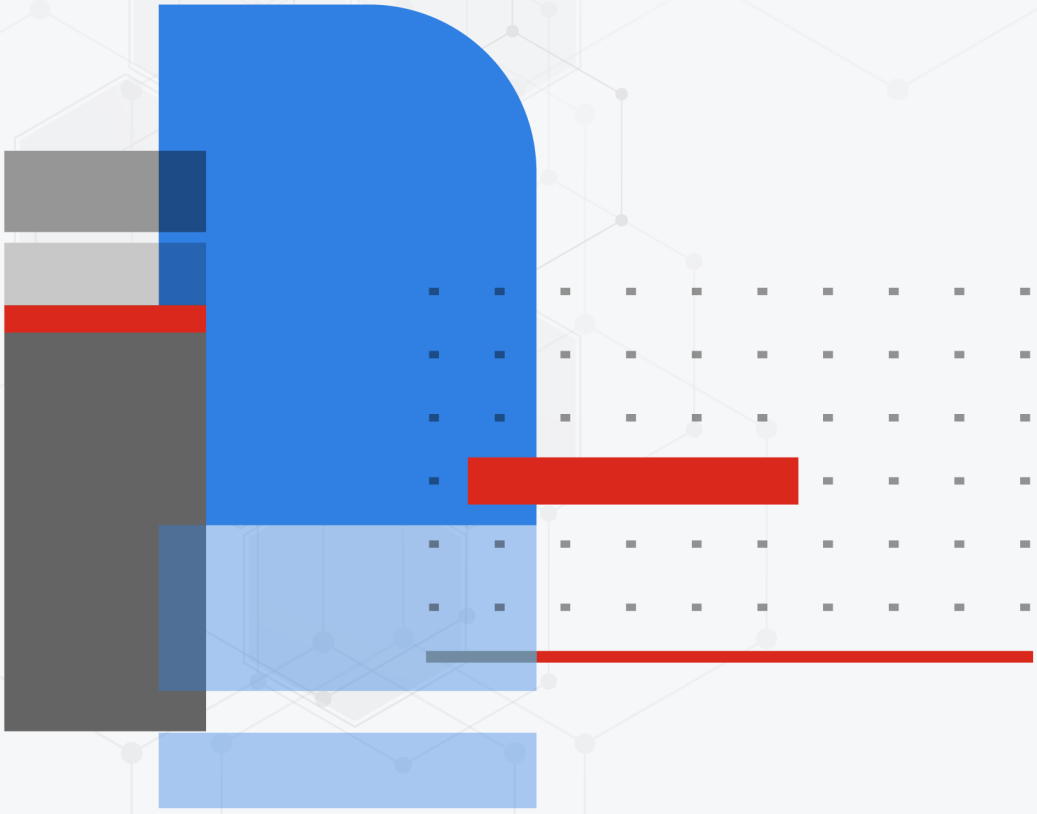
User Guide

FortiGuest 2.0.0



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

June 12, 2025
FortiGuest 2.0.0 User Guide
70-1118770-200-20250612

TABLE OF CONTENTS

Change log

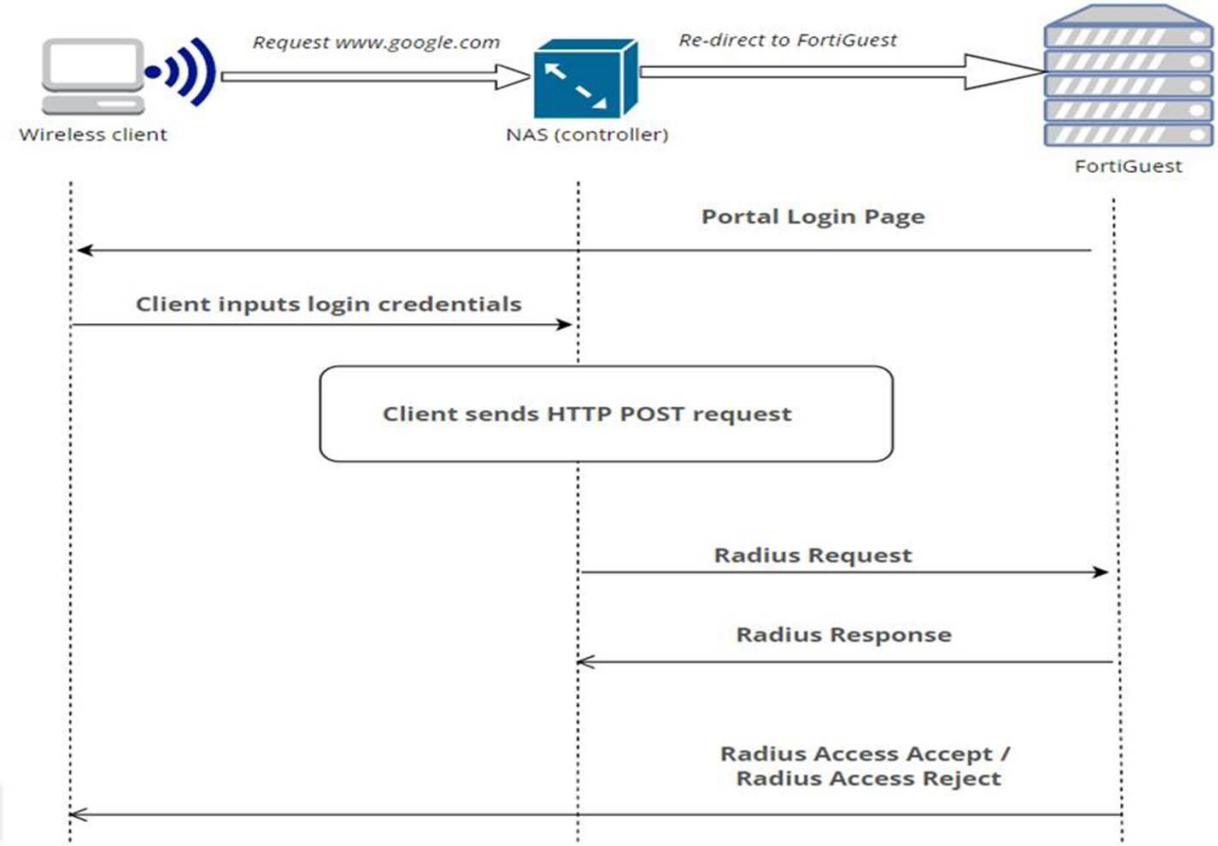
Date	Change description
2025-02-07	FortiGuest version 2.0.0 release document.
2025-03-25	Changed Twitter to X.

