



FortiPortal - Administration Guide

Version 6.0.6

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



October 5, 2021

FortiPortal 6.0.6 Administration Guide

37-606-645480-20211005

TABLE OF CONTENTS

Change Log	7
FortiPortal overview	8
Key features	8
Components	8
FortiAnalyzer modes	8
End-customer devices	9
FortiPortal concepts	10
Customer sites	10
Storage limits	10
Remote authentication	10
Trusted Hosts	11
Frequently asked questions	11
FortiPortal installation	12
VMware prerequisites	12
Downloading OVF files	13
Installing FortiPortal VMs	13
Start the VM	14
Basic setup	14
MySQL prerequisite	14
Sizing	15
Default login credentials	15
Database installation	15
Portal installation	16
FortiManager configuration	19
FortiAnalyzer configuration	20
Additional setup tasks	20
Alerts	21
Page actions	21
Administrative users	22
Page actions	22
Per-user actions	22
Create a user	23
Trusted Hosts	24
Admin user roles	25
Dashboard	26
Setting the top N entries	27
Customers	28
Page actions	28
Per-customer information	28
Per-customer actions	28

Add or edit a customer	30
Customer sites	37
Page actions	37
Per-site actions	37
Wireless Networks	39
Page actions	39
Per-network actions	39
Customer Users	41
Page actions	41
Per-user actions	41
Add a trusted host for a user	43
Customer user roles	44
Reports	46
FortiAnalyzer reports	46
Page actions	46
FortiManager devices	48
Page actions	48
Per-FortiManager actions	48
FortiManager high availability (HA)	48
Add a FortiManager	49
Edit a FortiManager	50
Manage FortiGate devices	51
FortiAnalyzer devices	52
Prerequisites	52
Page actions	52
Per-FortiAnalyzer actions	53
Edit a FortiAnalyzer	53
View FortiAnalyzer reports	54
Admin settings	55
Remote authentication using FortiAuthenticator	57
Configuring FortiAuthenticator	57
Configuring FortiPortal	58
RADIUS server configuration	59
RADIUS Roles	60
Remote authentication - SSO	62
SSO Roles	64
SSO example	66
Frequently asked questions (FAQs) about SSO configuration	66
SNMP	69
SNMP agent	69
SNMP v1/v2c communities	70
SNMP v3 users	73
SNMP MIBs	74
SNMP traps	74

Fortinet and FortiPortal MIB fields	75
Roles	77
Page actions	77
Per-role actions	77
System Log	79
Page actions	79
Theme	80
Custom theme options	80
Select a predefined color scheme	80
Create a custom color scheme	80
Using the color picker	81
Using a custom CSS file	83
Custom URLs and text	83
Disclaimers	84
Custom images	86
Resizing images	87
Details of the theme configuration fields	87
System Info	90
Version Information	90
License Information	90
Certificate Information	91
Upload a license	91
Trusted Hosts	92
Page actions	92
Per-host actions	92
Additional Resources	94
Page actions	94
Per-resource actions	95
System Notifications	96
Page actions	96
Per-notification actions	97
Audit	98
Page actions	98
Per-audit actions	98
Appendix: Sizing	100
Appendix: Installation using OpenStack	102
Prerequisites	102
Downloading FortiPortal image files	102
OpenStack Horizon Dashboard	102
Create an image for the portal	102
Create a volume for the portal	103
Launch the instance	103
Assign a floating IP address	104

Associate the volume to the instance	104
Reboot the instance	104
Determine the IP address and port number	104
Configure the portal parameters	105
Updating the SSL certificate file	106
Installing MySQL for FortiPortal databases	107
Reconfiguring MySQL password on FortiPortal	107
Appendix: Installation using Nutanix	108

Change Log

Date	Change Description
2021-10-05	Initial release.

FortiPortal overview

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

The service provides end customers with centralized reporting, traffic analysis, configuration management, and log retention without the need for the end customer 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

FortiPortal supports the following languages: English, French, German, Portuguese, Romanian, Spanish, and Italian.

Components

The end-customer'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.

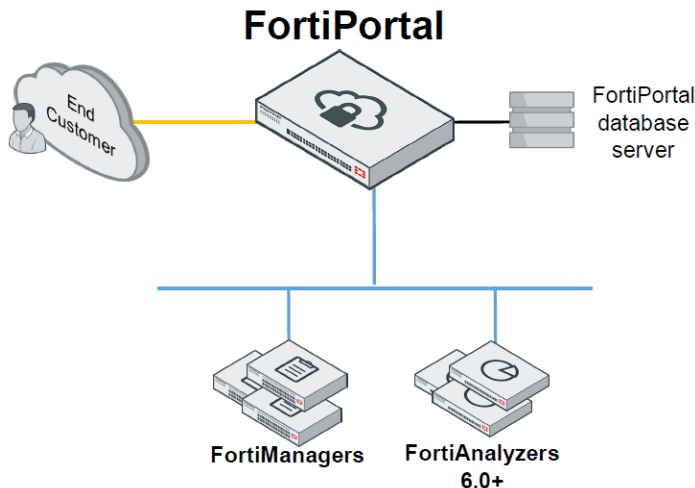
The portal provides an administrative web interface (for the administrative staff) and a customer web interface (for the end customers).

FortiAnalyzer modes

Starting in FortiPortal 5.2.0, you can go to *Admin > Settings* and select *FortiAnalyzer* for the Analytics Data Source setting. This setting changes the display of the Customers page, Add Customer form, and Edit Customer form for administrators. For end customers, this setting changes the display of the dashboard, Reports page, and View page.

FortiAnalyzer mode

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



The FortiPortal solution includes the following components in FortiAnalyzer mode:

- Portal: virtual appliance:
 - Provides the administrator web interface and the customer 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)
- Portal database: MySQL database:
 - Physical or virtual server provided by the administrator
 - The portal aggregates the logs into this database
 - FortiPortal includes only one portal database

The customer web interface enables each end customer to access/analyze their data and administer their service. For additional information about the customer web interface, see the [FortiPortal User Guide](#) (which is also available by selecting the help button in the customer web interface).

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

End-customer devices

FortiPortal requires that the customer FortiGate devices must be managed by FortiManager. FortiManagers may reside in the customer network or in the cloud.

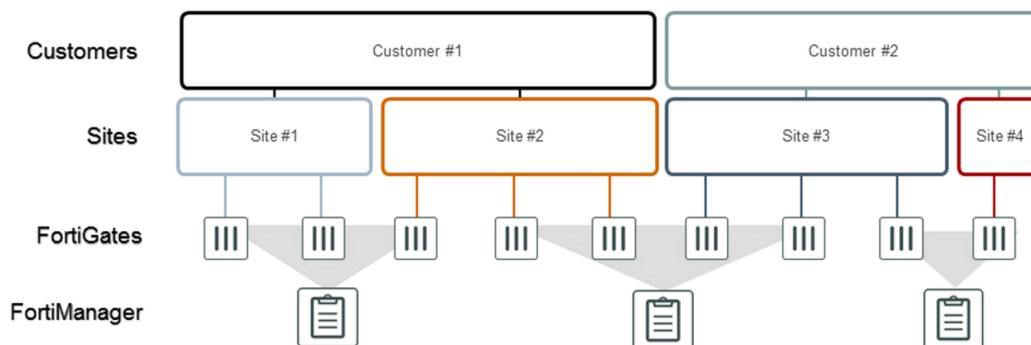
1. FortiGate: security devices in the customer environment:
 - generates the security logs
 - also fulfills the AP Wireless Controller role
2. FortiManager: manages a set of FortiGate devices:
 - All FortiGate devices in the FortiPortal must be managed by FortiManager
 - FortiManager provides device information to the FortiPortal
 - May reside in the customer network or in the cloud
3. (Optional) FortiAnalyzer: receives logs from the devices:
 - May reside in the customer network or in the cloud

FortiPortal concepts

FortiPortal introduces the following concepts:

Customer sites

- An end-customer 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 end-customer has a storage capacity maximum amount, which is expressed as a number of GB of database storage.

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

- Overwrite the oldest logs
- Stop logging

Remote authentication

You have the choice of local or remote user authentication of the Admin and Customer 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-customer allowlists.

If you enable Trusted Hosts as a global setting, the system enforces a configurable blocklist and configurable allowlist for all admin and customer users.

You can also enable Trusted Hosts as a customer setting. The system creates an allowlist of trusted hosts for the customer 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 a customer with Trusted Hosts enabled, the system also enforces the global blocklist and allowlist for the customer 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.

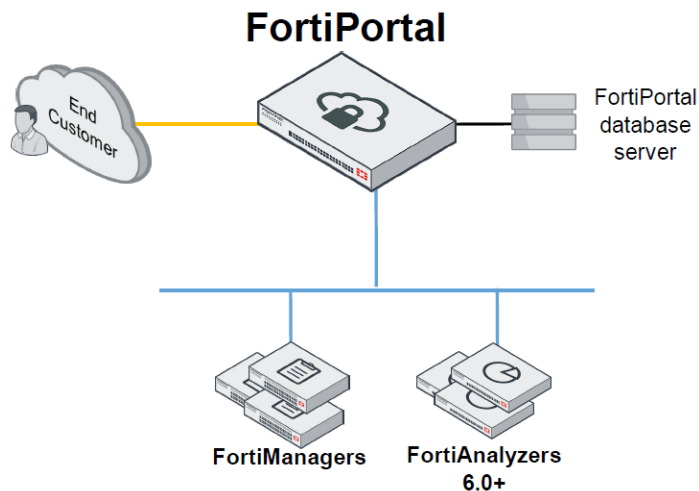
I can see data in the dashboard as a site administrator but not as customer user. How do I fix this?

Select the *User(s)* icon on the Customer List page to display the Customer User(s) page and then select the *Edit* icon for the specific customer user. Check if the customer user has permission to view information related to all sites and the devices associated with those sites.

For example, a customer 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

The following figure shows an example of a FortiPortal topology in FortiAnalyzer mode:



This chapter covers the following tasks:

- [VMware prerequisites on page 12](#)
- [Basic setup on page 14](#)
- [Additional setup tasks on page 20](#)

FortiPortal software provides a self-service management interface for customers (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 where each VM runs one of the following:

- Portal VM (which is the external interface for FortiManager)
- Portal database server VM

The basic installation requires several VMs. (Portal load balancing, which is discussed later, add additional VMs.)

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 database servers or FortiManager.

VMware prerequisites

For KVM and OpenStack, see [Appendix: Installation using OpenStack on page 102](#).

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

Before deploying your FortiPortal using VMware, you must do the following:

1. Install the VMware vSphere Client on the management computer.
2. All VM instances run on VMware ESXi Server version 5.5, 6.0, 6.5, and 6.7.

3. You must install one database server for the portal database.

Downloading OVF files

To download the required OVF files, follow these steps:

1. Navigate to the Fortinet customer service page (support.fortinet.com).
2. Go to *Download > Firmware Images*.
3. On the Firmware Images page, select *FortiPortal*.
4. Download the latest versions of the required zip file.
5. Extract the packages to a local folder on the management computer.

Installing FortiPortal VMs

Installing the portal includes the following major steps:

1. Create a VM instance. See [Create a VM instance on page 13](#).
2. Configure VM hardware settings. See [Configure VM hardware settings on page 14](#).
3. Power on the VM. See [Start the VM on page 14](#).
4. Configure the portal parameters.

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

Create a VM instance

This VM is intended for testing purposes only and should not be used for production environments.

1. Download the portal OVF file.
2. Launch the VMware vSphere client.
3. Enter the IP address or host name of your VMware server.
4. In the inventory menu, select the physical server where you will install the VM.
5. Select *File > Deploy OVF Template* to launch the OVF Template wizard. The wizard will guide you through a series of deployment steps.
6. *Source*: Use the Browse function to locate the OVF file:
 - Portal: FortiPortal-VM64.ovf
7. *OVF Template Details*: This page displays the following information: FortiPortal version, size of the download, and application size on disk. Select *Next*.
8. *End-user License Agreement*: Accept the end-user license agreement and select *Next*.
9. *Name and Location*: Enter a name for this virtual machine, select a location from the location inventory and select *Next*.
10. *Storage*: Select the destination storage for the virtual machine files and select *Next*.
11. *Disk Format*: This page displays the storage device that you selected in the previous step, along with available space. Select *Thin Provision* and select *Next*.
12. *Network Mapping*: Select the destination network to map to the source network in your OVF and select *Next*.
13. *Ready to Complete*: Review the deployment settings. Select *Back* to make any changes. When ready, select *Finish*.

Configure VM hardware settings

If required, adjust the VM CPU, memory and storage settings. The following are the default settings:

- CPU: 2
- Memory: 2 GB
- Hard drive: 80 GB

To adjust these numbers, select the newly created VM in the inventory list and select *Getting started > Edit virtual machine settings*.

Start the VM

In the inventory list, right-click the FortiPortal VM that you just installed and select *Power On*.

Basic setup

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 they interact with.

Basic setup covers the following tasks:

- [MySQL prerequisite on page 14](#)
- [Sizing on page 15](#)
- [Default login credentials on page 15](#)
- [Database installation on page 15](#)
- [Portal installation on page 16](#)
- [FortiManager configuration on page 19](#)
- [FortiAnalyzer configuration on page 20](#)

MySQL prerequisite

Before using MySQL, you need to check if MySQL is configured properly. The 'local_infile' variable needs to be on.

To check if the 'local_infile' variable is on, run the following query from the MySQL console:

```
SHOW GLOBAL VARIABLES LIKE 'local_infile';
```

If the 'local_infile' variable is off, run the following query to turn it on:

```
SET GLOBAL local_infile = 'ON';
```

When the 'local_infile' variable is off, FortiPortal will experience various issues, such as FortiView finding no matching records for session logs.

Sizing

FortiPortal sizing can be complex. Fortinet recommends that you work with your Fortinet systems engineer when possible. However, using the following guidelines, you can successfully complete this task:

- Portal VM—The default storage disk size is 80 GB, which is the recommended minimum. (The 2-GB disk in the VM is the flash memory; the 80-GB disk is storage.) If you have many customer logins and many devices, then increase the memory and disk sizes for improved performance.

Default login credentials

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

Component	Default User Name	Default password
Portal	admin	No password

Database installation

Fortinet does not provide this server as part of FortiPortal. Fortinet supports the databases created by FortiPortal and the connections to them.

The following is the overall installation procedure, which starts by configuring the database servers:

1. After you create the database server image, you must install at least once instance for the portal database.
2. Create the server VM and install the database server. FortiPortal supports MariaDB 10.2 and MySQL 5.7.
3. Install the portal. The portal requires a license.
4. After FortiPortal is running, you can add FortiManager devices and set up customers. See [FortiManager devices on page 48](#) and [Add or edit a customer on page 30](#).

After you create the server VM and install the database server, configure the following settings in MySQL (version 5.7 or later) or MariaDB (version 10.2):

1. Set the MySQL server `bind-address` and `sql_mode` parameters in the `[mysqld]` section of one of the following files:

For MariaSQL: `/etc/mysql/my.cnf`

For MariaDB 10.2: `/etc/mysql/mysql.conf.d/mysqld.cnf`

For MariaDB 10.2.x: `/etc/mysql/mariadb.conf.d/50-server.cnf`

For example:

```
[mysqld]
...
bind-address = 10.220.64.121
...
sql_mode = STRICT_TRANS_TABLES,NO_ZERO_IN_DATE,NO_ZERO_DATE,ERROR_FOR_DIVISION_BY_
ZERO,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION
```

- From the MySQL console, use the `show variables` command to check that the following parameters are correctly set:

```
mysql -u root -p
```

- Create a user for the portal, grant privileges to the user, and check that the user is created:

```
create user '<database_user_name>'@'%' identified by '<database_user_password>';
GRANT ALL PRIVILEGES ON *.* TO '<database_user_name>'@'%' IDENTIFIED BY <database_
user_password>;
flush privileges;
```

```
# Use the following query to check that the user and host are entered correctly
select host,user from mysql.user;
```

For example:

```
> create user 'fpc'@'%' identified by 'fpc';
> GRANT ALL PRIVILEGES ON *.* TO 'fpc'@'%' IDENTIFIED BY 'fpc';
> flush privileges;
> select host,user from mysql.user;
```



Ensure that from the MySQL instance you can resolve the MySQL server hostname (e.g. by pinging it), and that you can resolve the portal IP. Adding entries to `/etc/hosts` on the MySQL instance is one way of doing this.

Portal installation

Before doing the portal installation, Fortinet recommends taking a snapshot of the portal database server in its initial state. If there are any errors installing portal, you can revert the database server to its initial state.

- Install the portal VM image. For a new VMware installation, use the `fpcvm64imagePortal.out.ovf.zip` file. For the KVM version, see [Appendix: Installation using OpenStack on page 102](#).
- Configure the CLI settings. For example:

```
config system global
  set hostname portal # use whatever name that you want to give the VM
  set timezone 28 # use ? to identify the correct value for your region
end
```

```
config system interface
  edit port1
    set ip 10.220.64.120/24
    set allowaccess ping https ssh http
  end
```

```
config system route
  edit 1
    set device port1
    set gateway 10.220.64.1
  end
```

```
config system sql
```



```
set status remote
set database-name fp_fazlite
set database-type mysql # REQUIRED. If you omit this step, there will be problems with
    generating the portal database.
set database-port 3365 # this example changes the default MySQL port from 3306 to 3365
set username fpc # use the database user name instead of fpc
set password xyz # use the password for the database user name
set server 10.220.64.121
end
```



FortiPortal must be rebooted after a change is made to `config system sql`.



Using the `config system sql` command updates the database property file with the current values even if no changes are made. This causes the GUI session to disconnect. If you want to only check the SQL settings, use `show system sql` command.

