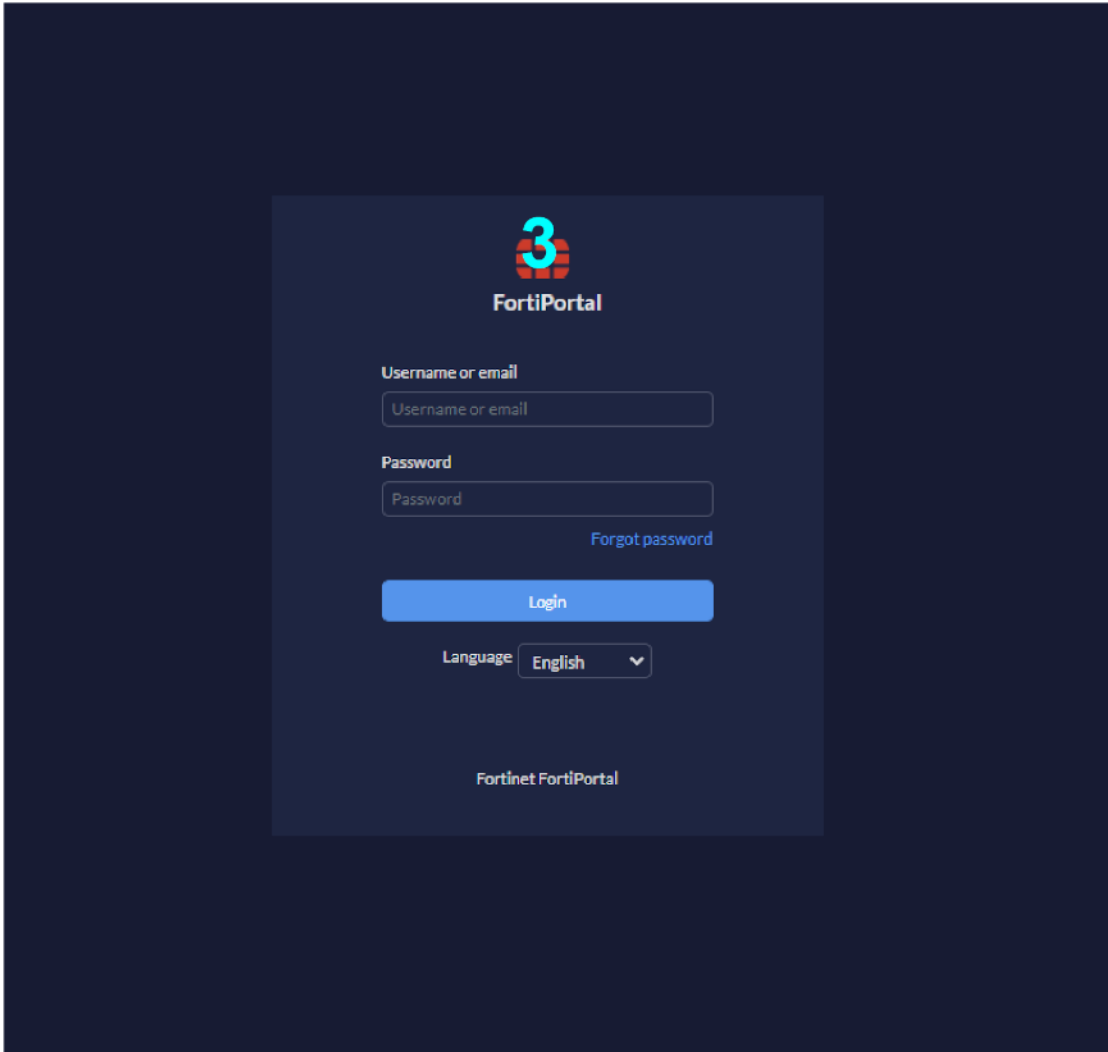
Custom images

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.

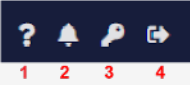
The following figure shows a downloaded alert icon image before resizing and after resizing:



Details of the theme configuration fields

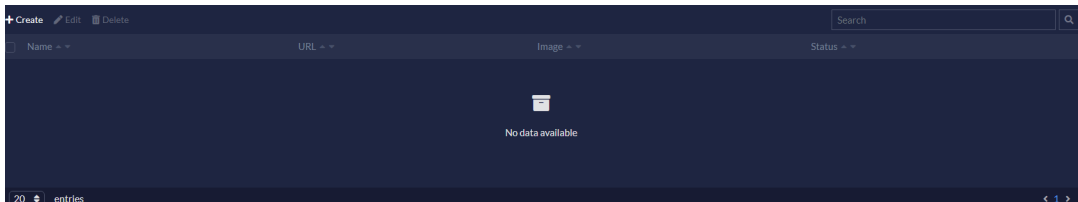
The following table describes the configuration fields:

Settings	Guidelines	Default value
URL values for Header and Footer		
There are links in the header and footer to various corporate web pages. The following URL values must be public web pages. Specify the full URL, including "http://".		
Company Name	The company name is displayed in the footer 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 activated from the company logo in the header, and the company name in the footer. Specify the URL to open, such as your company home page.	blank
Contact URL	Footer contains a link to the Contact page. Specify the target URL.	blank
Legal URL	Footer contains a link to the Legal page. Specify the target URL.	blank
Privacy URL	Footer contains a link to the Privacy page. Specify the target URL.	blank
Acceptable Use Policy URL	Footer contains a link to the Acceptable Use Policy page	blank
Color Scheme		
Color Scheme	Select a color scheme for the Admin pages. Select either the preconfigured color schemes (<i>Dark</i> or <i>Light</i>).	Light

Settings	Guidelines	Default value
	To edit a custom color scheme, select <i>Custom</i> and then select <i>Edit Custom Color Scheme</i> .	
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 Editing a custom color scheme on page 63 .	n/a
Disclaimers		
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
Image files		
	Unless otherwise stated, the supported file types for images include 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.	
Icons in the page banner		
1. Help Image	Image file for the help file icon in the page banner. The recommended image size is 30x30 pixels.	
2. Alert Image	Image file for the alert icon in the page banner. The recommended image size is 30x30 pixels.	
3. Change Password Image	Image file for the change password icon in the page banner. The recommended image size is 30x30 pixels.	
4. Logout Image	Image file for logging out of the FortiPortal in the page banner. The recommended image size is 30x30 pixels.	