Introduction

FortiGuest is an access management solution that provides secure network access to guests as per the configured policies. It monitors and reports user activity ensuring policy compliance and network security.

What is FortiGuest

FortiGuest is a complete provisioning, management, and reporting system that provides network access for guests and visitors. It works along side wireless controllers (FortiGate), LAN switches, NAC systems, firewalls, and other network enforcement devices that provide captive portal and enforcement points for user (remote) access. This diagram depicts the captive portal authentication process with FortiGuest.



Using FortiGuest with requisite privileges allows you to create user accounts and sponsor them for network access. FortiGuest performs full authentication of sponsors and user accounts. When user accounts are created, they are stored within the built-in database on the FortiGuest server. When using this database,

external network access devices can authenticate users against FortiGuest using the RADIUS protocol. FortiGuest provides vital network access accounting, by consolidating the entire audit trail from account creation to actual use of the account. This ensures that reports are generated through a central management interface.

After a user account is deleted, FortiGuest either deletes the account or sends a RADIUS message which notifies the controller of the amount of valid time remaining for the account before the controller removes the user.

Key Concepts

The following key concepts/terms are required to understand FortiGuest.

The Guest/User

The guest/user requires an account to access the network using their own device, connecting to a wired or wireless hotspot provided by an organization. They normally have their browser connection re-directed to a portal where they can login by the network enforcement device.

Sponsor

The sponsor creates the user account and is often an employee of the organization that provides the network access. Sponsors are specific individuals with certain job roles or employees who authenticate against a corporate directory such as Microsoft Active Directory (AD).

Admin

The admin is the administrator who configures and maintains FortiGuest.

Network Enforcement Device

These devices are the network infrastructure components that provide the network access. Additionally, network enforcement devices are responsible for pushing guests/users to a captive portal where they can enter their account details. The captive portal is present either on the network enforcement device or FortiGuest. When a user enters his or her user name and password, the network enforcement device checks those credentials against the accounts created by FortiGuest.

FortiGuest

FortiGuest ties together all the pieces of user access. FortiGuest links the sponsor creating the account, the account details passed to the guest/user, the user authentication against the network enforcement device, and the network enforcement device's verification of the user with FortiGuest. Additionally, FortiGuest consolidates accounting information from network enforcement devices to provide a single point of user access reporting who created the account, when the user accessed the network, and the network activity.

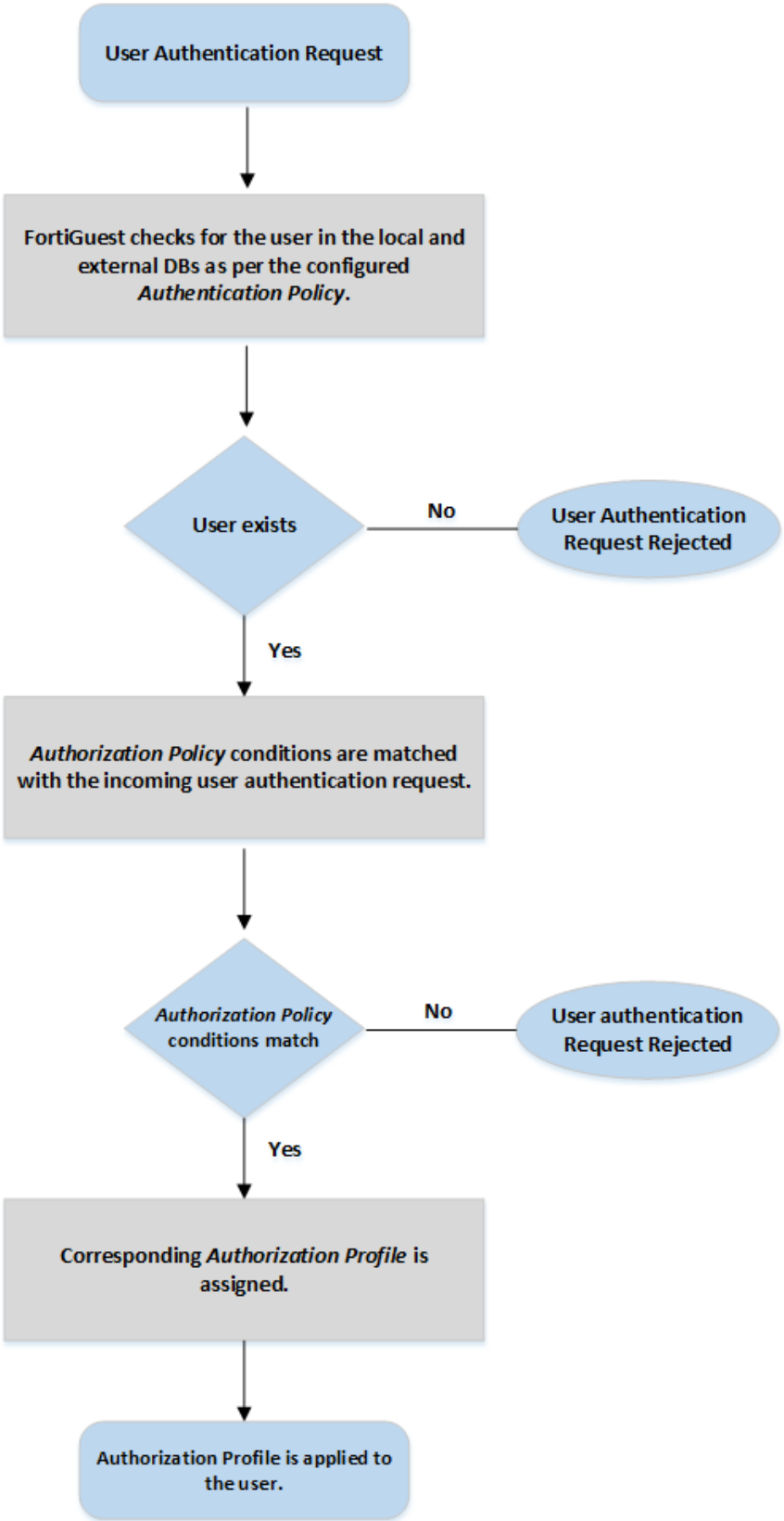
Limitations

The following limitations apply to this release of FortiGuest.