3. Check the NTP settings with the `show system ntp` command. Modify the settings for your environment if necessary.



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

4. Reboot the VM.
5. From the database console, check the FortiPortal version information:

```
select * from ftntpmcdb.fpc_version;
```

6. Log in to FortiPortal using the user name `spuser` and the password `test123`:

<https://10.220.64.120/fpc/login>



[Forgot password](#)

Language

Fortinet FortiPortal

The left pane is common for all of the pages (Dashboard, Customers, Devices, Admin, and Audit).

- Next, you need to set the portal database size available on the portal database server. Go to *Admin > Settings* to specify the *FPC Data Store Size*.
For example, 1024 GB.



The mail settings must also be configured during the first-time configuration.

- Next, upload the license file. Go to *Admin > System Info* and select *Upload License*.
- After the license is uploaded, check that the license status is valid and the number of devices allowed is correct.



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, select *Admin > System Info* to display information about the SSL certificate.

System Info page

The screenshot shows the FortiPortal Admin portal's System Info page. The page is divided into several sections: Version Information, License Information, and Certificate Information. The Version Information section displays the current version (6.0.0), database version (6.0.0), and build number (58 (Interim)). The License Information section shows the VM License status (valid), the number of devices allowed (100), the number of FSA devices used (16), and the license expiry date (Sun Jun 28 20:12:13 2020 GMT). The Certificate Information section includes fields for Certificate, Private Key, and Upload License, each with a 'Choose File' button and a 'Browse' button. A 'Save' button is located at the bottom of the Certificate Information section.

The Certificate Information panel displays the certificate file name and private key file name.

From this panel, you can select and upload a new certificate and private key for the FortiPortal (using 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:

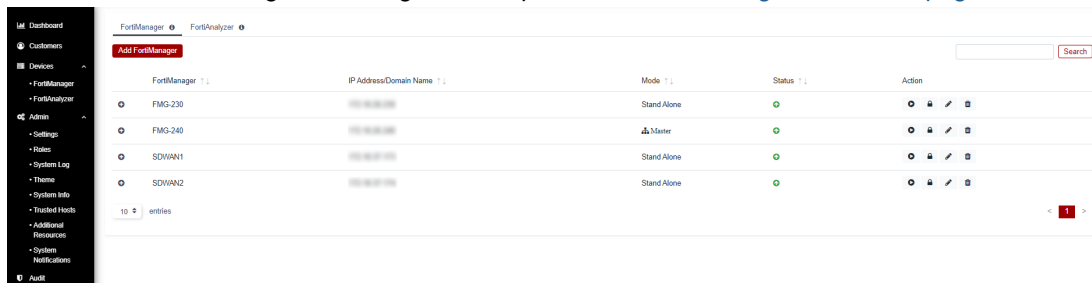
```
config system admin user
  edit fpc
    set profileid Super_User
    set adom all_adoms
    set policy-package all_policy_packages
    set password fortinet
    set rpc-permit read-write
  next
end
```

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 48](#).



FortiManager	IP Address/Domain Name	Mode	Status	Action
FMG-230	192.168.1.100	Stand Alone	●	⊙ ✎ ⊞
FMG-240	192.168.1.101	Master	●	⊙ ✎ ⊞
SDWAN1	192.168.1.102	Stand Alone	●	⊙ ✎ ⊞
SDWAN2	192.168.1.103	Stand Alone	●	⊙ ✎ ⊞

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 52](#).

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 48](#).
- To add wireless controllers, see [Manage FortiGate devices on page 51](#).
- To add FortiAnalyzer devices, see [FortiAnalyzer devices on page 52](#).
- To create an end customer, see [Add or edit a customer on page 30](#).
- To create customer sites, see [Customer sites on page 37](#).
- To create site administrators, see [Customer Users on page 41](#).

Alerts

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

<input type="checkbox"/>	Type	Message	Time
<input type="checkbox"/>	info	Delete data process for delete device(70-5/FGVM08TM21001075/root) from fortimanager ended	2021-04-12 14:09:38
<input type="checkbox"/>	info	Delete data process for delete device(70-5/FGVM08TM21001075/root) from fortimanager started	2021-04-12 14:09:22
<input type="checkbox"/>	info	Delete data process for delete device(70-5/FGVM08TM21001075/root) from fortimanager ended	2021-04-12 13:54:32
<input type="checkbox"/>	info	Delete data process for delete device(70-5/FGVM08TM21001075/root) from fortimanager started	2021-04-12 13:54:21
<input type="checkbox"/>	info	Delete data process for delete device(70-5/FGVM08TM21001075/root) from fortimanager ended	2021-04-12 13:39:34

For each alert, the window displays the following:


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

Page actions

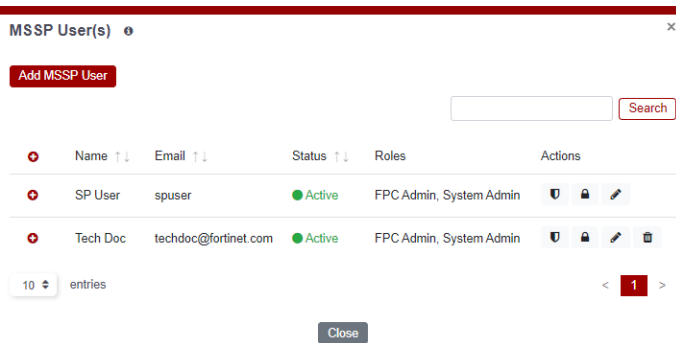
The *Alerts* window contains the following actions:

- *Filter*—filter the data (Last 60 Minutes, Last 1 day, Last 1 week)
- *Time zone*—use the dropdown to set the time zone to Local Time Zone (US/Pacific) or GMT Time Zone
- *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

Administrative users

Selecting the  icon on the top-right hand side displays the list of FortiPortal administrators.

These users are local users. The described commands are available only when *Admin Settings > Authentication Access* is set to *LOCAL*.







Page actions

In this window, the following actions are available:

- *Add MSSP User*—open a dialog to add an administrative user
- *Search*—enter text to search for user names containing that text
- *Show N entries*—filter the maximum number of customers to display in the page
- *Sort*—allows you to sort columns in ascending or descending order.

Per-user actions

When you scroll over a entry in the users list, the following icons appear in the Action column:

- —opens a dialog to edit the data for this user
- —deletes the entry.
- —opens the Trusted Host list
- —opens the Change Password dialog box



You cannot delete the default admin user.

Create a user

1. From the *MSSP User(s)* window, select *Add MSSP User*.

2. Input the fields, as described in the table.
3. Select *Save*.

The following table describes the fields in the *Add MSSP User/Edit MSSP User* dialog:

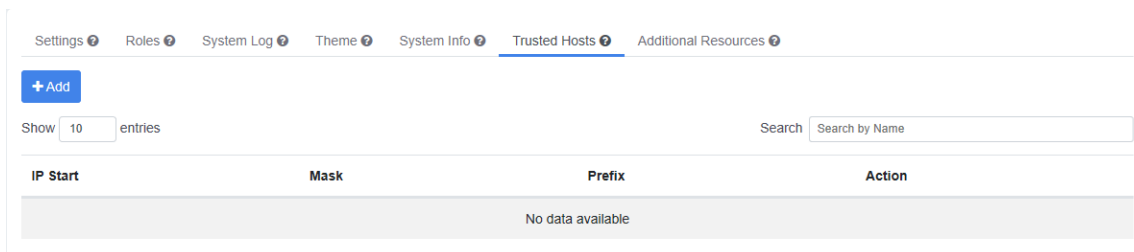
Settings	Guidelines
First Name	Name of the administrator
Last Name	
Email	Email address of the administrator
Password Policy	Enable or disable. If enabled, you can set one or more of the following types of character that the password must contain: <ul style="list-style-type: none"> • Uppercase Letters • Lowercase Letters • Numbers (0-9) • Special Characters
Password	The administrator uses these credentials to access the customer portal. The password must meet the requirements set by the password policy.
Confirm Password	
Minimum Length	Select the minimum number of characters that a password must contain.
Address1	Business address for the administrator
Address2	
CityState	

Settings	Guidelines
Country	
Zip	
Phone	Phone and fax numbers
Fax	
Available Roles	Roles that are available for this user type
Selected Roles	Selected roles for this user
Status	Select whether the administrative user is <i>Active</i> or <i>Disabled</i> .

Trusted Hosts

If you enable Trusted Hosts as a global setting (see [Admin settings on page 55](#)), the system enforces a configurable trust-host blacklist and allowlist for all admin and customer users.

You can also create a global trusted-host allowlist and subsequently open the list by selecting the *Trusted Host* tab.



From the allowlist, you can edit/delete an existing trusted host, or add a trusted-host entry.

The *Add IP BlockList/Edit IP BlockList* dialog contains the following fields:

Settings	Guidelines
IPv4	
IP Start	Start address for the range covered by this entry
Mask	Defines the range of IP addresses
IPv6	
IP Start	Start address for the range covered by this entry
Prefix	Defines the range of IP addresses covered by this entry

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 customer 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 Customer Portal pages.

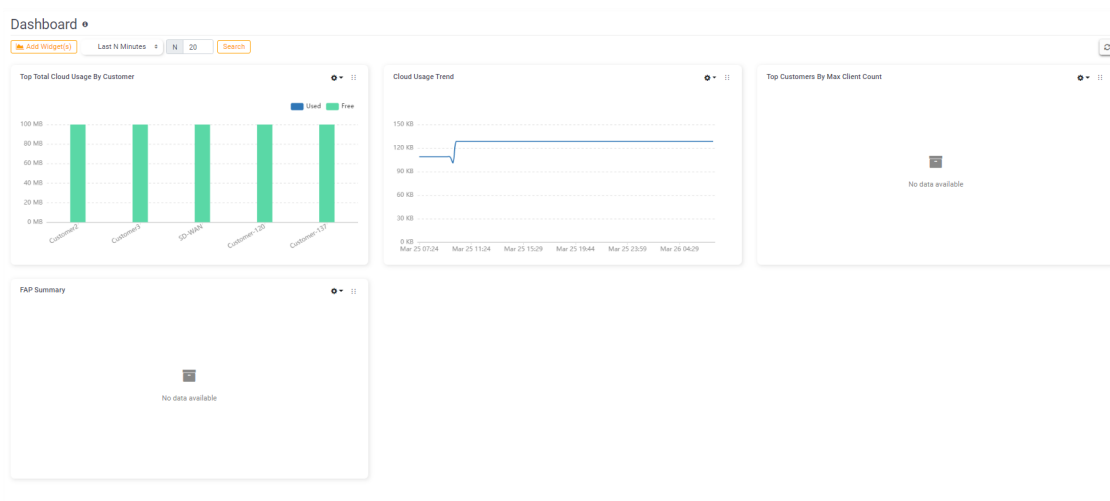
The system provides a set of default administrative roles. Using the FortiPortal Roles user interface, you can also create new roles or customize the default roles.

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 customer 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 customer 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 customer portal.

Dashboard

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



Actions available (at the top of the Dashboard):

- *Add Widget(s)*—add a widget to the dashboard
- *Filter*—filter the data based on time (last 5 Minutes, last 30 Minutes, last 60 Minutes, last N Minutes, last 4 Hours, last 12 Hours, last N Hours, last 1 Day, last 7 Days, last N Days, last N Months, or specify)



When you set the filter to *last N Minutes/Hours/Days/Months*, a search box appears next to *Filter*. Enter a value for *N* and click *Search* to apply this filter.

The widgets for the dashboard are updated according to your selection in *Filter* and the value entered in the *N* search box.

- *Refresh*—refresh the display for all of the widgets on the tab

The dashboard includes the following default widgets:

- Top Total Cloud Usage By Customer
 - Hover your cursor over each customer to view the detailed usage numbers
- Cloud Usage Trend
 - Hover your cursor over each customer to view the detailed numbers over the selected usage period
- Top Customer By Max Client Count
- Fortinet Access Point (FAP) Summary
 - Select the pie chart to view a list of the FAPs that are up (select the left side) or FAPs that are down (select the right side of the pie chart)

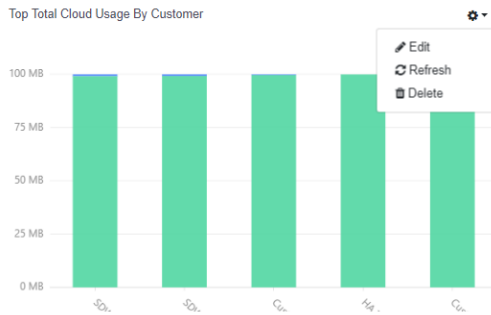
The title bar on each widget has an *action* dropdown that provides the following controls:

- *Edit*—opens a dialog to edit the widget details
- *Refresh*—refresh the widget display

- *Delete*—delete the widget
- *Drag to reorder*—select and then drag and drop to change the position of a widget in the pane

Setting the top N entries

On the upper right corner of most of the widgets, click the *Settings* icon and select *Edit* to configure the widget to show the top N entries (5, 10, 15):

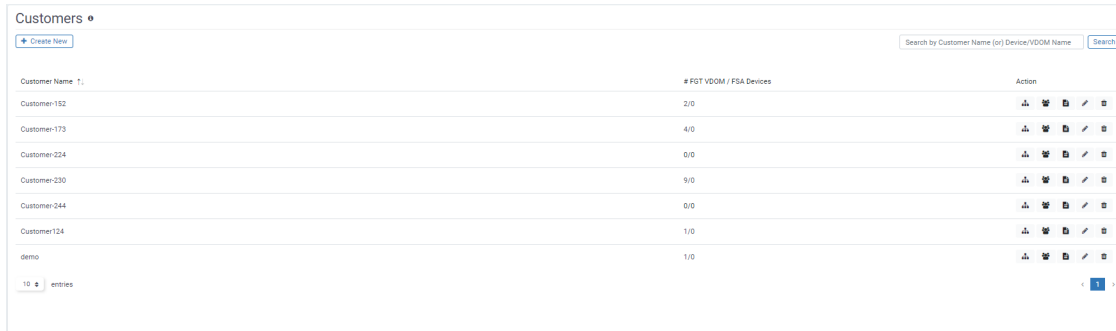


Select a number and select *Save* to refresh the report.

Customers

The *Customers* tab shows summary information for each customer.

The content pane lists the customer name and the number of devices that the customer has:



Customer Name	# FGT VDOM / FSA Devices	Action
Customer-152	2/0	⬇️ 🗑️ ✎️ 🗑️
Customer-173	4/0	⬇️ 🗑️ ✎️ 🗑️
Customer-224	0/0	⬇️ 🗑️ ✎️ 🗑️
Customer-230	9/0	⬇️ 🗑️ ✎️ 🗑️
Customer-244	0/0	⬇️ 🗑️ ✎️ 🗑️
Customer-124	1/0	⬇️ 🗑️ ✎️ 🗑️
demo	1/0	⬇️ 🗑️ ✎️ 🗑️

Page actions

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

- **Create New**—open a dialog to add a customer. See [Add or edit a customer on page 30](#).
- **Search**—enter text to search for customer names containing that text.
- **Sort**—allows you to sort data in ascending or descending order.
- **Show *N* entries**—filter the maximum number of customers to display in the page.

Per-customer information

The system displays the following information for each customer:

Field	Description
# FGT VDOM / FSA Devices	<i>FGT VDOM Devices</i> —the number of FortiManager/FortiAP devices that are registered to this customer <i>FSA Devices</i> —the number of FortiSandbox devices that are registered to this customer

Per-customer actions

The customer table displays the following icons in the Action column:

- *Edit*—opens a dialog with the form to [edit](#) the customer data. See [Add or edit a customer on page 30](#).
- *Delete*—deletes this customer.
- *Sites*—opens a window with a list of sites for this customer. See [Customer sites on page 37](#).
- *User(s)*—opens a window with a list of users for this customer. See [Customer Users on page 41](#).
- *Reports*—opens a window with a list of reports for this customer. See [Reports on page 46](#).

When you select a customer name in the list, the system opens the customer portal for this customer (in a new tab).

Add or edit a customer

Selecting *Create New* on the upper left of the *Customers* tab displays a dialog for adding a new customer (fields in the form are blank). (Hovering over any entry in the *Customer* tab and selecting the *Edit Settings* icon displays the *Edit Customer* dialog, which is identical to the *Add Customer* dialog except that fields are set to the values for this customer.)