Additional Resources

Go to *Admin > Additional Resources* to see the resource list, which enables administrators to add, edit, delete, or view the displayed resources:

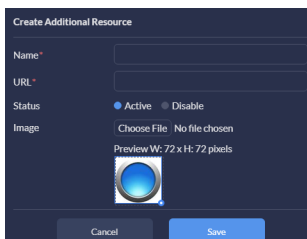


Page actions

The *Additional Resources* tab contains the following actions:

- *Create*—open a new dialog to add a resource
- *Edit*—edit the selected resource
- *Delete*—delete the selected resource
- *Search*—enter text to search for resources containing that text
- *Show x entries*—use the dropdown menu to set the number of entries to display (20 or 50)
- *Sort*—allows you to sort columns in ascending or descending order.

Selecting *Create* opens the *Create Additional Resource* dialog:

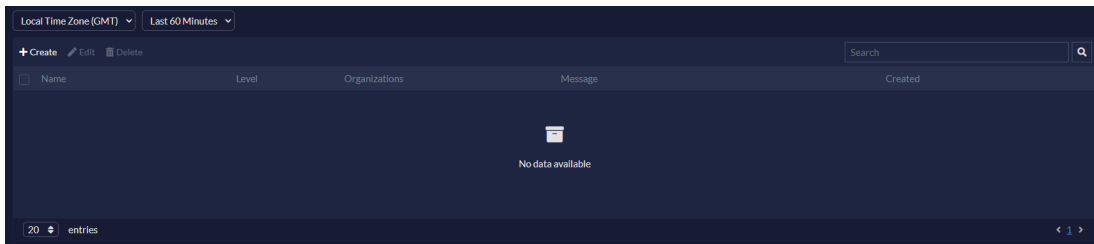


Enter the following button details:

Field	Description
Name	Required. Button or resource name.
URL	Required. Link to open when the button is selected.
Status	<i>Active</i> or <i>Disable</i>
Image	Default image is pre-populated. You can change or resize it with the <i>Choose File</i> button and resize icon.

Notifications

Go to *System > Notifications* to see which organizations are receiving which notifications:



Page actions

The *Notifications* tab contains the following actions:

- *Time zone*—use the dropdown to set the time zone to *Local Time Zone (US/Pacific)* or *GMT Time Zone*
- *Filter*—filter the data (*Last 60 Minutes*, *Last 1 Day*, *Last 1 Week*, or *Specify*)
- *Create*—opens a dialog to create a system notification
- *Edit*—edit selected notification
- *Delete*—delete selected notification
- *Search*—enter text to search for entries containing that text
- *Show x entries*—use the dropdown to set the number of entries to display per page (20 or 50)

Create notifications

1. Go to *System > Notifications* and select *Create*.
The *Create Notification* dialog opens.

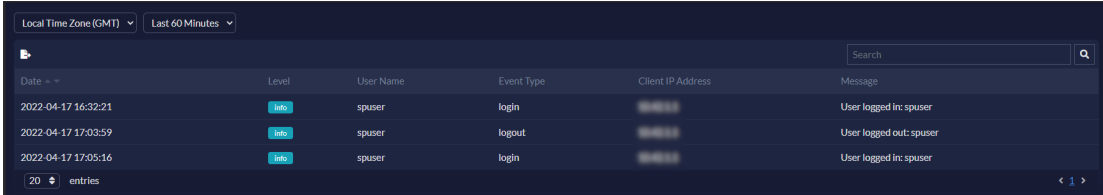
2. In the *Create Notification* window, enter the following information:

Field	Description
Name	Name of the notification
Level	The level of importance of events to send notifications about
Message	Text sent to the customers who will receive this notification. The maximum length of the message is 255 characters.
Organizations	From the dropdown, select an organization

3. Click **Save**

Audit

The *Audit* tab displays a log of user activity on the Administrative Web Interface:



The screenshot shows the Audit tab interface with a table of user activity logs. The table has columns for Date, Level, User Name, Event Type, Client IP Address, and Message. The logs show three entries for user 'spuser' with event types 'login', 'logout', and 'login'.

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*—use the dropdown to set the time zone *Local Time Zone (US/Pacific)* or *GMT Time Zone*
- *Filter*—set the duration 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*—use any column to search the audit log list by level, user name, event type, client IP address, or message
- *Show x entries*—use the dropdown to set the number of entries to display (20 or 50)
- *Sort*—allows you to sort some columns in ascending or descending order

Appendix A - Sizing

Sizing recommendations

The table below has sizing recommendations for the FortiPortal virtual machine.

Portal VM			
Number of customers	Number of VMs	RAM (GB)	vCPU
Minimum	1	16	4
500	1	16	8
1000	1	32	16
2500	1	64	16
5000	3(Cluster)	64	16
7500	3(Cluster)	64	24
10000	3(Cluster)	64	24



www.fortinet.com

Copyright© 2022 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.