- WPA 3 Personal authentication is supported only on Ubuntu 22.04 and 20.04, Android12, Windows 11, and MacOS 13.2.1.
- MSCHAPV2 TLS version 1.0 not working due to vulnerability restrictions.
- You are required to upload **certificates** on the trust store individually. Uploading multiple certificates is not supported.

Local and External Authentication

FortiGuest can authenticate sponsors/admins against entries in its own database (local) or against an external backend server like an Active Directory or LDAP. This section describes the procedure for user authentication.


User Authentication Request
FortiGuest checks for the user in the local and external DBs as per the configured *Authentication Policy*.
User exists
No
User Authentication Request Rejected
Yes
Authorization Policy conditions are matched with the incoming user authentication request.
Authorization Policy conditions match
No
User authentication Request Rejected
Yes
Corresponding *Authorization Profile* is assigned.
Authorization Profile is applied to the user.

Local Sponsor/Admin Authentication

Perform these steps to configure local sponsor/admin authentication.

1. Configure an *Authorization Profile*. Navigate to **Network Access Policies > Authorization Profiles** and create a user authorization profile. See section Authorization Profiles.
2. Configure an *Authorization Policy* to map the **Authorization Profile** to. Navigate to **Network Access Policies > Authorization Policies** and create a user authorization policy. See section Authorization Policies.
3. Configure local authentication to set up Sponsor user accounts directly on FortiGuest. Navigate to **Access Management > Authentication > Admin Users**. See section Adding Administrator.

External Sponsor/Admin Server Authentication

You can configure FortiGuest for authentication against a backend server. This includes both CP and WPA2 Enterprise.

1. Configure a *RADIUS Client*. Navigate to **Devices > RADIUS Clients**. See section RADIUS Clients.
2. Configure an *Authentication Policy*. The authentication policy is what the FortiGuest checks for an authentication request against a set of rules. Based on these rules, a user is mapped to its respective Account Group and Usage Profile. Navigate to **Network Access Policies > Authentication Policies**. See section Authentication Policies.

FortiGuest processes an incoming user authentication request based on the configurations described in this section.

Installing FortiGuest

You can install FortiGuest VMware ESXi 6.5 and above.

- Deploying FortiGuest on VMWare ESXi
- Deploying FortiGuest on Linux KVM.
- Deploying FortiGuest on Windows Hyper-V
- Setting up Network IP configuration
- Accessing FortiGuest
- Upgrading Firmware
- Licensing

Deploying FortiGuest on Public Cloud Platforms

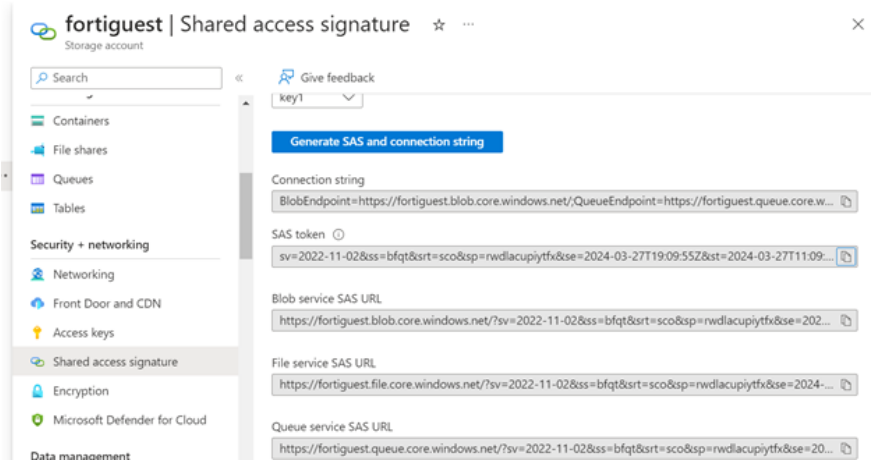
FortiGuest can now be deployed on the following public Cloud platforms.

- Microsoft Azure
- Google Cloud Platform
- Amazon Web Services (AWS)
- Oracle Cloud Infrastructure (OCI)

Microsoft Azure

Perform the following steps to deploy FortiGuest on Microsoft Azure.

1. Obtain the *FortiGuest_VM64_AZURE-v1.3.0-[build0xxx].azure.zip* file from Fortinet and extract it to obtain the *FortiGuest_VM64_AZURE-v1.3.0-[build0xxx].vhd* file.
2. Create a **Resource Group** and a **Storage Account** via the Azure CLI. See Mange Azure Resource Group.
3. Create a Container registry. See Create a container registry.
4. Upload the VHD file to Azure.
5. Obtain the SAS string from the Azure portal. Navigate to **Storage Accounts > Shared access signature**. Configure the parameters in the page and click **Generate SAS and connection string**.