Add or edit a customer

Add Customer ▾

Customer Details

* Customer Name

* First Name

* Last Name

* Email

Domains

Require Pattern Validation

Locale Use MSSP Locale

Attach Logo No file chosen

Contact Information

Address1

Address2

City

State

Country

Zip

Phone

Fax

Cloud Properties

Enable Analytics

* Total Storage MB

Others

Trusted Hosts Enable
 Disable

Policy Installation Scheduler: None
 Daily
 Weekly

Display Storage

Display Site

Comment-based Filter(s)

Name-based Filter(s)

Policy & Object Edit Permissions

<input checked="" type="checkbox"/> All	<input checked="" type="checkbox"/> Application Control	<input checked="" type="checkbox"/> AntiVirus
<input checked="" type="checkbox"/> Antispam	<input checked="" type="checkbox"/> DLP Filter RegEx	<input checked="" type="checkbox"/> Firewall Policy
<input checked="" type="checkbox"/> DLP Sensor	<input checked="" type="checkbox"/> Zone Interface	<input checked="" type="checkbox"/> IPS Sensor
<input checked="" type="checkbox"/> Firewall Address	<input checked="" type="checkbox"/> Rating Overrides	<input checked="" type="checkbox"/> Schedule
<input checked="" type="checkbox"/> Local Category	<input checked="" type="checkbox"/> User	<input checked="" type="checkbox"/> User group
<input checked="" type="checkbox"/> Service	<input checked="" type="checkbox"/> Web Filtering	<input checked="" type="checkbox"/> Web Filter RegEx
<input checked="" type="checkbox"/> Virtual IP		
<input checked="" type="checkbox"/> DNS Filter		

Policy Tab Permissions

<input type="checkbox"/> All	<input type="checkbox"/> IPv6 Interface Policy	<input type="checkbox"/> IPv6 DoS Policy
<input type="checkbox"/> Central NAT	<input type="checkbox"/> Interface Policy	<input type="checkbox"/> IPv6 Policy
<input type="checkbox"/> NAT64 Policy	<input type="checkbox"/> NAT46 Policy	

Tab Permissions

<input type="checkbox"/> All	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Reports
<input checked="" type="checkbox"/> Dashboard	<input checked="" type="checkbox"/> Objects	<input checked="" type="checkbox"/> Additional Resources
<input checked="" type="checkbox"/> Policy	<input type="checkbox"/> Device Manager	<input checked="" type="checkbox"/> WiFi
<input checked="" type="checkbox"/> Audit Logs	<input checked="" type="checkbox"/> Device Health	
<input checked="" type="checkbox"/> SD-WAN		

Widget Permissions

Available Widgets: search, Top Countries, Top Threats, Top Sources, Top Destinations, Top Applications, Policy Hits, Rogue Access Points, Authorized Access Points

Selected Widgets: search

Buttons: Add, Add all, Remove, Remove all

Adom Filter Permissions and Alias

Select All All Selected Not Selected

<input type="checkbox"/> 10.59.62.242/DC-62	<input checked="" type="checkbox"/>	<input type="checkbox"/> 10.59.62.242/SD-WAN-642	<input checked="" type="checkbox"/>
<input type="checkbox"/> 10.59.62.242/SD-WAN-644	<input checked="" type="checkbox"/>	<input type="checkbox"/> FMG-120/62	<input checked="" type="checkbox"/>
<input type="checkbox"/> FMG-120/64	<input checked="" type="checkbox"/>	<input type="checkbox"/> FMG-120/70-5	<input checked="" type="checkbox"/>
<input type="checkbox"/> FMG-120/test1	<input checked="" type="checkbox"/>	<input type="checkbox"/> FMG-120/testB	<input checked="" type="checkbox"/>
<input type="checkbox"/> FMG-121/customer_001	<input checked="" type="checkbox"/>	<input type="checkbox"/> FMG-1500/ropt	<input checked="" type="checkbox"/>
<input type="checkbox"/> FMG-189/uncredit	<input checked="" type="checkbox"/>	<input type="checkbox"/> FMG-189/VPN/Manager	<input checked="" type="checkbox"/>

< 1 2 >

To add or edit a customer:

1. Input the fields, as described in the following sections.
2. Select Save.

The *Add Customer* dialog comprises a number of panes. The following sections describe the fields in each pane.

Customer Details and Contact Information

These panes contain basic information about the customer:

Customer Details

* Customer Name

* First Name

* Last Name

* Email

Domains +

Require Pattern Validation

Use MSSP Locale

Locale

Attach Logo No file chosen

Contact Information

Address1

Address2

City

State

Country

Zip

Phone

Fax

Settings	Guidelines
Customer Details	
Customer Name	Customer's business name, which must be unique within this FortiPortal.
First Name	Name and email of the primary customer contact
Last Name	
Email	
Domains	<p>Enter a domain and then select the green + button. The new domain appears in the list below the entry box.</p> <p>Use this field for the customer domain. To specify a domain for the administrator, see Admin settings on page 55.</p> <hr/> <div style="display: flex; align-items: center;"> <p>When using remote authentication, a customer may have users defined in more than one domain.</p> </div> <hr/>
Use MSSP Locale	Uses the MSSP locale (the language configured in Admin Settings).
Language	If you deselect the <i>Use MSSP Locale</i> checkbox, you can select a language for this customer. When a customer user logs in to the GUI, pages will display in this language. For Administrative users, the system will continue to use the language set in the Admin Settings.

Settings	Guidelines
Attach Logo	Download an image file for this customer's logo. The maximum file size is 1 MB. The format can be jpg, gif, bmp, or png. The maximum file dimension is 144 pixels wide by 48 pixels tall.
Contact Information	
Address1	Address fields and phone and fax numbers for this customer
Address2	
City	
State	
Country	
Zip	
Phone	
Fax	

Cloud Properties

This pane contains information about portal storage for this customer.

The pane looks like the following figure:



Settings	Guidelines
Enable Analytics	Select to enable analytics.
	<div style="display: flex; align-items: center;"> <p>If you disable analytics for a customer, the <i>Dashboard</i>, <i>View</i>, and <i>Reports</i> tabs will not be displayed to that customer. If you disable analytics when adding a new customer, the system allocates less storage space for the customer (100 MB).</p> </div>
Total Storage	Total number of MB of storage that this customer can use. The default value is 100 MB when <i>Enable Analytics</i> is selected.

Others

This pane allows you to configure other settings.

Others

Trusted Hosts Enable Disable

Policy Installation Scheduler: None Daily Weekly

Display Storage

Display Site

Comment-based Filter(s)

Name-based Filter(s)

Settings	Guidelines
Trusted Hosts	Enable or disable trusted hosts for this customer. For additional information about trusted hosts, see Customer Users on page 41 .
Policy Installation Scheduler	Enables you to schedule automatic policy installation at a particular time (daily or weekly). All the pending policy updates will be installed at the configured schedule. If you select <i>None</i> , the installation scheduler is not invoked for this customer. If you select <i>Daily</i> , select the installation time. If you select <i>Weekly</i> , select the day and time for the policy installation.
Display Storage	Select to display the storage.
Display Site	Select to display the customer site.
Comment-based Filter(s)	<p>Enter text in this field to find comments in a policy that start with that text. Those policies will be hidden from customer users.</p> <p>For example, if you enter <code>hide_</code>, all policies with comments that start with <code>hide_</code> will be hidden from this customer's users. This feature can be used to hide static routes in a policy from customer users.</p> <p>Comment-based filter also supports exact matching to hide a policy with the comment that matches the text you have entered.</p> <p>Note: Currently, comment-based filter only works with firewall policies.</p>
Name-based Filter(s)	<p>Enter text in this field to find object names that start with that text. All objects with names that start with the specified text will be hidden from customer users.</p> <p>For example, if you enter <code>hide_</code>, all objects with names that start with <code>hide_</code> will be hidden from this customer's users.</p> <p>Name-based filter also supports exact matching to hide an object with the name that matches the text you have entered.</p> <p>Note: The name-based filter works with objects in the <i>Objects</i> tab.</p>

Policy & Object Edit Permissions

This pane configures the policies and objects that a customer can modify.

Policies and objects will not be visible to the customer in the customer web interface unless you select them.

For example, if you select *Web Filtering*, a web filter object will display in the object tree and a web filter column will display in the *Policy* tab:

Policy & Object Edit Permissions

- All
- AntiSpam
- DLP Sensor
- Firewall Address
- Local Category
- Service
- Virtual IP
- DNS Filter
- Application Control
- DLP Filter RegEx
- Zone Interface
- Rating Overrides
- User
- Web Filtering
- AntiVirus
- Firewall Policy
- IPS Sensor
- Schedule
- User group
- Web Filter RegEx

Settings **Guidelines**

Policy and Object Permissions

Check boxes for Policies and Objects

You can select edit permissions for *All* policies and objects or select edit permissions for individual policies and objects:

AntiSpam, Application Control, AntiVirus, DLP Sensor, DLP Filter RegEx, Firewall Policy, Firewall Address, Zone Interface, IPS Sensor, Local Category, Rating Overrides, Schedule, Service, User, User group, Virtual IP, Web Filtering, Web Filter RegEx, and DNS Filter

Policy Tab Permissions

This pane determines which policy tabs are visible in the customer web interface. Select the check boxes for tabs that you want to make visible for this customer. Select *All* to make all of the tabs visible.

Policy Tab Permissions

- All
- Central NAT
- NAT64 Policy
- DoS Policy
- IPv6 Interface Policy
- Interface Policy
- NAT46 Policy
- IPv6 DoS Policy
- IPv6 Policy

Tab Permissions

This pane determines the tabs that are visible in the customer web interface. Select the check boxes for tabs that you want to make visible for this customer. Select *All* to make all of the tabs visible.

Tab Permissions

- All
- Dashboard
- Policy
- Audit Logs
- SD-WAN
- View
- Objects
- Device Manager
- Device Health
- Reports
- Additional Resources
- WiFi



You must include at least one of the following tabs: *Dashboard*, *Policy*, or *Objects*.

Widget Permissions

This pane determines the widgets that are available in the dashboard of the customer web interface.

Use the arrow keys to move the widgets from the left pane to the right pane (these widgets will appear in the dashboard for this customer). The double-arrow keys move the entire list.

Add or edit a customer

Widget Permissions

Available Widgets

- Top Countries
- Top Threats
- Top Sources
- Top Destinations
- Top Applications
- Policy Hits
- Remote Access Points

Selected Widgets

Add >
Add all >>
< Remove
<< Remove all



If you selected *Dashboard* in the *Tab Permissions* pane, you must select at least one widget for display in the dashboard.

ADOM Filter Permissions and Alias

This pane allows you to select the devices that will be listed for a customer in dropdown menus of devices.

Select the pen icon to give the device an alias for ADOM/Device/VDOM to prevent customers from knowing the MSSP configuration.

Adom Filter Permissions and Alias

Select All All Selected Not Selected

<input checked="" type="checkbox"/> 172.18.26.120/62 (test_name)	<input checked="" type="checkbox"/> 172.18.26.120/64 (test_name_2)
<input checked="" type="checkbox"/> 172.18.26.120/70-5 (test_name_3)	<input checked="" type="checkbox"/> 172.18.26.120/andrew1
<input checked="" type="checkbox"/> 172.18.26.120/test8	<input type="checkbox"/> FMG-1500b/root

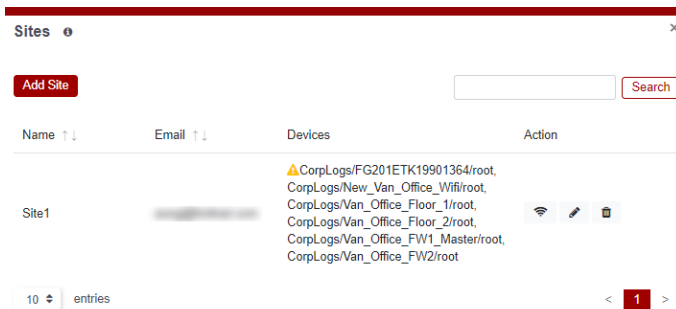
< 1 >

Customer sites

The *Customers* tab contains a set of action icons:

 — *Sites*, *Customer User(s)*, *Reports*, *Edit Customer*, and *Delete* respectively.

Selecting the *Sites* icon displays information about the customer sites. For each site, you see the name, devices, and email address of the site administrator:



Page actions

The *Sites* window contains the following actions:

- *Add Site*—open a dialog to add a site
- *Search*—enter text to search for site names containing that text
- *Show N entries*—filter the maximum number of sites to display in the page
- *Sort*—allows you to sort columns in ascending or descending order.

Per-site actions

The following icons are available in the *Action* column:

 — *Wireless Network*, *Edit*, and *Delete* respectively.

- *Wireless Network*—opens a window with a list of wireless networks for the selected site. See [Wireless Networks on page 39](#).
- *Edit*—opens a dialog to edit existing site data
- *Delete*—deletes the selected site

Selecting *Add Site* displays the *Add/Edit Site* dialogs (selecting the *Edit Settings* icon under *Actions* displays an identical form with fields supplied):

Add Site
✕

* Site Name

* Contact Name

* Email

Phone

Select All
 All
 Selected
 Not Selected



<input checked="" type="checkbox"/> 62/FGT60FTK19040995/root (test) ✎	<input type="checkbox"/> 64/FGVM08TM20003381/root ✎
<input type="checkbox"/> 70-5/FGVM08TM20003630/vdom4 ✎	<input type="checkbox"/> 70-5/FGVM08TM21000891/root ✎
<input type="checkbox"/> andrew1/FGVM08TM20003891/root ✎	<input type="checkbox"/> test8/FGVM08TM21001075/root ✎
<input type="checkbox"/> test8/FGVM08TM21001075/vdom1 ✎	

<
1
>

Enable sandbox for all selected devices

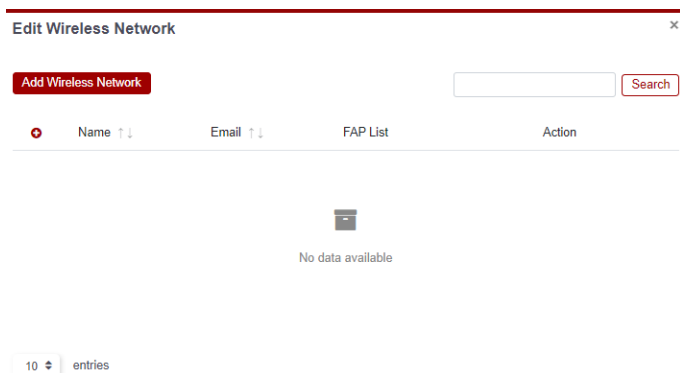
Save
Cancel

The dialogs contain the following fields:

Settings	Guidelines
Site Name	Name for the Site, which must be unique across this customer's sites
Contact Name	Name and email of the customer contact for this site
Email	
Phone	
Device List	<p>Select the devices to associate with this site. Ensure that you add only the devices with the correct ADOM for this customer.</p> <p>Use the search box to filter the choices available.</p> <hr/> <div style="display: flex; align-items: center; border-bottom: 1px solid #ccc;"> <div style="flex: 1; text-align: center; padding: 10px;">  </div> <div style="flex: 2; padding: 10px;"> <p>Select the pen icon to give the device an alias for ADOM/Device/VDOM to prevent customers from knowing the configuration.</p> </div> </div> <hr/>
Enable sandbox for all selected devices	<p>Set this option if you want to enable sandbox capability for all of the selected devices.</p> <hr/> <div style="display: flex; align-items: center; border-bottom: 1px solid #ccc;"> <div style="flex: 1; text-align: center; padding: 10px;">  </div> <div style="flex: 2; padding: 10px;"> <p>An extra license is required for each device that you enable with sandbox.</p> </div> </div> <hr/>

Wireless Networks

Selecting the *Wireless Network* icon on the *Sites* window displays the *Wireless Networks* window for a given site. This window displays information about the site's wireless networks (network name, FAP list, email of the administrator):



From this window, you can add wireless networks to the site, edit a site, and edit the list of associated Fortinet Access Points.

Page actions

In this window, the following actions are available:

- *Add Wireless Network*—open a dialog to add a wireless network
- *Search*—enter text to search by network name, device or email
- *Show N entries*—filter the maximum number of wireless networks to display in the page
- *Sort*—allows you to sort columns in ascending or descending order.

Selecting *Add Wireless Network*, displays a dialog for adding a new network (fields in the form are blank).

Per-network actions

When you scroll over a entry in the wireless network table, the following icons appear in the Action column:

- *Edit*—opens a dialog to edit the wireless network data
- *Delete*—deletes the selected wireless network

Selecting the *Edit* icon displays the *Edit Wireless Network* dialog, which is identical to the *Add Wireless Network* dialog except that the fields are filled:

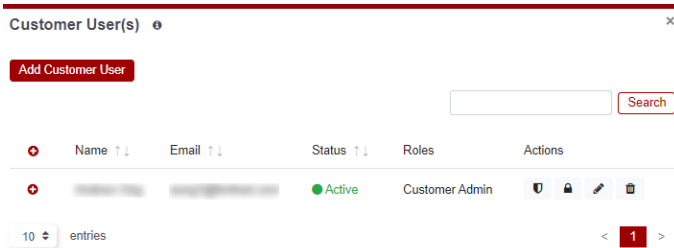
When you add or edit a wireless network, the dialog contains the following fields:

Settings	Guidelines
Wireless Network Name	Name for the wireless network
Contact Name	Name and email of the customer contact for this network
Email	
Phone	
Available Devices	Lists of discovered wireless AP devices Use the search box to filter the choices available.
Selected Devices	Select the wireless AP devices to associate with this network. Use the search box to filter the choices available.

Customer Users

Selecting the *User(s)* icon on the *Customer* tab displays the *Customer User(s)* window, which displays information about the local administrative users configured for this customer.

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



Page actions

In this window, the following actions are available:

- *Add Customer User*—opens a dialog to add a user
- *Search*—enter text to search for user names containing that text
- *Show N entries*—filter the maximum number of users to display in the page
- *Sort*—allows you to sort columns in ascending or descending order.

Per-user actions

When you scroll over a entry in the users list, the following icons appear in the Action column:

- —opens a dialog to add/edit data for existing users
- —deletes this user
- —opens a dialog to add a trusted-host entry for this customer
- —opens a dialog to change the password for this customer

Add Customer User ✕

* First Name

* Last Name

* Email

* Password

* Confirm Password

* Password Policy
 Enable Disabled

▼ Contact Info

Address1

Address2

City

State

Country

Zip

Phone

Fax

Available Roles

search

Customer Admin

Add >
Add all >>
< Remove
<< Remove all

Selected Roles

search

Available Sites

search

Site1

Add >
Add all >>
< Remove
<< Remove all

Selected Sites

search

* Status
 Active Disabled

Save **Cancel**

The *Add Customer User* and *Edit Customer User* dialogs contain the following fields:

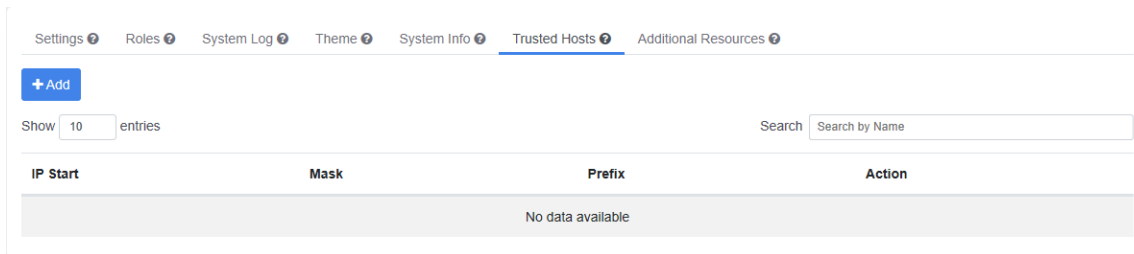
Settings	Guidelines
First Name Last Name	Name of the user
Email Password Confirm Password	Email and password for the user. The user will use these credentials to access the customer portal.
Password Policy	Enable or disable. If enabled, you can set one or more of the following types of character that the password must contain: <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.
Address1 Address2 City State Country Zip	Business address for the user
Phone Fax	Phone and fax number for the user
Available Roles	Roles that are available for this user type. You can specify multiple roles for a user.
Selected Roles	Selected roles for this user
Available Sites	Sites that are available for this user to access.
Selected Sites	Sites that this user can access. You can specify multiple sites for a user. If no site is selected, the user has access to all sites.
Status	Select whether the customer user is <i>Active</i> or <i>Disabled</i> .