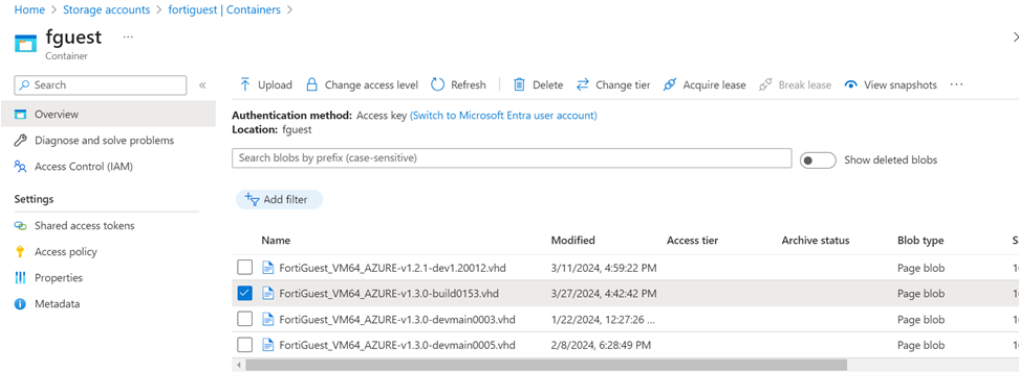


Paste the SAS code from the generated string and upload the VHD file.

```
./azcopy cp "./FortiGuest_VM64_AZURE-v1.3.0-devmain0005.vhd"
"https://fortiguest.blob.core.windows.net/fguest/?sv=2022-11-
02&ss=bfqt&srt=sco&sp=rwdlacupiytfx&se=2024-02-08T20:36:43Z&st=2024-02-
08T12:36:43Z&spr=https&sig=UOaq5aSWEpS%2BWesKJXTT9IJ4WC%2Bc8QM2NbWaem2FGVc%3
D" --blob-type=PageBlob.
```

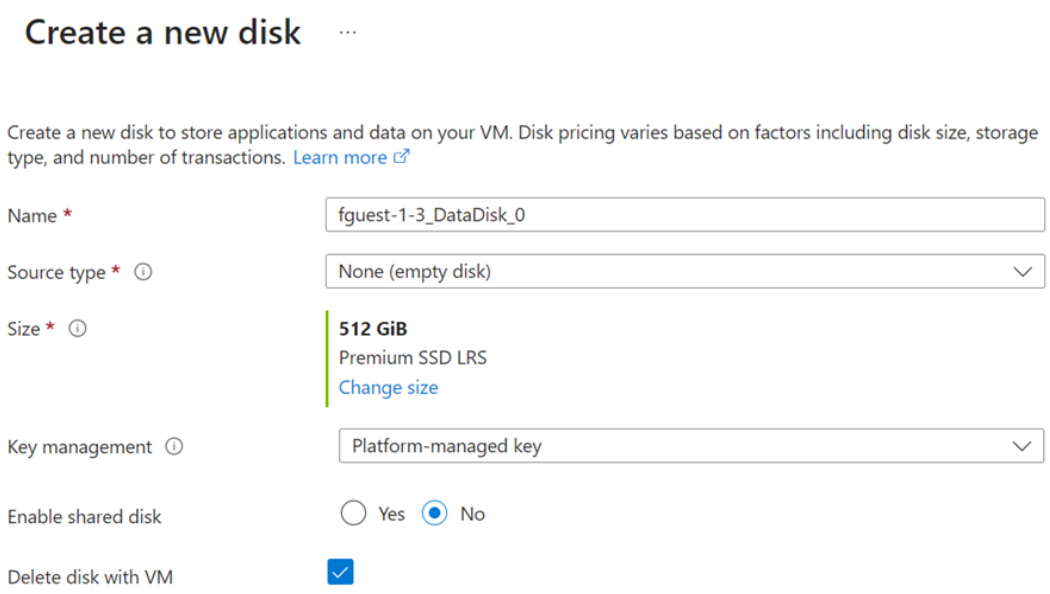
For more information on the `azcopy` command, see azcopy copy.

6. After the upload is successfully completed, you can view the file in **Storage Accounts > Container**.



7. Create a managed image from the uploaded VHD file. Navigate to **Images > Create an image** in the Azure portal and configure the following settings.
   - **OS type** – Linux
   - **VM generation** – Gen 1
   - **Storage blob** – Browse to the uploaded VHD file.
     Note: You are not required to add the data disk as it is created along with the VM.
8. Create the VM from the managed image that you just generated.
   - **Image** - Select the managed image generated in the previous step.
   - **Select inbound ports** - Configure network inbound rules to allow SSH access.

9. Click **Next: Disks** to configure disk data. The recommended disk size is a minimum of 500 GB.

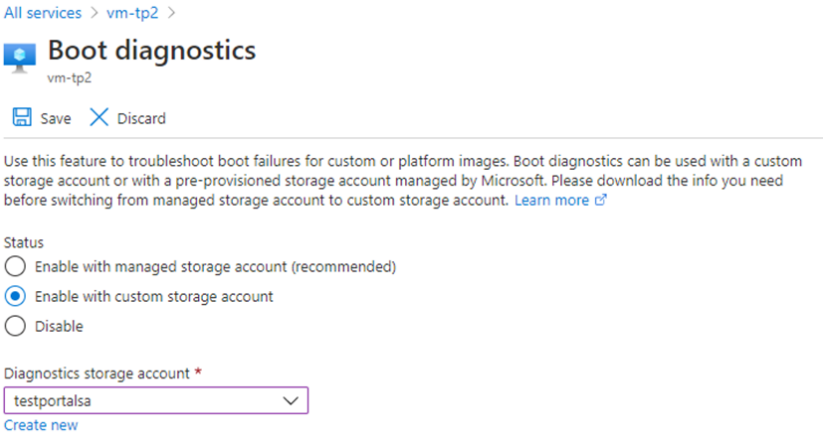


10. Connect the VM via SSH or the serial console.
    - To connect via SSH, obtain the public IP address of the VM – `ssh admin@ <public_ip_address>`.

```
> ssh -i ../fimg-v1_key.pem admin@20.120.161.23
FOSAZU #
 config     Configure object
 get        Get dynamic and system information
 show       Show configuration
 execute    Execute static commands
 exit       Exit the CLI

FOSAZU # show
config system global
end
config system interface
    edit port1
        set mode dhcp
        set allowaccess ssh
    next
end
config system route
end
config system dns
end
config system ntp
end
config system admin
    edit admin
    next
```

    - To connect via the serial console, select the running VM and click **Serial Console**. Click on the prompt

in the right to configure.