Add a trusted host for a user

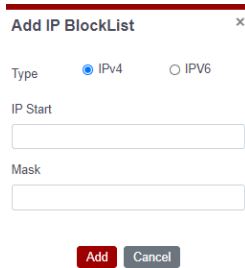
If you have enabled the Trusted Host option for this customer, the system creates a allowlist of trusted hosts for the customer users. The default entry in the allowlist is to allow all users, so you need to edit/delete this entry to create a valid allowlist.

Select the *Trusted Hosts* tab to open the allowlist for this customer.

Go to *Admin > Trusted Hosts* to open the allowlist for this customer.



Select *Add* to create an IP address blocklist for this customer.



The *Add IP BlockList* and *Edit IP BlockList* dialogs contain the following fields:

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.
:Prefix	Define the range of IP addresses covered by this entry.

Customer user roles

User roles enable you to authorize each customer 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 Customer 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 customer.

The system provides a set of default customer user roles. You can also create new roles or customize the default roles using the Roles page. See [Roles on page 77](#).

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 Customer Portal for that customer. Because this role is far-reaching, we recommend that you assign this role to a limited number of users.

- All of the customer roles provide read-write access to the dashboard.
- All of the "Read" roles provide read access to all of the customer 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.

To provide a customer user with read-write access to a specific object or policy, you must set the corresponding write permission for this customer in the Customer data. Refer to *Policy and Object Permissions* in [Add or edit a customer on page 30](#).

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 Customer Portal for that customer
Schedule Report Read	Read access to the Report Definitions page
Schedule Report Write	Read access to the Report Definitions page and allows the user to add or edit a customer-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

Reports

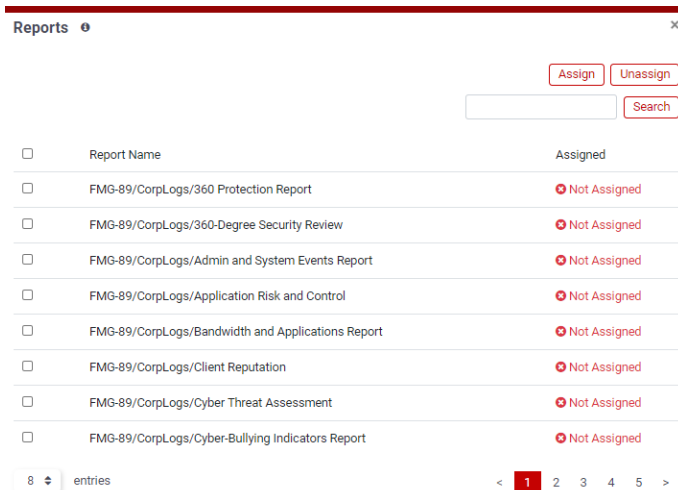
The administrator can create reports for the customer. Similarly, the customer can also create reports. The ability (for a specific customer user) to create reports or run reports is based on the roles assigned to that user. For additional information, refer to [Customer Users on page 41](#).

When you select the Reports icon from the Action column of the *Customers* tab, the *Reports* window displays information about the reports that are available to this customer.

In the *Admin > Settings* tab, you specify the maximum number of reports (*Max Reports Allowed*) that can be defined for this customer. This number includes customer-defined reports and reports added by the administrator. If you try to add a report beyond the maximum number for this customer, the system displays an error message.

FortiAnalyzer reports

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



Page actions

The *Reports* window contains the following actions:

- *Show x entries*—sets the number of entries that are displayed (8, 25, 50, or all)
- *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



- 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.
-

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	Action
FMG-126	192.168.1.126	Primary	Green	Expand, Hide, Edit, Delete
FMG-224	192.168.1.224	Stand Alone	Green	Expand, Hide, Edit, Delete
FMG-230	192.168.1.230	Stand Alone	Green	Expand, Hide, Edit, Delete
FMG-242	192.168.1.242	Stand Alone	Green	Expand, Hide, Edit, Delete
FMG-244	192.168.1.244	Stand Alone	Green	Expand, Hide, Edit, Delete
SOWAN1	192.168.1.1	Stand Alone	Red	Expand, Hide, Edit, Delete

Page actions

In this tab, the following actions are available:

- *Add FortiManager*—opens a dialog to add a FortiManager
- *Show x entries*—sets the number of entries that are displayed at once (10, 20, 50, or All)
- *Search*—enter text to search for FortiManager names containing that text. You can also search by IP address
- *Sort*—allows you to sort columns in ascending or descending order.

Per-FortiManager actions

For every entry in the FortiManager list, the following icons appear in the Action column:

- *Expand*—select the button to view a list of the devices managed by this FortiManager
- *Hide*—select the button to hide the devices managed by this FortiManager
- *Edit*—select to open a dialog to edit the FortiManager data
- *Delete*—select to delete the FortiManager
- *Poll Now*—select to poll the FortiManager
- *Change Password*—select to change the password for the FortiManager

FortiManager high availability (HA)

A FortiManager HA cluster consists of an active primary unit, and up to four standby secondary units. If the primary unit becomes unavailable, one of the standby secondaries will become the new primary.

In most situations, the FortiPortal provides access to the primary FortiManager in the HA cluster. Configuration changes in the primary will be synchronized to the secondary units. If no primary exists, the FortiPortal provides read-only access to the secondary units.

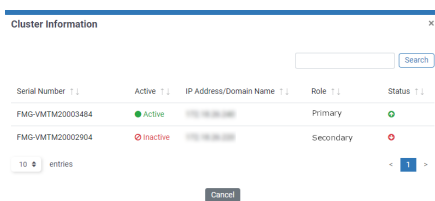


When a FortiManager unit with an HA configuration is added to FortiPortal, FortiPortal must be able to reach all the IP addresses that are part of the FortiManager HA cluster (including the secondary). If FortiPortal cannot reach the secondary IP address, FortiPortal cannot detect the HA switchover.

In the FortiManager table, the Mode includes the following values:

- *Standalone*—the FortiManager is independent of a high-availability cluster
- *Primary*—the FortiManager is the primary in a high-availability cluster
- *Secondary*—the FortiManager is a secondary in a high-availability cluster

Select the *HA* icon to display information about the FortiManagers in this HA cluster:



The *Cluster Information* window provides the following information for each FortiManager in the cluster:

Field	Description
FortiManager SN	Serial number of the FortiManager
Active	Displays green arrow for an active FortiManager or a red x for an inactive FortiManager
IP Address	IP address of the FortiManager
Role	The role is Primary or Secondary.
Status	Indicates whether the FortiManager is operational

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. Select *Add FortiManager*.

2. Input the fields, as described in the table in the next section.

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. Select the *Edit* button (in the Action column).
2. Input the fields, as described in the table below.
3. Select *Save*.

The following table contains descriptions of the fields:

Field	Description
FortiManager Name	A name for the FortiManager. The name must be unique within this FortiPortal.
IP Address/Domain Name	Enter the IP address or domain name of the FortiManager
Admin Username	User name for a valid FortiManager administrative user
JSON Port	Port number to use to connect with the FortiManager. The default for JSON is 443.
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, Monthly.
Last Poll Time	Read-only field. Indicates when the FortiPortal last polled this FortiManager device.

Manage FortiGate devices

Selecting the  button on the *FortiManager* tab displays a list of the FortiGate devices managed by this FortiManager. The system displays an additional search box, for searching within the list of devices.

For each device, the system displays the following fields and action buttons.

- *Device*—name of the managed FortiGate device
- *Status*—status of the device
- *Customer Name*—the customer name
- *Wireless*—indicates whether this FortiGate device is functioning as a wireless controller. Selecting *Edit* displays the *Edit Wireless Controllers* pane. Select the *Wireless* check box if you want to convert the device into a wireless controller. Select the polling frequency to control how often the device is checked.
- *Action*—includes *Edit* option that allows editing wireless controllers.

Device	Status	Customer Name	Wireless	Action
CorpLogs/FG201ETK19901364/root	Active	Customer-230		Cancel

Edit Wireless Controllers

Wireless

Controller Name

ADOM

VDom

IP Address/Domain Name

Serial Number

Polling Frequency

Save

The system displays a cluster icon to represent a FortiGate cluster. Hovering over the icon displays the list of individual FortiGate units in the cluster (see the following figure):

Devices (FMG-230)

Search by All

Device	Status	Customer Name	Wireless	Action
ADOM1/FGT61F-V64/root	Active	Customer-230		Disable
ADOM1/FWF61E-V64/root	Active	Customer-230		Disable
CorpLogs/New_Van_Office_Wifi/root	Active			Disable
CorpLogs/Van_Office_Floor_1/root	Active			Disable
CorpLogs/Van_Office_FW1_Master/root	Active			Disable
CorpLogs/Van_Office_FW2/root	Active			Disable
HA-v56/fgt56-ha-2/root	Active			Disable
HA-v60/fgt60-ha-2/Secondary - FGVM32TM19000367	Active			Disable
HA-v60/FWF-61E-kding/root	Active			Disable
HA-v62/fgt62-ha-1/root	Active			Disable

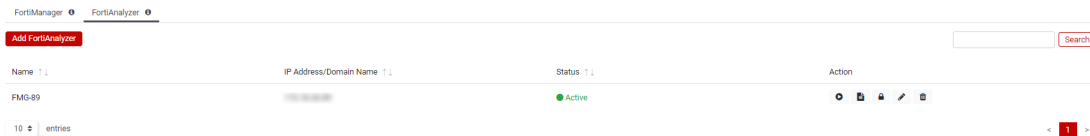
10 entries



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. The name of the Security Fabric they belong 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 customers. Refer to the *Reports* window in the *Customers* tab. The list displays the FortiAnalyzer name, the IP address, and the status for each FortiAnalyzer:



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:

- *Add FortiAnalyzer*—opens a dialog to add a FortiAnalyzer device. To use FortiAnalyzer mode, you must be running FortiAnalyzer 6.0 or later
- *Show x entries*—sets the number of entries that are displayed at once (10, 20, 50, or All)
- *Search*—enter text to search with FortiAnalyzer names
- *Sort*—allows you to sort columns in ascending or descending order.

Per-FortiAnalyzer actions

For every entry in the FortiAnalyzer list, the following icons appear in the Action column:

- *Edit*—opens a dialog to edit the FortiAnalyzer data
- *Delete*—deletes the selected FortiAnalyzer
- *Poll Now*—polls the FortiAnalyzer to obtain the most recent data
- *Reports*—displays a list of FortiAnalyzer reports
- *Change Password*—select to change the password for the FortiAnalyzer

Edit a FortiAnalyzer

To edit the FortiAnalyzer:

1. Select the *Edit* button (in the Action column).
2. Change the fields as needed; see the field descriptions in the table.
3. Select *Save*.

The following figure shows the dialog to edit a FortiAnalyzer:

Edit FortiAnalyzer: FAZ_211 ✕
 * Name:
 * IP Address/Domain Name:
 * Admin Username:
 * ports:
 Polling Frequency:
 Last Poll Time:

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.
IP Address/Domain Name	Enter the IP address or domain name of the FortiAnalyzer.
Admin Username	User name for the FortiAnalyzer user assigned to this FortiPortal.
Password	Password for the FortiAnalyzer user assigned to this FortiPortal.

Settings	Guidelines
ports	Port number to use to connect with the FortiAnalyzer. The default for JSON is 443.
Polling Frequency	How often the FortiPortal will poll FortiAnalyzer to update the device information. The default value is one day. The polling frequency is not configurable.
Last Poll Time	The most recent time that FortiPortal polled FortiAnalyzer.

View FortiAnalyzer reports

When you select the *Reports* icon for a FortiAnalyzer in the list, FortiPortal opens a pane:

FortiAnalyzer Reports (FMG-89) ✕

Search

Report Name	Customer Name
CorpLogs/360 Protection Report	
CorpLogs/360-Degree Security Review	
CorpLogs/Admin and System Events Report	
CorpLogs/Application Risk and Control	
CorpLogs/Bandwidth and Applications Report	
CorpLogs/Client Reputation	
CorpLogs/Cyber Threat Assessment	
CorpLogs/Cyber-Bullying Indicators Report	

8 entries < 1 2 3 4 5 >

Admin settings

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

The following figure shows the *Settings* tab (with authentication set to remote and RADIUS as the remote server):


The screenshot displays the FortiPortal Settings interface with the following sections and configurations:

- Administration Settings:**
 - FPC Data Store Size: 1000 GB
 - Session Timeout: 30 (15-3240 Minutes)
 - Trusted Host: Enable Disable
- Email Settings:**
 - SMTP Server: exch-cas.fortinet.com
 - Port: 25
 - Email From: aong@fortinet.com
 - Authentication: Enable Disable
- Remote Log Server:**
 - Primary Server: [Empty]
 - Primary Port: [Empty]
 - Secondary Server: [Empty]
 - Secondary Port: [Empty]
- Other:**
 - Load Balancer Domain/IP Address: [Empty]
 - Load Balancer Port: 443
 - Max Reports Allowed: 6
 - Alert Email From: [Empty]
 - Alert Email To: [Empty]
 - Language: English
 - Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, Li
 - TLS/SSL Versions: TLSv1.2 TLSv1.1 TLSv1.3
 - FortiManager HA polling frequency: Every 5 Minutes
- User Authentication:**
 - Authentication Access: Local Remote
 - Allow Service Provider Usernames without Domain: Enable Disable
 - Remote Server: RADIUS
 - Domains: Select...
 - View/Change Radius Roles: [View Radius Roles](#)
 - Remote Server IP Address: [Empty]
 - Remote Server Port: [Empty]
 - Remote Server Key: [Empty]
 - Authentication Protocol: CHAP

Buttons: [Submit](#) [Reset](#)

The following table describes the settings:

Settings	Guidelines
Administration Settings	
FPC Data Store Size	Required. Amount of database storage (in GB) to reserve for the portal DB
Session Timeout	Required. Timeout for user sessions on the Administrative or Customer web interfaces. The default is 30 minutes. The range is 15-3240 minutes.
Trusted Hosts	Select <i>Enable</i> or <i>Disable</i> . When enabled, you can create a allowlist of originating IP subnetworks; only log-in requests from these subnetworks will be allowed. The system also provides a blocklist, for blocking rogue log-in attempts.
Email Settings	
SMTP Server	Required. URL of the SMTP serve from which FortiPortal sends emails
Email From	Required. Email address. Emails sent from FortiPortal will originate from this address.
Port	Required. Email server port. The default value is 25.
Authentication	Enable or disable authentication. If you enable authentication, enter a user name and password. You can use special characters in the user name.
Remote Log Server	
Primary Server	Primary log server IP address
Primary Port	Primary log server port number (mandatory if the server address is supplied)
Secondary Server	Secondary log server IP address
Secondary Port	Secondary log server port number (mandatory if server address supplied)
Other	
Load Balancer Domain/IP Address	Load balancer IP address or domain name, if you have configured multiple instances of the Apache Tomcat server.
Load Balancer Port	Load balancer port number (required if you specified a load balancer IP address, not required for a domain name). The default value is 443.
Max Reports Allowed	Maximum number of reports that can be defined for this customer. This number includes customer-defined reports and also any reports that the administrator has defined for this customer.
Alert Email From	Alert emails will be sent from this email address.
Alert Email To	Alert emails will be sent to this email address.
	 <p>If the storage is close to the allocated limit, an alert notification is sent to this email address.</p>
Language	Desired language (default, English) If you change the language, save the settings and log out. The change takes effect upon subsequent logins.

Settings	Guidelines
Time Zone	Select the appropriate time zone to use.
TLS/SSL Versions	Select which TLS/SSL versions are used.
User Authentication	
Authentication Access	<p>Select <i>Local</i> or <i>Remote</i>.</p> <p>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 customer user for each end-customer user.</p> <p>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 <i>cannot</i> be used when remote authentication is selected. See Remote authentication using FortiAuthenticator on page 57, RADIUS server configuration on page 59, and Remote authentication - SSO on page 62. If you select <i>RADIUS</i> or <i>SSO</i> as the remote server, the system displays the <i>View Roles</i> button. Select this button to map the RADIUS (RADIUS Roles on page 60) or SSO (SSO Roles on page 64) roles with the local roles.</p> <p>If you select <i>RADIUS</i> as the remote server, the <i>Authentication Protocol</i> dropdown allows you to choose between CHAP or PAP authentication protocols.</p> <hr/> <div style="display: flex; align-items: center;">  <p>When you change the authentication configuration from local to remote or from remote to local, you must restart FortiPortal.</p> </div> <hr/>

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:

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 > Remote*, 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.