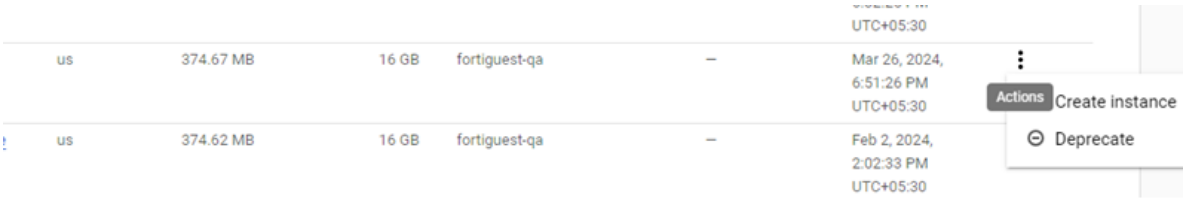


11. Click **Save**.

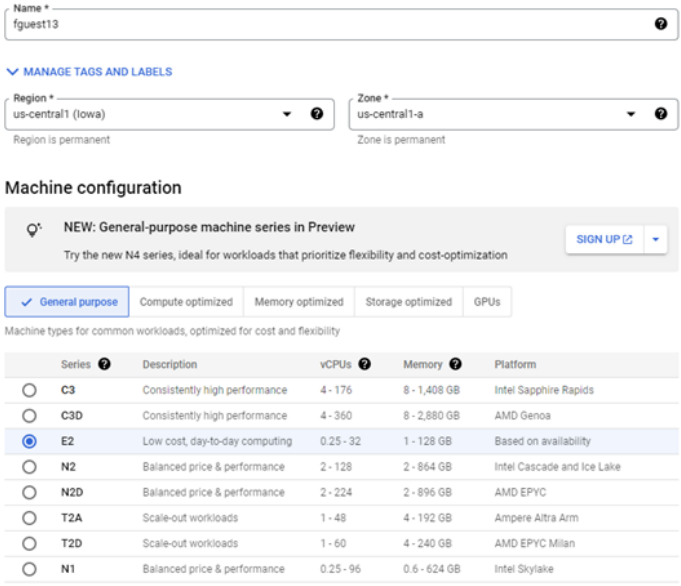
Google Cloud Platform

Perform the following steps to deploy FortiGuest on Google Cloud.

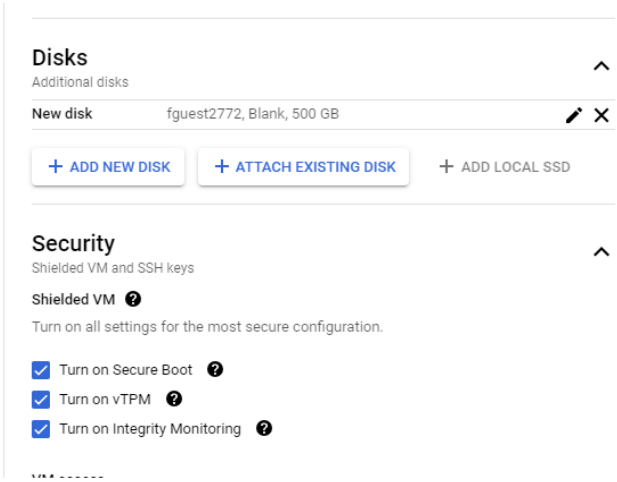
1. Obtain the file *FortiGuest_VM64_GCP-v1.3.0-[build0xxx].zip* from Fortinet and extract it to obtain *FortiGuest_VM64_GCP-v1.3.0-[build0xxx].gcp.tar.gz*.
2. Install and setup **gsutil** to access Cloud storage from the CLI using HTTPS. To install **gsutil**, see Install gsutil.
3. Alternatively, run the following command to download the Linux 64-bit archive file.
   `curl -O https://dl.google.com/dl/cloudsdk/channels/rapid/downloads/google-cloud-cli-389.0.0-linux-x86_64.tar.gz`
4. Extract the contents of the file to any location on your file system (preferably your Home directory). To replace an existing installation, remove the existing *google-cloud-sdk* directory and then extract the archive to the same location - *tar -xf google-cloud-cli-389.0.0-linux-x86.tar.gz*.
5. Run the script (from the root of the folder you extracted the file to) - *./google-cloud-sdk/install.sh*.
6. Run `./google-cloud-sdk/bin/gcloud init` to initialize GCP CLI.
7. Upload the file *FortiGuest_VM64_GCP-v1.3.0-[build0xxx].gcp.tar.gz* to the Cloud storage bucket in the GCP console.
   `./google-cloud-sdk/bin/gsutil FortiGuest_VM64_GCP-v1.3.0-[build0xxx].gcp.tar.gz gs://my-some-bucket`
   `./import2gcpimg.sh fguest27 FortiGuest_VM64_GCP-v1.3.0-[build0xxx].gcp.tar.gz fortiguest_3`
   Run the `gcloud compute instances update IMAGE_NANE --shielded-secure-boot` command to enable secure boot or enable it on the GUI prior to the instance starting.
8. In the **Compute Engine** service interface, click the **Actions** menu and select **Create instance** for the uploaded image. For more information, see Create a VM.



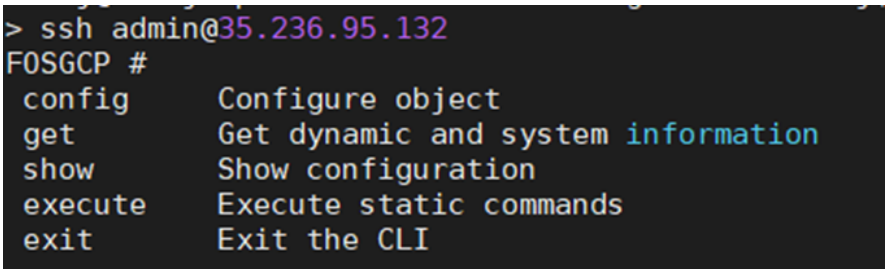
9. Provide a unique instance name and configurations, such as, machine type, enabling HTTP firewall access, and select the network interface card.



Add a blank standard persistence disk of 500 GB and enable secure mode. Click **Create instance**.



10. Connect the VM instance and login.
    - To connect via the Compute Engine console, click **VM Instances** and select the VM instance that you want to connect to. Click **Connect to Serial Console**. See Connect to the Serial Console. In the console interface, login with the user name admin. A password in not required.
    - To connect via the SSH, obtain the public IP address from the VM Instances interface and connect via SSH.



Amazon Web Services (AWS)

Perform the following steps to deploy FortiGuest on AWS.

1. Obtain the file *FortiGuest_VM64_AWS-v1.3.0-[build0xxx].aws.zip* from Fortinet.
2. Install or gain access to the AWS CLI. See Get started with the AWS CLI.
3. Configure the AWS CLI as per your access requirements. These are some sample values that you must replace with the relevant ones.

```
$ aws configure
   AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
   AWS Secret Access Key [None]: YEXAMPLEKEY
   Default region name [None]: us-west-2
   Default output format [None]: json
```

4. Create an IAM role named *vmimport*. This operation requires IAM permissions.

```
cat <<EOF > trust-policy.json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": { "Service": "vmie.amazonaws.com" },
         "Action": "sts:AssumeRole",
         "Condition": {
            "StringEquals":{
               "sts:Externalid": "vmimport"
             }
         }
      }
    ]
}
EOF
aws iam create-role --role-name vmimport --assume-role-policy-document
file://trust-policy.json
```

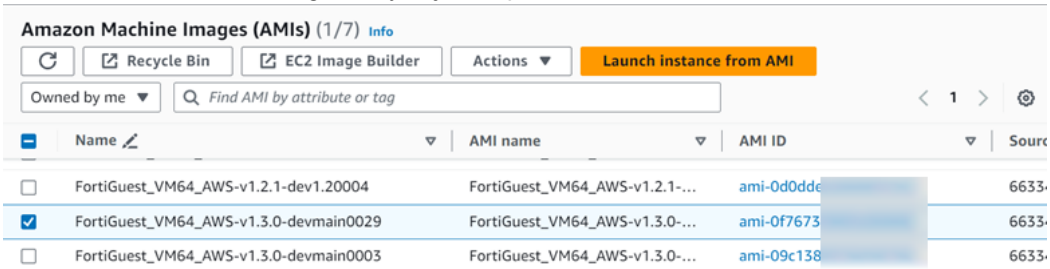
   a. Create a policy and attach it to an Amazon S3 bucket.

```
   cat <<EOF > role-policy.json
   {
      "Version":"2012-10-17",
      "Statement":[
         {
            "Effect":"Allow",
            "Action":[
               "s3:GetBucketLocation",
               "s3:GetObject",
               "s3:ListBucket
            ],
            "Resource":[
               "arn:aws:s3:::$s3BacketName",
               "arn:aws:s3:::$s3BacketName/*"
            ]
         },
         {
           "Effect":"Allow",
```

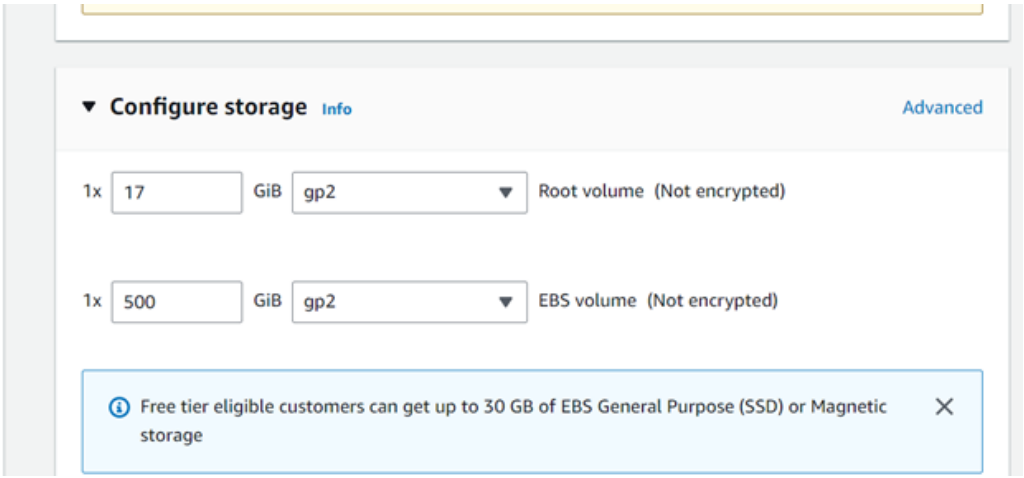
```
            "Action":[
                "ec2:ModifySnapshotAttribute",
                "ec2:CopySnapshot",
                "ec2:RegisterImage",
                "ec2:Describe*"
            ],
            "Resource":"*"
        }
    ]
}
EOF
aws iam put-role-policy --role-name vmimport --policy-name vmimport --
policy-document file://role-policy.json
```

For more information, see Importing a VM as an Image.

5. Extract the file *FortiGuest_VM64_AWS-v1.3.0-[build0xxx].aws.zip*. Post extraction, you have the following files.
   - VHD - *FortiGuest_VM64_AWS-v1.3.0-[build0xxx].vhd*
   - Import script - *import2awsimg.sh*
6. Run the *import2awsimg.sh* script to import the VM.
   Note: To import the VM, you must have read & write permissions to the Amazon bucket, EC2 Snapshot, and image create/import.
7. Launch an instance from the Amazon Machine Images (AMI). Select **Images > AMI** in the EC2 service interface and select the image that you just imported. Click **Launch instance** from AMI.



8. Update the configurations on this page. Select the instance type and configure the disk size to 500 GB. Click **Launch instance**.



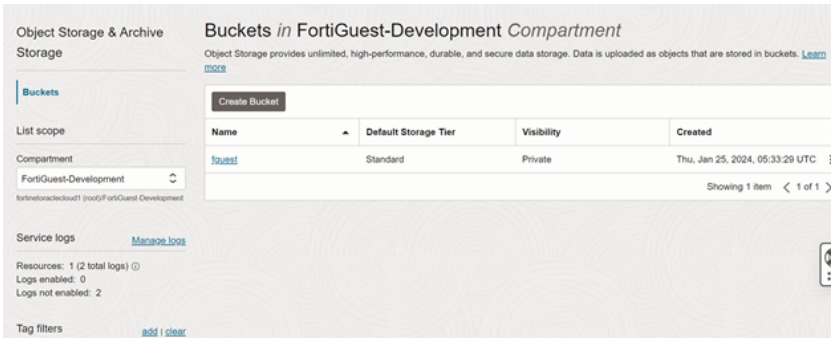
9. Obtain the public IP address of the instance from the EC2 service interface and connect via a private key using SSH.