User Authentication

Authentication Access Local Remote

* Allow Service Provider Usernames without Domain Enable Disable

* Remote Server

Domains

* Remote Server IP Address

* Remote Server Port

* Remote Server Key

* Remote Server User

The following table describes the remote authentication fields:

Settings	Guidelines
Allow Service Provider Usernames without Domain	Enable or disable. If you enable this field, the user can enter the 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.
Remote Server	Select <i>FortiAuthenticator</i> .
Domains	The site administrator may allow administrative users to be defined in more than one domain. Enter a domain and then select the + button. The new domain appears in the list below the entry box.
Remote Server IP Address	IP address of the authentication server

Settings	Guidelines
Remote Server Port	Port for the authentication server (default is 443)
Remote Server Key	Secret key for REST API requests
Remote Server User (FortiAuthenticator only)	Administrator user name for the authentication server. This user must have sufficient permission to initiate REST API requests.

To configure FortiPortal:

1. Go to *Admin > Settings*.
2. For Authentication Access, select *Remote*.
3. In the Remote Server drop-down menu, select *FortiAuthenticator*.
4. In the Remote Server Key field, paste the REST API key that you received in email (see step 3 in “[Configuring FortiAuthenticator](#)”).
5. In the Remote Server Port field, enter 443.
6. In the Remote Server User field, enter the name of the admin user from step 1 of “[Configuring FortiAuthenticator](#).”
7. In the Domains field, add the domain for the administrator user. For example, if the administrator user is `abc@test.com`, add `test.com` in the Domains field.

User Authentication

Authentication Access Local Remote

* Allow Service Provider Usernames without Domain Enable Disable

* Remote Server

Domains

* Remote Server IP Address

* Remote Server Port

* Remote Server Key

* Remote Server User

8. Select **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

```

- 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
```

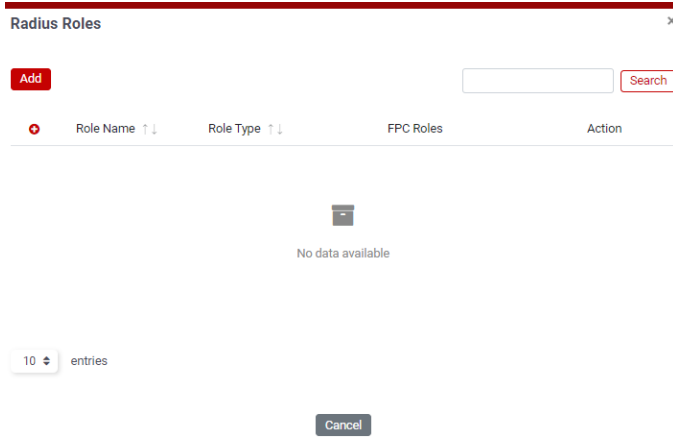


A user will not be able to login to FortiPortal if the roles are not configured on the RADIUS server.

- 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
- 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

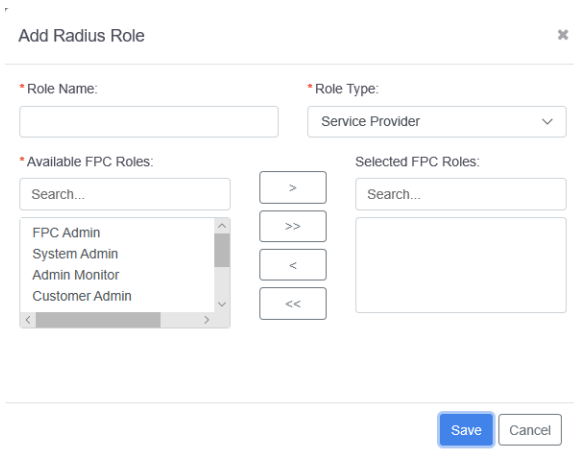
RADIUS Roles

Selecting the *View Radius Roles* button on the *User Authentication* pane 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 type (Service Provider or Customer) and a list of FortiPortal roles that map to the RADIUS role.



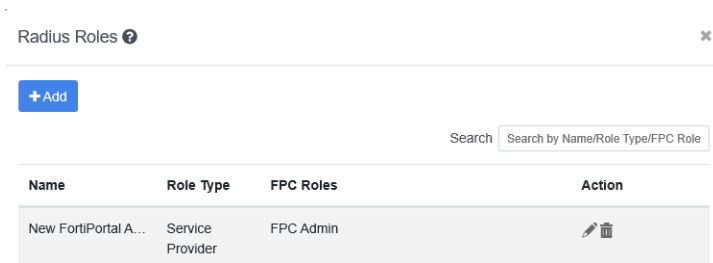
The *RADIUS Roles* window contains the following actions:

- *Add*—open a dialog to add a RADIUS role (see immediately below)
- *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 (10, 25, 30, or 50).
- *Sort*—allows you to sort columns in ascending or descending order.



When you scroll over a entry in the RADIUS role list, the following icons appear in the Action column:

- *Edit*—opens a dialog to edit an existing RADIUS role (see below)
- *Delete*—deletes the selected RADIUS role



The *Add Radius Role* and *Edit Radius Role* dialogs contain the following fields:

Settings	Guidelines
Role Name	Names the RADIUS role. The name must match a role name in the RADIUS server.
Role Type	Service Provider or Customer
Available FPC Roles:	Lists of available FortiPortal roles Use the search box to filter the choices available.
Selected FPC Roles	Selects the FortiPortal roles to associate with this RADIUS role Use the search box to filter your selected choices.

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.

If you select SSO as the remote server type, the system displays additional settings to configure:

User Authentication

Authentication Access Local Remote

* Allow Service Provider Usernames without Domain Enable Disable

* Remote Server

Domains

View/Change SSO Roles [View SSO Roles](#)

* SSO IDP Entity URL

* IDP Sign On Service Post Endpoint URL

* IDP Sign On Service Redirect Endpoint URL

* SSO Application ID

* SSO Audience URL

* Role Attribute

Tenant Identification Attribute


SSO Error URL


IDP Logout Service Endpoint

* SSO Certificate

Site Attribute

For SSO, FortiPortal supports Service Provider-initiated or Identity Provider-initiated SAML authentication. The following table describes the SSO authentication fields:

Settings	Guidelines
Allow Service Provider Usernames without Domain	Enable or Disable. 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.
Remote Server	SSO When you select SSO as the remote server, the system displays the <i>View SSO Roles</i> button. Select this button to map the SSO roles (SSO Roles on page 64) with the local roles.
Domains	Enter a domain, URL, or URN attribute and then select the + button. The new domain appears in the list below the entry box. If you do not want to provide a domain for the site administrator, select <i>Enable</i> for 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 a customer, see Add or edit a customer on page 30 .
	 <p>The site administrator may allow administrative users to be defined in more than one authentication domain.</p>
SSO IDP Entity URL	IDP Entity URL (ID) or URN for SAML provided by IDP server
IDP Sign On Service Post Endpoint URL	Endpoint URL for IDP (Post) provided by IDP Server
IDP Sign On Service Redirect Endpoint URL	Endpoint URL for IDP (Redirect) provided by IDP Server
SSO Application ID	SSO application provided by IDP
SSO Audience URL	URL used for audience within assertion (format: <code>https://<FPC_PORTAL>/fpc/saml/SSO</code>)
Role Attribute	Attribute parameter name that maps to the corresponding role in FortiPortal
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.

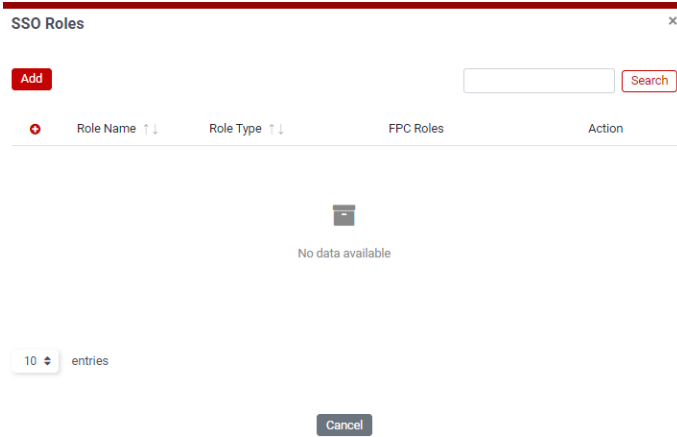
Settings	Guidelines
	<p>If you configure "My Customer Id" as the attribute value, FortiPortal expects the following in the authentication response from the SSO server:</p> <pre data-bbox="557 342 1182 369"><My Customer Id>Fortinet</My Customer Id></pre> <p>where Fortinet is the value returned by the SSO server.</p> <p>This value must have been supplied to the "Domains" field in the Customer Add/Edit screen.</p> <p>For a RADIUS server, the Tenant Identification Attribute value is a Fortinet Vendor Attribute value. The server will send "Fortinet" in the authentication response.</p> <hr/> <div data-bbox="609 657 690 762" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="738 678 1398 741" style="display: inline-block; vertical-align: middle;"> <p>FortiPortal treats the attribute values from either RADIUS or SSO server equally.</p> </div> <hr/>
SSO Error URL	(Optional) Error URL provided by IDP
IDP Logout Service Endpoint	(Optional) IDP logout URL provided by IDP
SSO Certificate	Certificate provided by IDP used by SP to decrypt the signed response
Site Attribute	<p>Attribute parameter name that specifies which sites the customer user can access.</p> <p>For example, an attribute name of "site" might have the values "site1" and "site2". A customer user assigned to "site" would be able to access "site1" and "site2".</p> <pre data-bbox="557 1129 1365 1339"><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></pre>

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

```
https://<Portal>/fpc/adminuser/login
```

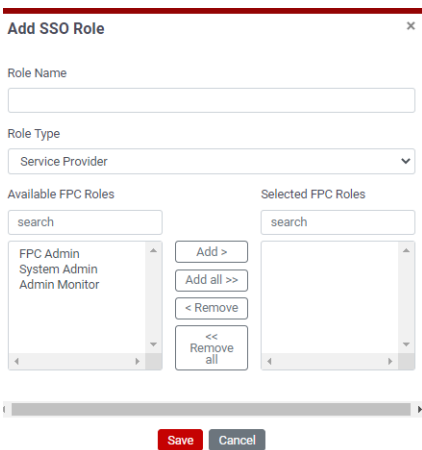
SSO Roles

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



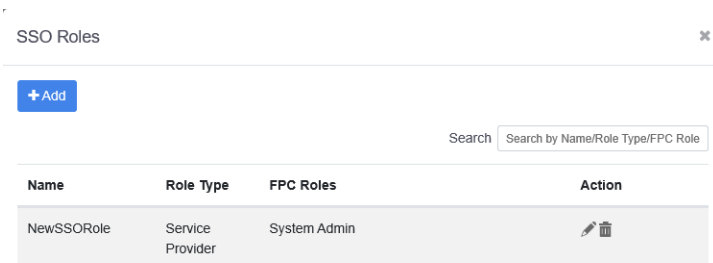
The *SSO Roles* window contains the following actions:

- **Add**—open a dialog to add an SSO role (see immediately below)
- **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 (10, 25, 30, or 50).
- **Sort**—allows you to sort columns in ascending or descending order.



When you scroll over a entry in the SSO role list, the following icons appear in the Action column:

- **Edit**—opens a dialog with the form to edit an existing SSO role (see below)
- **Delete**—deletes the selected SSO role



The *Add SSO Role* and *Edit SSO Role* dialogs contain the following fields:

Settings	Guidelines
Role Name	Names the SSO role. The name must match a role name in the SSO server.
Role Type	Service Provider or Customer
Available FPC Roles:	Lists of available FortiPortal roles Use the search box to filter the choices available.
Selected FPC Roles	Selects the FortiPortal roles to associate with this SSO role Use the search box to filter your selected choices.

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 *Admin > Settings*.
3. In the User Authentication section, select *Remote* for Authentication Access and *SSO* for Remote Server.
4. In the Tenant Identification Attribute field, enter `FPC_Tenant`.
5. Fill out the rest of the fields and select *Save*.
6. Go to *Customers* and select *Add*.
7. In the Domains field, enter `Local.com` and select *+*.
8. Fill out the rest of the fields and select *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)?

Use the following procedure to select the Role Type to make sure the right roles are mapped:

1. Go to *Admin > Settings*.
2. In the User Authentication area, select *Remote* for Authentication Access.
3. Select *SSO* for the Remote Server.
4. Select *View SSO Roles*.
The SSO Roles window opens.
5. Select *Add*.
6. In the Add SSO Role window, enter the Role Name (This name must be an SSO role.) and then select the *Role Type*.
7. Select one or more roles from the *Available FPC Roles* box. Select *>* to move the roles to the Selected FPC Roles box.
8. Select *Save* to save your changes.

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

The site administrator can create different roles on FortiPortal by going to *Admin > Roles* and selecting *Add*. 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 customer level.

These permission groups can be created from the UI by going to *Admin > Roles*.

Name	Role Type	Permissions	Type	Action
Admin Monitor	Service Provider	Additional Resources-Read-Only,AddressObject-Read-Only,AntiVirusObject-Read-Only,ApplicationSensor...	Default	
Customer Admin	Customer	Additional Resources-Read-Only,AddressObject-Read-Write,AntiVirusObject-Read-Write,ApplicationSens...	Default	

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 customer users.

During authentication, the FortiPortal unit needs to identify whether each user is an administrator or a customer 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 a customer or an administrator. Based on that mapping, the system displays the correct UI.

If the Tenant Identification attribute is configured in *Admin > Settings* and is provided in the SAML assertion, the value in the Tenant Identification Attribute field is used to match the domain name provided in the MSSP settings or in the Add Customer or Edit Customer page. If the domain provided does not match any MSSP or customer domains, an error message is displayed.

If the Tenant Identification attribute is not configured in *Admin > Settings* 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 the Tenant Identification Attribute field.

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

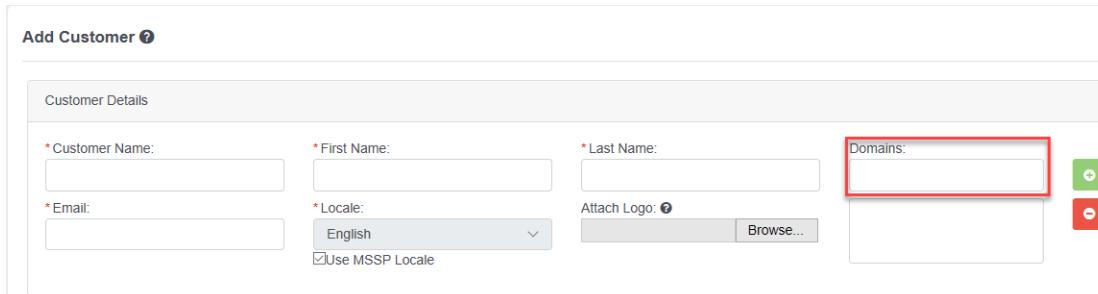
The Tenant ID attribute value is processed from the IDP response, and the value is mapped with the domain name field in the FortiPortal unit. For example, if tenant ID is map_id, FortiPortal gets the respective value for the map_id attribute from the SAML response and maps that value with the domain name listed in Add Customer or Edit Customer form or

the *Admin > Settings* form. If the value matches with the customer domain name, the user is granted access to the customer. If the value matches with the domain name in the *Admin > Settings* form, FortiPortal loads the administrator UI.

How can I add a domain name to the customer?

A unique domain name identifies the customer. You can add the domain name to the customer when you add a customer or edit the customer. In the Add/Edit Customer window, there is the Domains field. Enter the domain name and select the + icon to add the name to the domain list.

The administrator can add more than one domain to a customer.



The screenshot shows the 'Add Customer' form with the following fields and controls:

- Customer Name:** Text input field.
- First Name:** Text input field.
- Last Name:** Text input field.
- Domains:** Text input field, highlighted with a red box.
- Email:** Text input field.
- Locale:** Dropdown menu with 'English' selected.
- Attach Logo:** Button with a plus icon and a 'Browse...' button.
- Use MSSP Locale:** Checked checkbox.
- Buttons:** A green '+' button and a red '-' button are located to the right of the Domains field.

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

After you select FortiSSO/FortiAuthenticator/FortiRADIUS as a remote server in the Settings page, you will see an option for the domain field.

SNMP

Enable the SNMP agent on the FortiPortal device so it can send traps to and receive queries from the computer that is designated as its SNMP manager. This allows for monitoring the FortiPortal with an SNMP manager.

SNMP has two parts—the SNMP agent that is sending traps, and the SNMP manager that monitors those traps. The SNMP communities on monitored FortiGate devices are hard coded and configured by the FortiPortal system—they are not user configurable.

The FortiPortal SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP manager applications, such as those on your local computer, have read-only access to FortiPortal system information and can receive FortiPortal system traps.

SNMP agent

The SNMP agent sends SNMP traps originating on the FortiPortal system to an external monitoring SNMP manager defined in a SNMP community. Typically an SNMP manager is an application on a local computer that can read the SNMP traps and generate reports or graphs from them.

The SNMP manager can monitor the FortiPortal system to determine if it is operating properly, or if there are any critical events occurring. The description, location, and contact information for this FortiPortal system will be part of the information an SNMP manager will have — this information is useful if the SNMP manager is monitoring many devices, and it will enable faster responses when the FortiPortal system requires attention.

To set up an SNMP agent, use the following CLI syntax:

```
config system snmp sysinfo
  set status {enable | disable}
  set description <description>
  set engine-id <string>
  set fortianalyzer-legacy-sysoid {enable | disable}
  set location <location>
  set contact-info <string>
  set trap-high-cpu-threshold <percentage>
  set trap-low-memory-threshold <percentage>
  set trap-cpu-high-exclude-nice-threshold <percentage>
end
```

Variable	Description
status {enable disable}	Enable/disable the SNMP agent. Default: disable.
description <description>	Enter a description of this FortiPortal system to help uniquely identify this unit. Character limit: 35.
engine-id <string>	Local SNMP engine ID string. Character limit: 24.