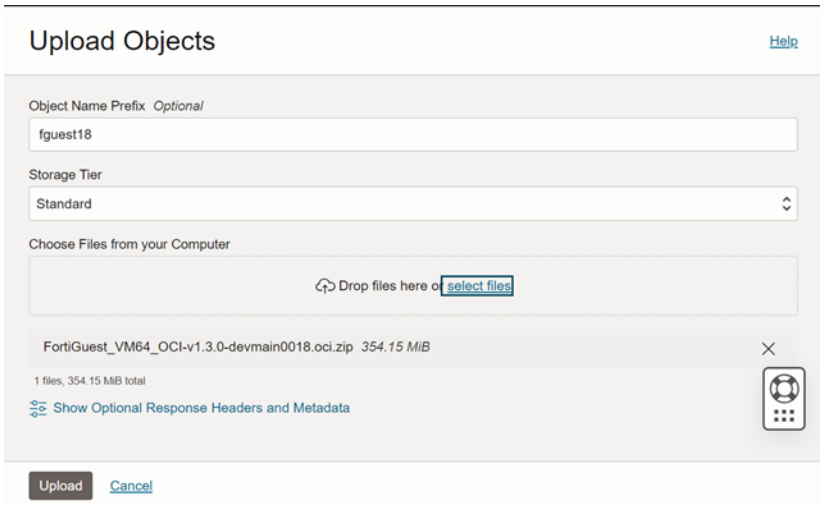
```
> ssh -i ../zhultest.pem admin@54.245.74.
FOSAWS #
 config      Configure object
 get         Get dynamic and system inform
 show        Show configuration
 execute     Execute static commands
 exit        Exit the CLI

FOSAWS # show
config system global
end
config system interface
    edit port1
        set mode dhcp
        set allowaccess ssh
    next
end
config system route
end
config system dns
end
config system ntp
end
config system admin
    edit admin
    next
```

Oracle Cloud Infrastructure (OCI)

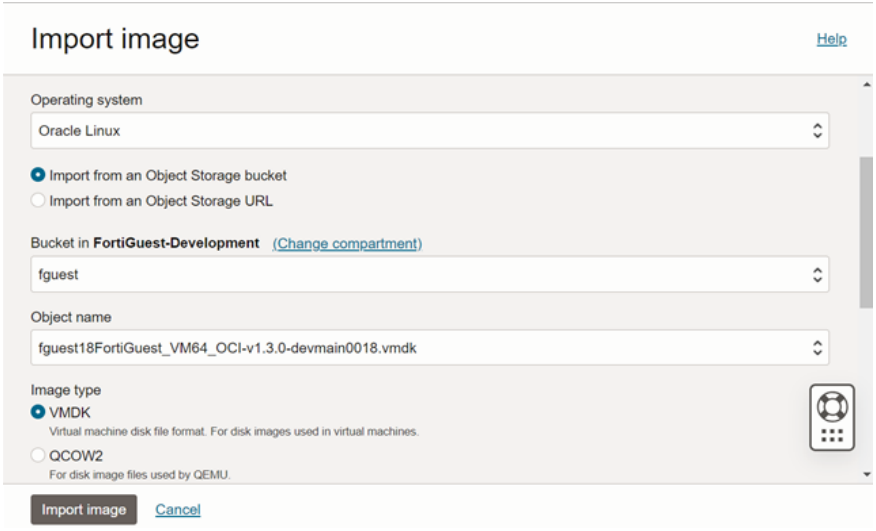
Perform the following steps to deploy FortiGuest on OCI, for more information, see OCI Documentation.

1. Obtain the file *FortiGuest_VM64_OCI-v1.3.0-[build0xxx].oci* from Fortinet.
2. To create a Bucket in OCI, log in to your OCI account and navigate to the **Object Storage & Archive Storage > Buckets > Create Bucket** in the OCI portal.
3. Enter a unique name for your Bucket and select the relevant *Compartment*.
4. Click **Create** or **Confirm**.

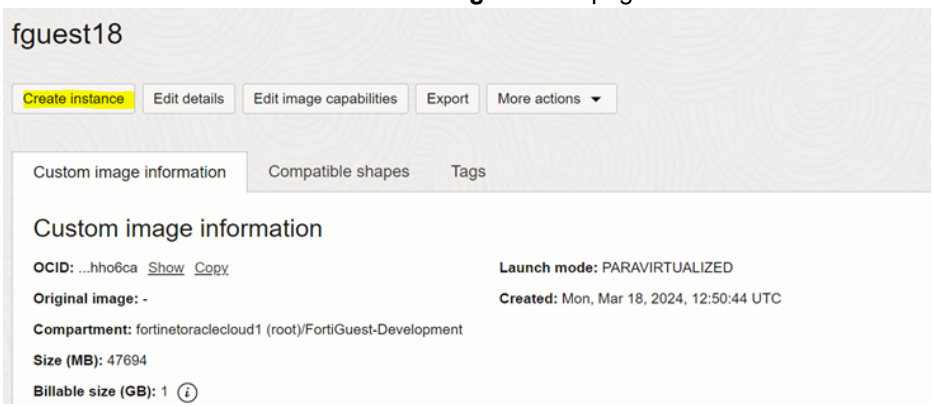




5. Extract the file *FortiGuest_VM64_OCI-v1.3.0-[build0xxx].oci* to obtain *FortiGuest_VM64_OCI-v1.3.0-[build0xxx].vmdk*. Navigate to **Object Storage & Archive Storage > Buckets > Create Bucket** in the OCP portal.
6. Select **Custom Images** and import the extracted VMDK file.