Variable	Description
fortianalyzer-legacy-sysoid {enable disable}	Enable the legacy FortiAnalyzer sysObjectOID.
location <location>	Enter the location of this FortiPortal system to help find it in the event it requires attention. Character limit: 35.
contact-info <string>	Enter the contact information for the person in charge of this FortiPortal system. Character limit: 35.
trap-high-cpu-threshold <percentage>	CPU usage when trap is set. Default: 80.
trap-low-memory-threshold <percentage>	Memory usage when trap is set. Default: 80
trap-cpu-high-exclude-nice- threshold <percentage>	CPU high usage excludes nice when the trap is sent.

Example

This example shows how to set up an SNMP agent, and add basic SNMP information.

```
config system snmp sysinfo
  set status enable
  set contact-info 'System Admin ext 245'
  set description 'Internal network unit'
  set location 'Server Room A121'
end
```

SNMP v1/v2c communities

An SNMP community is a grouping of equipment for network administration purposes. You must configure your FortiPortal to belong to at least one SNMP community so that community's SNMP managers can query the FortiPortal system information and receive SNMP traps from it.



These SNMP communities do not refer to the FortiGate devices the FortiPortal system is managing.

Each community can have a different configuration for SNMP traps and can be configured to monitor different events. You can add the IP addresses of up to eight hosts to each community. Hosts can receive SNMP device traps and information.

To create an SNMP community, use the following CLI syntax:

```
config system snmp community
  edit <index_number>
    set status {enable | disable}
    set name <community_name>
```

```

set query-v1-port <integer>
set query-v1-status {enable | disable}
set query-v2c-port <integer>
set query-v2c-status {enable | disable}
set trap-v1-rport <integer>
set trap-v1-status {enable | disable}
set trap-v2c-rport <integer>
set trap-v2c-status {enable | disable}
set events <events_list>
config hosts
  edit <host_number>
    set interface <interface_name>
    set ip <ipv4_address>
  end
end

```

Variable	Description
<index_number>	Enter the index number of the community in the SNMP communities table. Enter an unused index number to create a new SNMP community.
status {enable disable}	Enable/disable this SNMP community. Default: <i>enable</i> .
name <community_name>	Enter a name to identify the SNMP community. Note: This name cannot be edited later.
query-v1-port <integer>	Enter the SNMPv1 query port number the FortiPortal unit uses to send a v1 query to the FortiPortal unit in this community. Note: By default, the SNMPv1 query port number is 161. Range: 1 to 65535.
query-v1-status {enable disable}	Enable/disable SNMPv1 queries for this SNMP community. Default: <i>enable</i> .
query-v2c-port <integer>	Enter the SNMPv2c query port number the FortiPortal unit uses to send a v2c query to the FortiPortal unit in this community. Note: By default, the SNMPv2c query port number is 161. Range: 1 to 65535.
query-v2c-status {enable disable}	Enable/disable SNMPv2c queries for this SNMP community. Default: <i>enable</i> .
trap-v1-rport <integer>	Enter the remote port number the FortiPortal unit uses to send v1 traps to the FortiPortal unit in this community. Note: By default, the remote port number is 162. Range: 1 to 65535.
trap-v1-status {enable disable}	Enable/disable SNMPv1 traps for this SNMP community. Default: <i>enable</i> .
trap-v2c-rport <integer>	Enter the remote port number the FortiPortal unit uses to send v2c traps to the FortiPortal unit in this community. Note: By default, the remote port number is 162. Range: 1 to 65535.
trap-v2c-status {enable disable}	Enable/disable SNMPv2c traps for this SNMP community. Default: <i>enable</i> .
events <events_list>	Enable the events that will cause SNMP traps to be sent to the community. <ul style="list-style-type: none"> • <i>cpu_high</i>: CPU usage too high. • <i>disk_low</i>: Disk usage too high. • <i>ha_switch</i>: HA switch.

Variable	Description
	<ul style="list-style-type: none"> • <code>intf_ip_chg</code>: Interface IP address changed. • <code>lic-dev-quota</code>: High licensed device quota detected. • <code>lic-gbday</code>: High licensed log GB/day detected. • <code>log-alert</code>: Log base alert message. • <code>log-data-rate</code>: High incoming log data rate detected. • <code>log-rate</code>: High incoming log rate detected. • <code>mem_low</code>: Available memory is low. • <code>raid_changed</code>: RAID status changed. • <code>sys_reboot</code>: System reboot. <p>Default: All events enabled.</p> <p>Note: The <code>raid_changed</code> event is only available for devices which support RAID.</p>
hosts variable	
<code><host_number></code>	Enter the index number of the host in the table. Enter an unused index number to create a new host.
interface <code><interface_name></code>	Enter the name of the interface that connects to the network where this SNMP manager is located. Note: This must be done if the SNMP manager is on the Internet or behind a router.
ip <code><ipv4_address></code>	Enter the IP address and netmask of an SNMP manager. Note: By default, the IP address is 0.0.0.0 so that any SNMP manager can use this SNMP community.

Example

This example shows how to add a new SNMP community named `SNMP_Com1`.

In this example, the community is added, given a name, and all v2c functionality is disabled because this community is SNMP v1 compatible. After the community is configured, the host, or the SNMP manager is added.

The SNMP manager IPv4 is 192.168.20.34, and the interface is internal.

```
config system snmp community
  edit 1
    set name SNMP_Com1
    set query-v2c-status disable
    set trap-v2c-status disable
  config hosts
    edit 1
      set interface internal
      set ip 192.168.10.34
    end
  end
end
```


SNMP v3 users

The FortiPortal SNMP v3 implementation includes support for queries, traps, authentication, and privacy. SNMP v3 users can be created, edited, and deleted as required.

To create an SNMP user, use the following CLI syntax:

```
config system snmp user
  edit <name>
    set auth-proto {md5 | sha}
    set auth-pwd <passwd>
    set security-level {auth-no-priv | auth-priv | no-auth-no-priv}
    set notify-hosts <ipv4_address>
    set priv-proto {aes | des}
    set priv-pwd <passwd>
    set queries {enable | disable}
    set query-port <integer>
    set events <events_list>
  end
end
```

Variable	Description
<name>	Enter an SNMPv3 user name.
auth-proto {md5 sha}	Authentication protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable. The following options are available: <ul style="list-style-type: none"> md5: HMAC-MD5-96 authentication protocol. sha: HMAC-SHA-96 authentication protocol .
auth-pwd <passwd>	Password for the authentication protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable.
security-level {auth-no-priv auth-priv no-auth-no-priv}	Security level for message authentication and encryption. The following options are available: <ul style="list-style-type: none"> <code>auth-no-priv</code>: Message with authentication but no privacy (encryption). <code>auth-priv</code>: Message with authentication and privacy (encryption). <code>no-auth-no-priv</code>: Message with no authentication and no privacy (encryption) (default).
notify-hosts <ipv4_address>	The IP address or addresses of the host.
priv-proto {aes des}	Privacy (encryption) protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable. The following options are available: <ul style="list-style-type: none"> aes: CFB128-AES-128 symmetric encryption protocol des: CBC-DES symmetric encryption protocol
priv-pwd <passwd>	Password for the privacy (encryption) protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable.
queries {enable disable}	Enable/disable queries for this user. Default: <code>enable</code> .
query-port <integer>	SNMPv3 query port. Default: 161.

Variable	Description
	Range: 1 to 65535.
events <events_list>	<p>Enable the events that will cause SNMP traps to be sent to the SNMP manager.</p> <ul style="list-style-type: none"> cpu-high-exclude-nice: CPU usage exclude nice threshold. cpu_high: The CPU usage is too high. disk_low: The log disk is getting close to being full. ha_switch: A new unit has become the primary HA. intf_ip_chg: An interface IP address has changed. lic-dev-quota: High licensed device quota detected. lic-gbday: High licensed log GB/Day detected. log-alert: Log base alert message. log-data-rate: High incoming log data rate detected. log-rate: High incoming log rate detected. mem_low: The available memory is low. raid_changed: RAID status changed. sys_reboot: The FortiManager unit has rebooted. <p>Default: All events enabled.</p> <p>Note: The <code>raid_changed</code> event is only available for devices which support RAID.</p>

Having set up the SNMP agent, communities, and users, you can test the configuration by using the following command:

```
snmputil get <your_fpc_ip> SNMP_Com1 .1.3.6.1.2.1.1.5.0 where SNMP_Com1 is the name of the community you have set up.
```

SNMP MIBs

You can obtain the MIB files from Customer Service & Support (<https://support.fortinet.com>):

- /FortiAnalyzer/v5.00/Core MIB/FORTINET-CORE-MIB.mib
- /FortiAnalyzer/v5.00/5.2/5.2.0/FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib

To be able to communicate with the SNMP agent, you must include all of these MIBs into your SNMP manager. Generally your SNMP manager will be an application on your local computer. Your SNMP manager might already include standard and private MIBs in a compiled database that is ready to use. You must add both MIBs to this database.

SNMP traps

Fortinet devices share SNMP traps, but each type of device also has traps specific to that device type. For example, FortiPortal units have FortiPortal specific SNMP traps. To receive Fortinet device SNMP traps, you must load and compile the FORTINET-CORE-MIB.mib file into your SNMP manager.

Traps sent include the trap message as well as the unit serial number (fnSysSerial) and host name (sysName). The Trap Message column includes the message that is included with the trap, as well as the SNMP MIB field name to help locate the information about the trap.

Trap message	Description
ColdStart, WarmStart, LinkUp, LinkDown	Standard traps as described in RFC 1215.
CPU usage high (fnTrapCpuThreshold)	CPU usage exceeds the set percent. This threshold can be set in the CLI using the following commands: <pre>config system snmp sysinfo set trap-high-cpu-threshold <percentage value> end</pre>
CPU usage excluding NICE processes (fnSysCpuUsageExcludedNice)	CPU usage excluding NICE processes exceeds the set percentage. This threshold can be set in the CLI using the following commands: <pre>config system snmp sysinfo set trap-cpu-high-exclude-nice-threshold <percentage value> end</pre>
Memory low (fnTrapMemThreshold)	Memory usage exceeds 90 percent. This threshold can be set in the CLI using the following commands: <pre>config system snmp sysinfo set trap-low-memory-threshold <percentage value> end</pre>
Log disk too full (fnTrapLogDiskThreshold)	Log disk usage has exceeded the configured threshold. Only available on devices with log disks.
Temperature too high (fnTrapTempHigh)	A temperature sensor on the device has exceeded its threshold. Not all devices have thermal sensors. See manual for specifications.
Voltage outside acceptable range (fnTrapVoltageOutOfRange)	Power levels have fluctuated outside of normal levels. Not all devices have voltage monitoring instrumentation.
Power supply failure (fnTrapPowerSupplyFailure)	Power supply failure detected. Available on some devices that support redundant power supplies.
Interface IP change (fnTrapIpChange)	The IP address for an interface has changed. The trap message includes the name of the interface, the new IP address and the serial number of the Fortinet unit. You can use this trap to track interface IP address changes for interfaces with dynamic IP addresses set using DHCP or PPPoE.

Fortinet and FortiPortal MIB fields

The Fortinet MIB contains fields reporting current Fortinet unit status information. The following tables list the names of the MIB fields and describe the status information available for each one. You can view more details about the information available from all Fortinet MIB fields by compiling the FORTINET-CORE-MIB.mib file into your SNMP manager and browsing the Fortinet MIB fields.

System MIB fields:

MIB field	Description
fnSysSerial	Fortinet unit serial number.

Administrator accounts:

MIB field	Description
fnAdminNumber	The number of administrators on the Fortinet unit.
fnAdminTable	Table of administrators.
	fnAdminIndex Administrator account index number.
	fnAdminName The user name of the administrator account.
	fnAdminAddr An address of a trusted host or subnet from which this administrator account can be used.
	fnAdminMask The netmask for fnAdminAddr.

Custom messages:

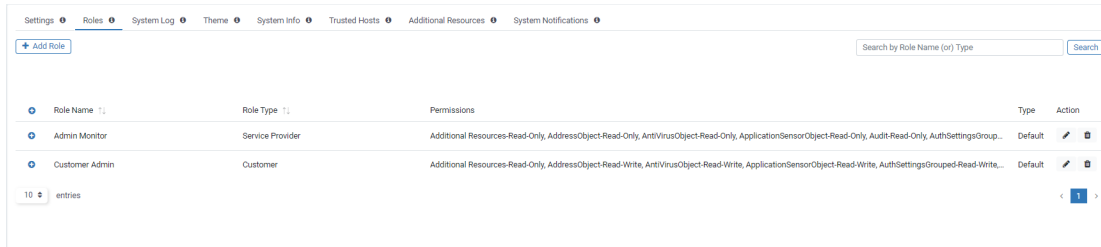
MIB field	Description
fnMessages	The number of custom messages on the Fortinet unit.

MIB fields and traps:





MIB field	Description
fmModel	A table of all FortiPortal models.

Roles

Go to *Admin > Roles* to see role information (type and permissions) for each FortiPortal role:



The screenshot shows the FortiPortal Roles page. At the top, there is a navigation menu with tabs for Settings, Roles, System Log, Theme, System Info, Trusted Hosts, Additional Resources, and System Notifications. Below the navigation is a search bar labeled "Search by Role Name (or) Type" and a search button. The main content is a table with the following columns: Role Name, Role Type, Permissions, Type, and Action. The table contains two rows of data:

Role Name	Role Type	Permissions	Type	Action
Admin Monitor	Service Provider	Additional Resources-Read-Only, AddressObject-Read-Only, AntiVirusObject-Read-Only, ApplicationSensorObject-Read-Only, Audit-Read-Only, AuthSettingsGroup...	Default	 
Customer Admin	Customer	Additional Resources-Read-Only, AddressObject-Read-Write, AntiVirusObject-Read-Write, ApplicationSensorObject-Read-Write, AuthSettingsGrouped-Read-Write...	Default	 

At the bottom left of the table, there is a dropdown menu showing "10 entries". At the bottom right, there is a pagination control showing "1" and navigation arrows.

Page actions

The *Roles* tab contains the following actions:

- *Add Role*—open a dialog to add a role
- *Search*—enter text to search for role names containing that text
- *Show x entries*—sets the number of entries that are displayed at once (10, 20, 50, or 100)
- *Sort*—allows you to sort columns in ascending or descending order.

Per-role actions

When you scroll over a entry in the roles list, the following icons appear in the Action column:

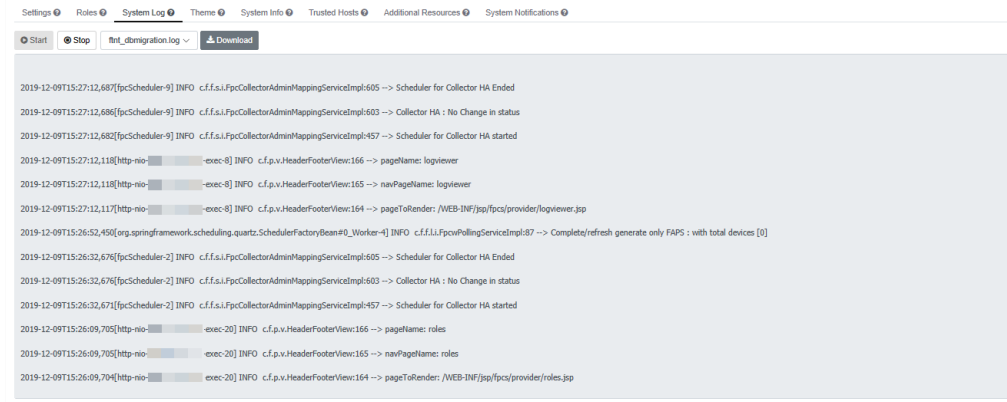
- *Edit*—opens a dialog to edit an existing role
- *Delete*—deletes the selected role

Selecting the *Add Role* button displays the *Add Role* dialog, which contains the following fields (selecting the *Edit Settings* icon under *Actions* displays an identical form with the fields entered):

Settings	Guidelines
Role Name	Name for the role, which must be unique for this customer
Role Type	Service Provider or Customer
Available Permissions:	List of available FortiPortal permissions Use the search box to filter the choices available.
Selected Permissions	FortiPortal permissions to associate with this role Use the search box to filter your selected choices.

System Log

Go to *Admin > System Log* to monitor and download a set of system logs:



Page actions

- *Start*—starts to display the system logs
- *Stop*—stops the system logs
- *Download*—exports the captured system logs in a file

Theme

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

Custom theme options

You can configure customizations such as:

- Select a predefined color scheme. There are five predefined color schemes: default, blue, grey, orange, and red.
- Create a custom color scheme using the Color Picker.
- Upload a custom cascading style sheets (CSS) file.



If the custom CSS file contains any invalid styles, the web interface is reset to the default settings.

- 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 log-in page and page banner

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

Select a predefined color scheme

From the *Color Scheme* pane in the *Theme* tab, select one of the predefined schemes. This scheme takes effect when you select *Save*.

Create a custom color scheme

Define a custom color scheme by selecting colors in the *Color Picker* or by changing the FortiPortal CSS file. Although you can switch between the two methods, these systems are independent. For example, changes made in *Color Picker* do not modify the colors in the CSS file.

The following figure shows the *Color Scheme* pane after you select to customize a scheme:

Color Scheme

Color Scheme

Type

Color Picker

Using the color picker

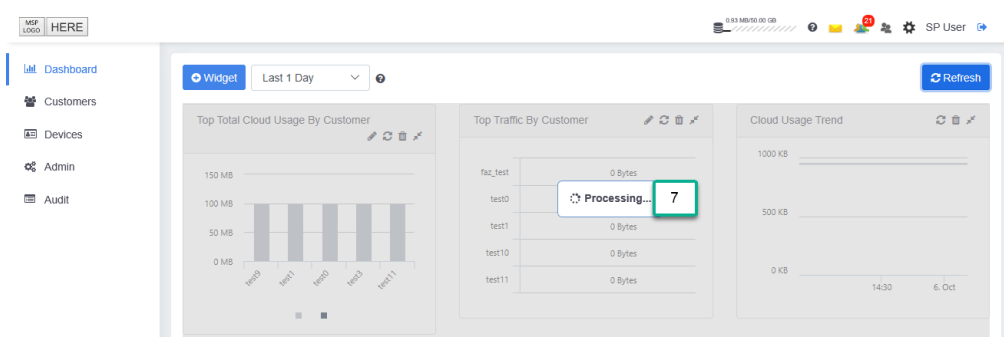
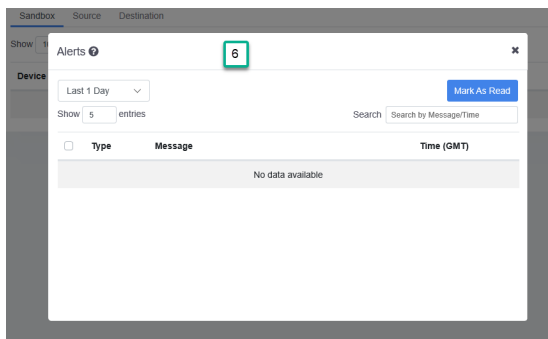
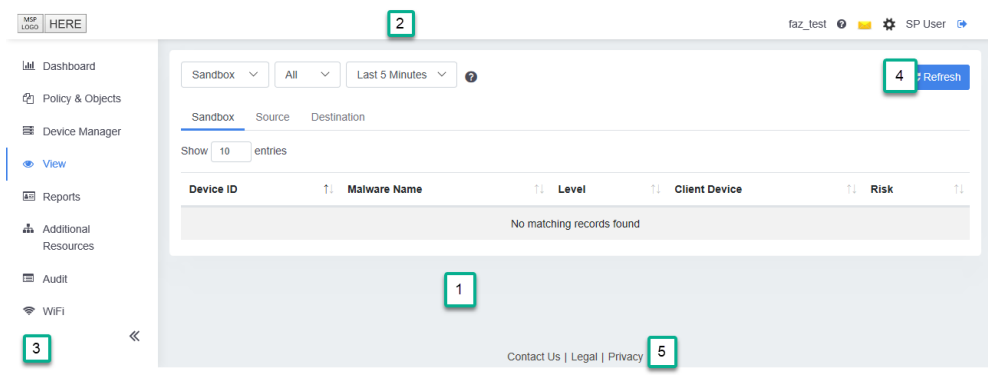
To use the color picker to create a custom color scheme, select *custom* in the *Color Scheme* pane, select *Color Picker* as the *Type*, and then select *Create New Color Scheme* or *Edit Custom Color Scheme*. This opens the *Add Custom Color Scheme* or *Edit Custom Color Scheme* dialog.

The form is divided into the following sections:

- Global Settings
 - Select the font family for all text on the site.
- Background Color Settings
 - Select the background colors for various page elements.
- Font/Text Color Settings
 - Select the text colors for various text fields.

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):



The following table describes the callout labels in the three figures:

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	Page Footer	Background and text color for the bottom portion of the page.
6	Widget header	Background and text color for the widgets (and dialog boxes) on the dashboard and for some content on other pages.
7	Progress Bar	Background and text color for the progress indicator.

Using a custom CSS file

Upload a custom CSS file to have more control over the appearance of the web interface.

Color Scheme

Color Scheme

default
 blue
 grey
 orange
 red
 custom

Type

Color Picker
 Upload CSS

CSS File

To update the CSS file, follow these steps:

1. Select *custom* in the *Color Scheme* pane.
2. Select *Upload CSS* for the type.
3. Select *Export* to export the current CSS file. The file is saved in the Downloads folder of your local machine.
4. Edit the file to make changes as needed and save the file.
5. Select *Import place_holder_custom.css*.
6. Use the file chooser to select your updated CSS file.



If the imported file contains any invalid CSS style, the style will be reset to the default CSS style.

Custom URLs and text

The following figure displays the *URL Settings* pane.

URL Settings

Company Name

Service Name

Service Login Footer

Header URL

Contact URL

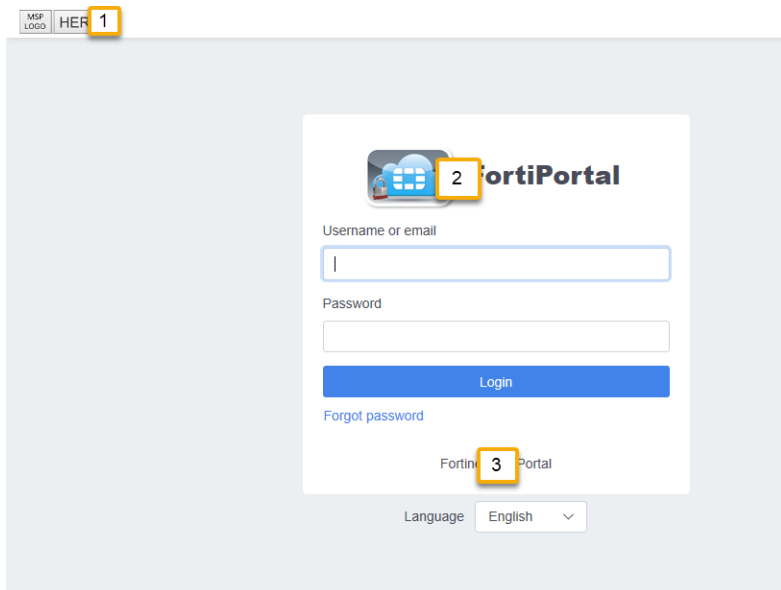
Legal URL

Privacy URL


Acceptable Use Policy URL

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):



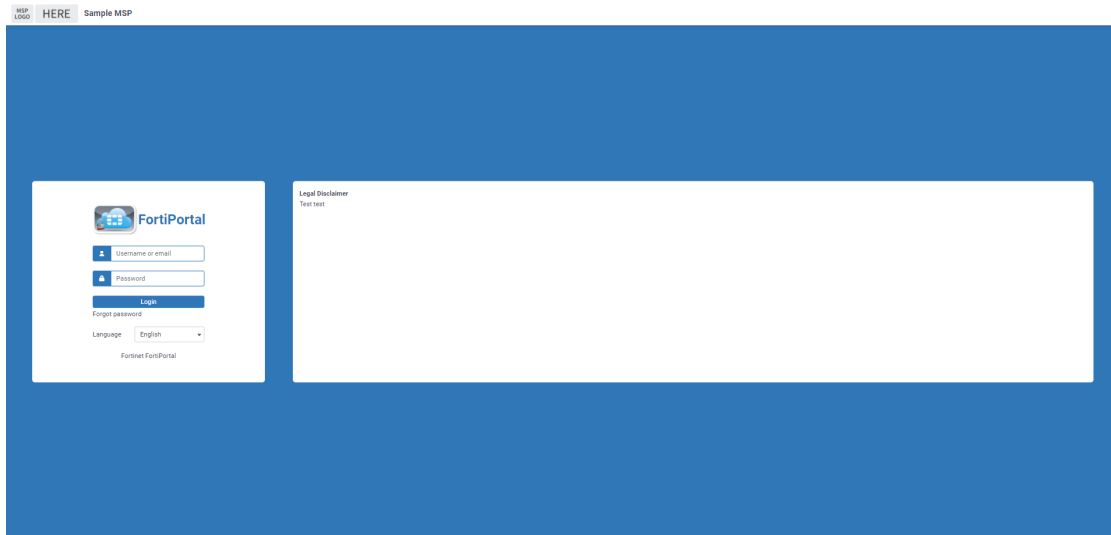
The following table describes the callout labels in the preceding figure:

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

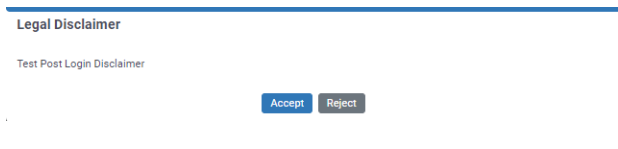
Disclaimers

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:



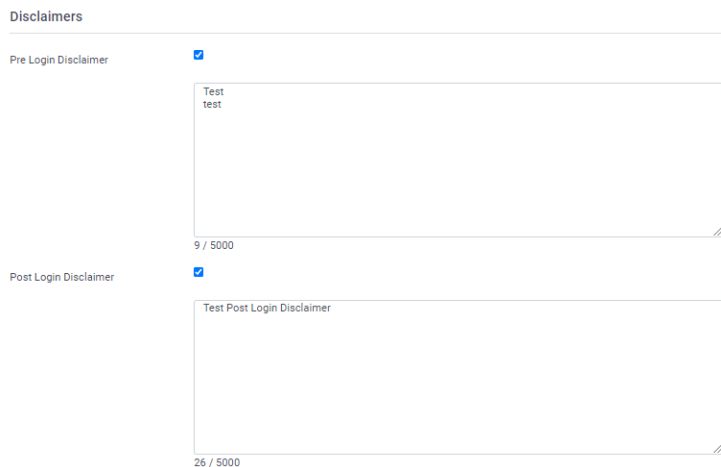
Once you are successfully authenticated, a post-login disclaimer banner appears only when the login attempt was made by a customer user. The customer user must click *Accept* to access FortiPortal. If the customer clicks *Reject*, they are logged out immediately.



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

To set up disclaimers:

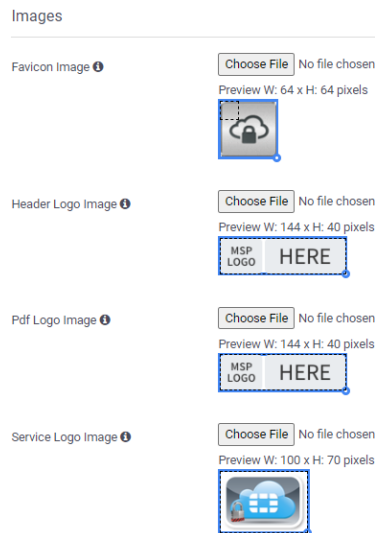
1. Go to *Admin > Theme*.
2. In the *Disclaimers* pane, select *Pre Login Disclaimer* and/or *Post Log in Disclaimer* checkboxes, and enter the disclaimer content. Both pre-login and post-login disclaimers are selected here.



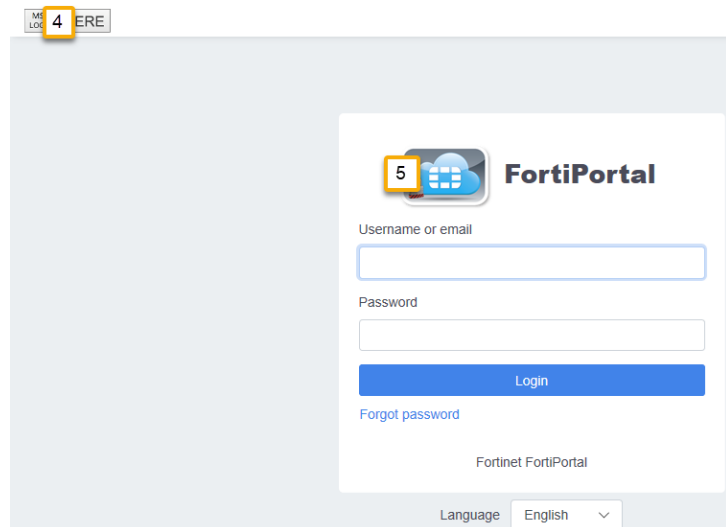
3. Click *Save* to save the changes.
At the next instance of login, and depending on whether you are an administrative user or a customer user, relevant disclaimers appear.

Custom images

The following figure shows the *Images* pane:



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	Description
Header Logo Image	4	Logo image in the page header
Service Logo Image	5	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
Color Scheme	Select a color scheme for the Admin pages. Select the <i>Color Picker</i> icon to add (that is, edit) a custom color scheme.	Blue
Type	Visible for a custom scheme. Select <i>Color Picker</i> or <i>Upload CSS</i> .	Color Picker
Color Picker	Visible only when you select Color Picker as the color scheme type. Opens the Edit Custom Color Scheme form. See the "Using Color Picker" section for details.	n/a

Settings	Guidelines	Default value
CSS File	Visible when you select Upload CSS as the color scheme type. Displays buttons to export or import a CSS file.	n/a
Export	Exports the current CSS file. The file is saved in the Downloads folder of your local machine.	n/a
Import	Imports a file that replaces the current CSS file in use. Opens a file-chooser dialog allowing you to select a CSS file.	n/a
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	(mandatory field) 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
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.		

Settings	Guidelines	Default value
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
PDF Logo Image	Image file that FortiPortal will use as the logo in PDF reports. 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. Alert Image	Image file for the alert icon in the page banner. The recommended image size is 30x30 pixels.	
2. Customer Count Image	Image file for the customer icon in the page banner. The recommended image size is 30x30 pixels.	
3. Users Image	Image file for the administrative users icon in the page banner. The recommended image size is 30x30 pixels.	
4. Change Password Image	Image file for the change password icon in the page banner. The recommended image size is 30x30 pixels.	

System Info

Go to *Admin > System Info* to see additional information about the system.

System Info tab

The screenshot shows the 'System Info' tab in the FortiPortal interface. It is divided into three main sections: 'Version Information', 'License Information', and 'Certificate Information'. The 'Version Information' section displays 'Version' as 6.0.1, 'DB Version' as 6.0.1, and 'Build Number' as 98 (Interim). The 'License Information' section shows 'VM License' as valid, 'Expiry Date' as Wed Oct 21 17:05:00 2020 GMT, 'Devices Allowed [Used]' as 5000 [23], 'FAPs Allowed [Used]' as 50000 [0], and 'Serial Number' as FPC-VM0000005930. The 'Certificate Information' section includes fields for 'Certificate', 'Private Key', and 'Upload License', each with a 'Choose file' button and a 'Browse' button. There are 'Save' buttons at the bottom of the sections.

The tab displays the following panels:

- Version Information
- License Information
- Certificate Information
- Upload License

Version Information

The *Version Information* pane displays the FortiPortal version, database version, and the build number.

License Information

This pane provides information about the FortiPortal license and enables you to upload a new license.

Field	Description
VM License	Indicates the type of license and whether the license is valid
Devices Allowed [Used]	Number of devices to be managed that are included in the license (number in brackets indicates the number of devices currently used)
FAPs Allowed [Used]	Number of Fortinet AP devices that are included in the license (number in brackets indicates the number of devices currently used)

Field	Description
Expiry Date	Expiry date of the license
Serial Number	Your FortiPortal serial number.

Certificate Information

The *Certificate Information* pane displays the certificate file name and private key file name.

From this pane, you can select and upload a new certificate and private key for the FortiPortal (using PKCS#8 format).

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 *Admin > System Info* tab, including the number of devices allowed, the number of devices used, the number of Fortinet Access Points (FAPs) allowed, and the number of FAPs used.

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

If the administrative user creates a customer site, assigns a device to it, and the administrative user has selected the FortiSandbox 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 *Admin > System Info* tab.

When the administrative user removes a device from the customer site, the number of devices used decreases by one, and the number of devices allowed increases by one. Refer to the *Admin > System Info* tab.

The Expiry Date on the *Admin > System Info* tab shows when the FortiPortal license expires.

Use the following steps to upload the FortiPortal license:

1. Go to *Admin > System Info* and locate the *Upload License* pane.
2. In the *Upload License* pane, select *Browse*.
The system opens a file chooser window.
3. Select a license file and select *Open*.
4. The system automatically restarts the FortiPortal VM to apply the license.

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.

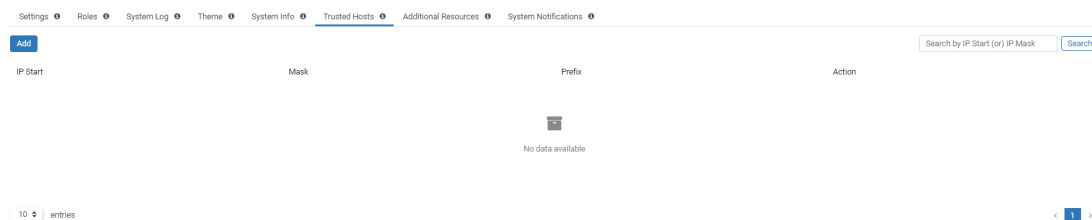


FortiPortal periodically checks for license status update with FortiGuard, when the license is renewed, the interface is available again.

Trusted Hosts

If you enable Trusted Hosts as a global setting (see [Admin settings on page 55](#)), the system enforces a configurable blocklist and allowlist for all admin and customer users. The *Trusted Hosts* tab displays the blocklist, which is a list of IP addresses that are blocked. Refer to [Administrative users on page 22](#) for information about creating the Trusted Hosts allowlist.

Go to *Admin > Trusted Hosts* to create and edit blocklisted IP addresses.



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

Page actions

The *Trusted Hosts* tab contains the following actions:

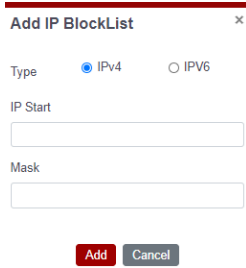
- *Add*—opens a dialog to add a blocklist entry
- *Show x entries*—use the dropdown menu to set the number of entries to display
- *Search*—enter text to search for roles containing that text

Per-host actions

When you scroll over an entry in the hosts list, the following icons appear in the Action column:

- *Edit*—opens a dialog to edit a blocklist entry
- *Delete*—deletes the Trusted Host

The following figure shows the *Add IP BlockList* dialog:



Add IP BlockList ✕

Type IPv4 IPv6

IP Start

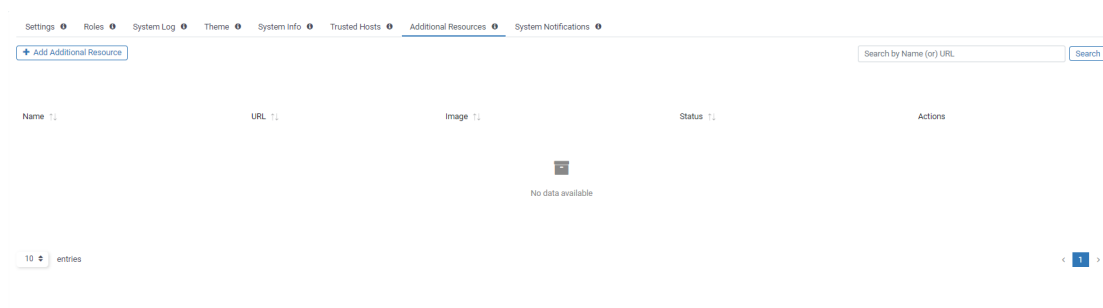
Mask

The *Add/Edit IP BlockList* dialogs contain the following fields:

Settings	Guidelines
IPv4	
IP Start	Start address for the range covered by this entry
Mask	If you entered an IPv4 address, the Mask field becomes visible. Defines the range of IP addresses covered by this entry
IPv6	
IP Start	Start address for the range covered by this entry
Prefix	If you entered an IPv6 address, the Prefix field becomes visible. Defines the range of IP addresses covered by this entry

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:

- *Add Additional Resource*—open a new dialog to add a 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
- *Sort*—allows you to sort columns in ascending or descending order.

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

Add Additional Resource

* Name

* URL

Status

Active Disable

Image

place_holder_button.png

Preview W: 72 x H: 72 pixels

Enter the following button details:

Field	Description
Name	Button or resource name

Field	Description
URL	Link to open when the button is selected
Status	Active or Disabled
Image	Default image is pre-populated. You can change or resize it with the <i>Browse</i> button and resize icon.

Per-resource actions

When you hover over a resource row, the following icons appear in the Action column:

- *Edit*—opens a dialog to edit an existing role
- *Delete*—deletes the selected role

Selecting *Edit* displays the Edit Resource: *button* dialog, where *button* can be Chat, FAQ, or Help:


Edit Resource: FAQ ✕

* Name:

* URL:

* Status: Active Disabled

Image:

 (W:73 x H:73 pixels)

At any time, you can select the *Delete* icon to remove the button row:

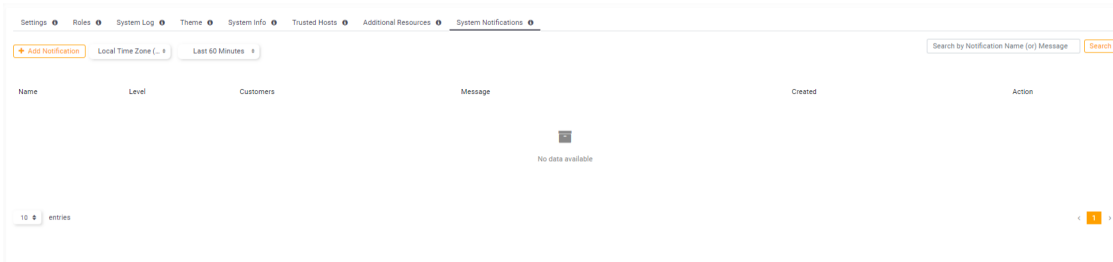
Settings ⌵ Roles ⌵ System Log ⌵ Theme ⌵ System Info ⌵ Trusted Hosts ⌵ Additional Resources ⌵ System Notifications ⌵

Show entries Search

Name	URL	Image	Status	Action
Fortinet	https://www.fortinet.com/	place_holder_button.png	● Active	✎ ✕

System Notifications

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



Page actions

The *System Notifications* tab contains the following actions:

- *Add Notification*—opens a dialog to add a system notification
- *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*)
- *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

Selecting *Add Notification* opens the *Add Notification* dialog:

Enter the following notification details and then select **Save**:

Field	Description
Name	Name of the system notification

Field	Description
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.
Available Customers	Customers who can receive notifications
Selected Customers	Customers who will receive this notification

Per-notification actions

When you hover over a notification row, the following icons appear in the Action column:

- *Edit*—opens a dialog to edit an existing notification
- *Delete*—deletes the selected notification

Selecting *Edit* displays the *Edit Notification* dialog:

At any time, you can select the *Delete* icon to remove the notification row:

Name	Level	Customers	Message	Created (GMT)	Action
testNotificaiton	High	*All	This is to test system notifications, the service provider is going to broadcast this information.	2019-12-10 00:12:32.0	
TestOnlyForOneCustomer	Medium	test	test notifications with only one customer, customer name: test. This is low priority notification.	2019-12-10 00:13:34.0	

Audit

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

The screenshot shows the 'Audit Log List' interface. At the top left, there are two dropdown menus: 'Last 60 Minutes' and 'Local Time Zone (...)'. To the right, there is an 'Export to CSV' button, a search input field labeled 'Search by Client IP Address (or) Message', and a 'Search' button. Below these are the column headers: 'Date', 'Level', 'User Name', 'Event Type', 'Client IP Address', 'Message', and 'Action'. The table body is empty, with a 'No data available' message in the center. At the bottom left, there is a dropdown menu showing '10 entries', and at the bottom right, there are navigation arrows and a page number '1'.

Page actions

- *Filter*—set the duration of the logs to display (*Last 60 Minutes*, *Last 1 Day*, *Last 1 Week*, or *Specify*)
- *Time zone*—use the dropdown to set the time zone *Local Time Zone (US/Pacific)* or *GMT Time Zone*
- *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
- *Sort*—allows you to sort columns in ascending or descending order

Per-audit actions

When you select the *Details* button for an audit entry for changed settings, the system opens a window to display the details of the change. The details window shows the original ("oldDetails") and new ("newDetails") field values.

Details



```
{
  "oldDetails": [
    {
      "serialNumber": "FGT6001100636412",
      "wifiFrequencyValue": "Every 15 Minutes",
      "port": 443,
      "ipAddress": "0.0.0.0",
      "wifiController": "No",
      "deviceName": "ADOM_QA_60/FGTM0060/root"
    }
  ],
  "newDetails": [
    {
      "serialNumber": "FGT6001100636412",
      "wifiFrequencyValue": "Every 15 Minutes",
      "port": 443,
      "ipAddress": "0.0.0.0",
      "wifiController": "Yes",
      "deviceName": "ADOM_QA_60/FGTM0060/root"
    }
  ]
}
```

Cancel

Appendix: Sizing

Before you start your setup, you need to determine the storage requirements.

The following calculation can be used to determine the total storage value:



By default, the storage size set for each customer is 100 MB.

Total storage size = number of customers * storage size set for each customer.

For example:

Number of customers = 5

When you substitute these values into the calculation:

Total storage size = 5 * 100 = 500 MB.

The system requires other overheads as well, which may take 15 GB of storage. As a minimum, 40 GB of storage is required.



In FortiAnalyzer mode, all the logs are stored on the FortiAnalyzer side, and the storage required for each customer on FortiPortal is the total storage size defined.

Sizing recommendations

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

Number of customers	Portal VM				Portal DB			
	Number of VMs	RAM (GB)	vCPU	Storage (GB)	Number of VMs	DB RAM (GB)	vCPU	Storage (GB)
Minimum	1	4	2	100	1	4	2	100
500	1	8	4	200	1	8	2	100
1000	1	16	8	400	1	16	4	200

Number of customers	Portal VM				Portal DB			
	Number of VMs	RAM (GB)	vCPU	Storage (GB)	Number of VMs	DB RAM (GB)	vCPU	Storage (GB)
2500	1	32	12	600	1	32	8	500
5000	2	64	16	1000	1	32	8	1000
7500	2	64	16	1500	1	32	8	1000
10000	2	128	16	2000	1	64	12	2000

Appendix: Installation using OpenStack

The FortiPortal software runs on virtual machines.

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

Prerequisites

Note the following prerequisite items:

1. You must provide a MySQL server for the portal database.
2. Download the portal image from Fortinet Support site.
3. Access the OpenStack Horizon Dashboard for your OpenStack environment.

Downloading FortiPortal image files

To download the required image files:

1. Navigate to the Fortinet customer service page (<https://support.fortinet.com>).
2. Go to *Download > Firmware Images*.
3. In Firmware Images page, select *FortiPortal*.
4. Download the latest image files in QCOW2 format:
 - fpcvm64imagePortal.out.qcow2

OpenStack Horizon Dashboard

Log in to the OpenStack Horizon Dashboard, which provides a web-based user interface to OpenStack services.

Create an image for the portal

Create a portal image.

Use the following steps to create an image:

1. From the left menu, select *Compute > Images*.
2. Select *Create Image*.

3. System opens a form. Enter the following fields in the form:
 - a. Enter a unique name for the image.
 - b. Image Source: select *Image File*.
 - c. Select *Choose File* to open the file chooser.
 - d. Select the portal that you saved on the hard drive.
 - e. Format: QCOW2.
 - f. Architecture: leave blank.
 - g. Minimum Disk: 80.
 - h. Minimum Ram: 16.
 - i. Select *Create Image*.

Create a volume for the portal

Create a storage volume for the portal.

Use the following steps to create a volume:

1. Select *Volumes* in the main menu.
2. Select *Create Volume*.
3. System opens a form. Enter the following fields in the form:
 - a. Enter a unique name for the volume.
 - b. *Volume Source*: No source, empty volume.
 - c. *Type*: No volume type.
 - d. *Size*: 80.
 - e. *Availability Zone*: select a zone.
 - f. Select *Create Volume*.

Launch the instance

Launch one instance for the portal.

To launch a VM instance:

1. Select *Instances* in the main menu.
2. Select *Launch Instance*.
3. System opens a form. Enter the following fields in the Details tab of the form:
 - a. *Availability Zone*: select a zone.
 - b. *Instance Name* Enter a unique name for the instance.
 - c. *Flavor*: Select the appropriate size of VM.
 - d. *Instance Count*: You can create one or more instances.
 - e. *Instance Boot Source*: Select Boot from image.
 - f. *Image Name*: Select the image name.

4. In the *Access & Security* tab:
 - a. *Key Pair*: Select a key pair.
 - b. *Security Groups*: Select the default.
5. In the *Networking* tab:
 - a. *Available networks*: Select a network.
6. Select *Launch*.

Launch one instance for the portal.

Assign a floating IP address

To associate an IP address to the instance:

1. Select *Instances* in the main menu.
2. In the *Actions* column, select *Associate Floating IP* in the pull-down list.
3. Select the + key to obtain an available IP address.
4. Select *Associate*.
Note the Floating IP address value. You will need this to configure the IP interface.

Associate the volume to the instance

To associate the storage volume to the instance:

1. Select *Volumes* in the main menu.
2. In the *Actions* column of the new volume, select *Manage Attachments* in the pull-down list.
3. Select the instance to associate.
4. Select *Attach Volume*.

Reboot the instance

To reboot the instance:

1. In the *Action* column, select *Hard Reboot* in the pull-down list.

Determine the IP address and port number

After the reboot, use the FortiPortal CLI to determine the IP address and external port number for the instance:

1. Select *Instances* in the main menu.
2. *Note the instance internal IP address*.
3. Select the instance name. The system displays the instance overview.

4. Select the *Console* tab.
5. Log in using default credentials.
6. Run the interface configuration command, and *note the Ethernet port number*:

```
exe shell
  ifconfig
exit
```

Configure the portal parameters

After the reboot, use the FortiPortal CLI to configure the portal parameters. Configure the parameters using the following steps:

1. Open the *OpenStack* console tab to view the console for the portal.
2. Log in using the default user ID (admin, with no password required).
3. Use the CLI instructions (see the steps below) to set the following parameters:

Setting	Description
Hostname	Host name for the portal VM
IP address and Default Gateway	Floating IP address for the portal VM and the route to the default gateway
SQL settings	Floating IP Address of the portal SQL server, database name, user credentials.
NTP settings	IP Address of the NTP server

For the portal VM and SQL server, use the Floating IP addresses created in [Assign a floating IP address on page 104](#).

CLI steps

1. Configure the host name for the portal VM:

```
config system global
  set hostname <host name>
end
```

2. Configure the system IP address and default gateway for the portal VM:

```
config system interface
  edit <port number>
    set ip <IP address> <mask>
    set allowaccess ping https http ssh snmp telnet
  end
config system route
  edit 1
    set device <port number>
    set gateway <default gateway>
  next
end
```

3. Configure the SQL settings:

```

config system sql
  set status remote
  set database-port <mySQL port>
  set database-type mysql
  set database-name fp_fazlite
  set username <portal database mySQL username>
  set password <portal database mySQL password>

  set server <IP address or FQDN for the portal database>
end

```

4. Configure the NTP settings for the portal VM:

```

config system ntp
  config ntpserver
    edit 1
      set server <NTP server>
    end
  set status enable
end

```

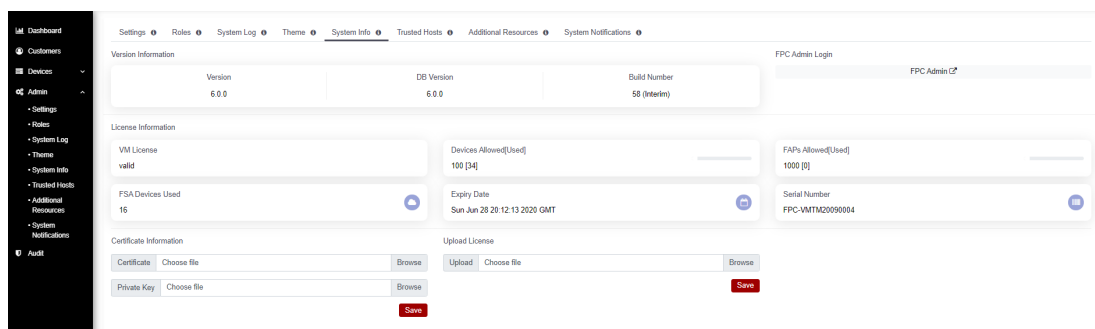
5. Reboot the VM.

Updating the SSL certificate file

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

From the Admin portal, select *Admin > System Info* to display information about the SSL certificate.

System Info page



The Certificate Information panel displays the certificate file name and private key file name.

From this panel, you can select and upload a new certificate and private key for the FortiPortal (using the PKCS#8 format).

Installing MySQL for FortiPortal databases

The MySQL database server for the portal is a standard physical or virtual server.

Edit the `my.cnf` file to adapt the MySQL configuration for FortiPortal:

1. Edit the bind address to make the database reachable from the FortiPortal:
`bind-address = <IP address of the database server>`
2. Fortinet recommends that you create a dedicated MySQL user for FortiPortal. You will need to know the credentials for this user when you create the portal.

Notes:

- The portal database bind-address should match the SQL server address that you configure in the SQL settings of the portal (see *Configure Portal Parameters*).
- If you are using MySQL 5.7.x, please add the following lines in the `my.cnf` file:
 - `[mysqld] sql_mode = STRICT_TRANS_TABLES,NO_ZERO_IN_DATE,NO_ZERO_DATE,ERROR_FOR_DIVISION_BY_ZERO,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION`

Reconfiguring MySQL password on FortiPortal

If you change the password for the FortiPortal user in the portal MySQL database, you need to update the configuration in the portal:

```
config system sql
  set status remote
  set database-type mysql
  set password <portal db MySQL password>
end
```

Appendix: Installation using Nutanix

The FortiPortal software runs on virtual machines.

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

Once you have downloaded and extracted the virtual hard drive image file with the extension `qcow2`, you can create the virtual machine in your Nutanix environment. See [Appendix: Installation using OpenStack on page 102](#).

To upload the FortiPortal deployment image to Nutanix:

1. Launch the Prism Element web console.
2. Go to *Settings > Image Configuration*.
3. Upload the FortiPortal image by clicking *Upload Image*.
4. In the *Name* field, enter FortiPortal.
5. In the *Image Type* dropdown, ensure *Disk* is selected.
6. In the *Storage Container*, select the storage container to use.
7. In the *Image Source* pane, click *Upload a file*.
8. Select the `.qcow2` file previously downloaded.
9. Click *Save*.

Wait a few minutes, then refresh the browser. You will find the newly created VM image in the image list. Confirm that its state is active.

To create the FortiPortal-VM from the image file:

1. In Prism Element web console, go to *VM > Create VM*.
2. For *General Configuration* and *Compute Details*, enter the following configuration information:
 - a. In the *NAME* field, enter the desired name for VM, for example FortiPortal-VM.
 - b. In the *VCPU(s)* field, enter 2.
 - c. In the *MEMORY* field, enter 8.
3. By default, a CD-ROM is listed under *Disks*. Delete the CD-ROM.
You must create a boot disk and a data disk for the VM.
4. Create the boot disk:
 - a. Click *Add New Disk*.
 - b. The boot disk will be cloned from the VM image uploaded. In the *OPERATION* dropdown, select *Clone from Image Service*.
 - c. In the *BusType* dropdown, select *PCI*.
 - d. In the *IMAGE* dropdown, select the FortiPortal disk image uploaded in [To upload the FortiPortal deployment image to Nutanix](#).
 - e. Click *Add*. The boot disk has been added.
5. Add a network interface for the VM:
 - a. Under *Network Adapters (NIC)*, click *Add New NIC*.
 - b. Under *VLAN NAME*, select *NR_PRT_STATIC* and click *Add*.
 - c. Click *Save*.

The system displays a *Successfully submitted Create operation* message when the VM has been created successfully with no error.

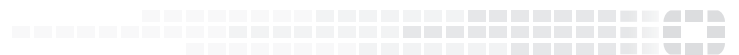
To power on FortiPortal-VM:

1. In Prism Element, find the newly created FortiPortal-VM and go to its VM dashboard.
2. By default, the FortiPortal-VM is shutdown after initial creation. Click *Power On*.
After a successful bootup, the FortiPortal-VM instance now shows a green light.

To configure the host name, IP address, default gateway, SQL, and NTP settings for the portal VM, see [CLI steps on page 105](#).



FORTINET[®]



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