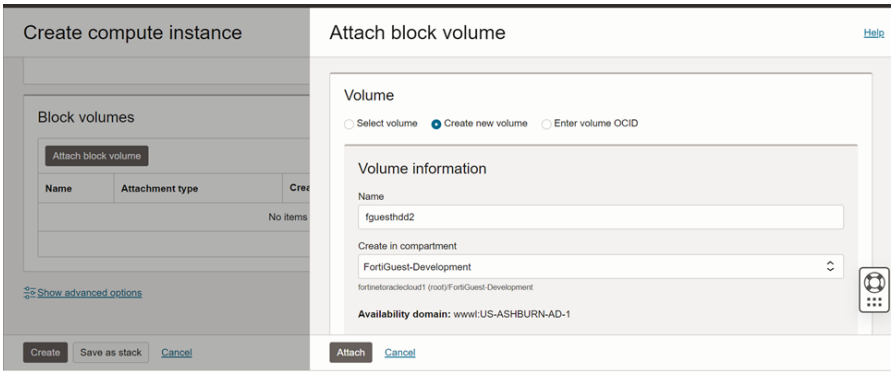


7. Create an instance with the uploaded custom image. Navigate to **Compute Service** in the OCI portal.
8. Click **Create instance** in the **Custom image details** page.



9. In the **Shape Series**, set the number of CPUs to 4 and RAM to 16 GB as per your requirements. Wait for the import process to complete. This may take 6-10 minutes (approximately).

10. Select **Block Volumes > Attach block volume** and attach a 500 GB block volume to the instance.



11. Save any private keys or SSH keys that you may need to access the instance.

Deploying FortiGuest on VM Platforms

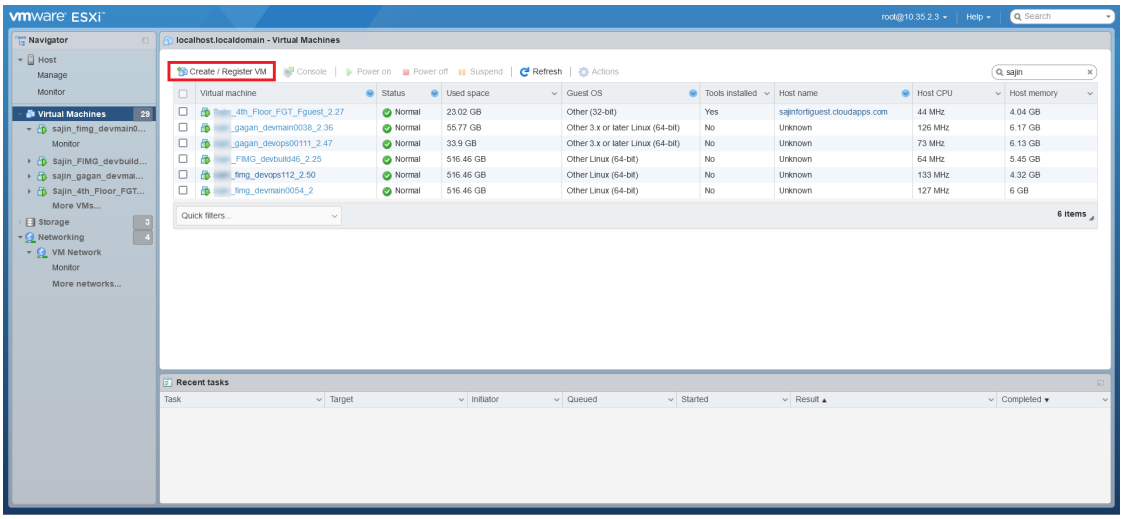
You can deploy FortiGuest on VMWare ESXi, Hyper-V, and Linux KVM.

- Deploying FortiGuest on VMWare ESXi
- Deploying FortiGuest on Linux KVM.
- Deploying FortiGuest on Windows Hyper-V
- Deploying FortiGuest on Nutanix
- Deploying FortiGuest on Proxmox

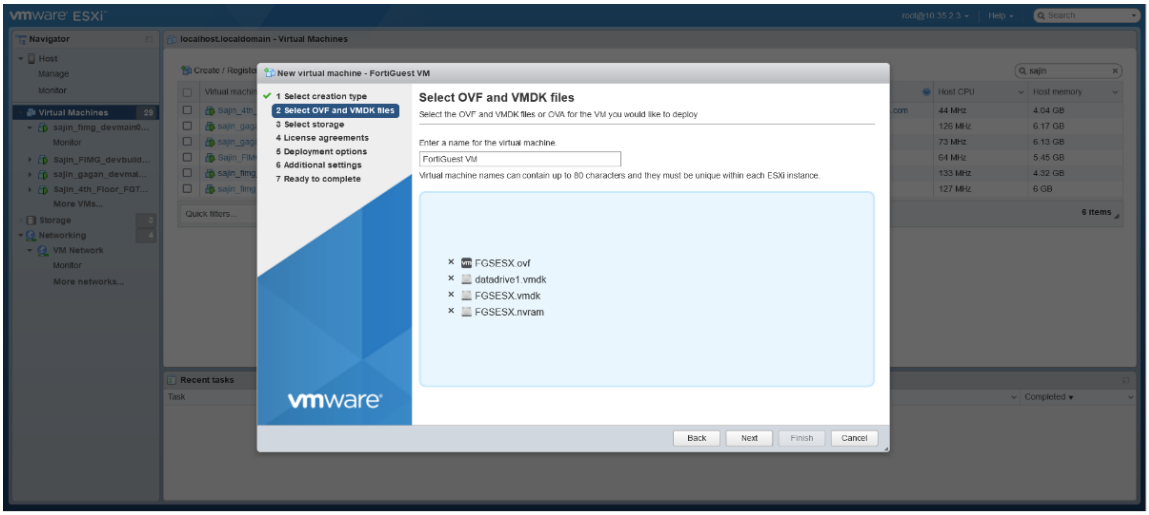
Deploying FortiGuest on VMWare ESXi

Perform the following steps to create and configure FortiGuest on the VMware ESXi server 7.0.3 and above.

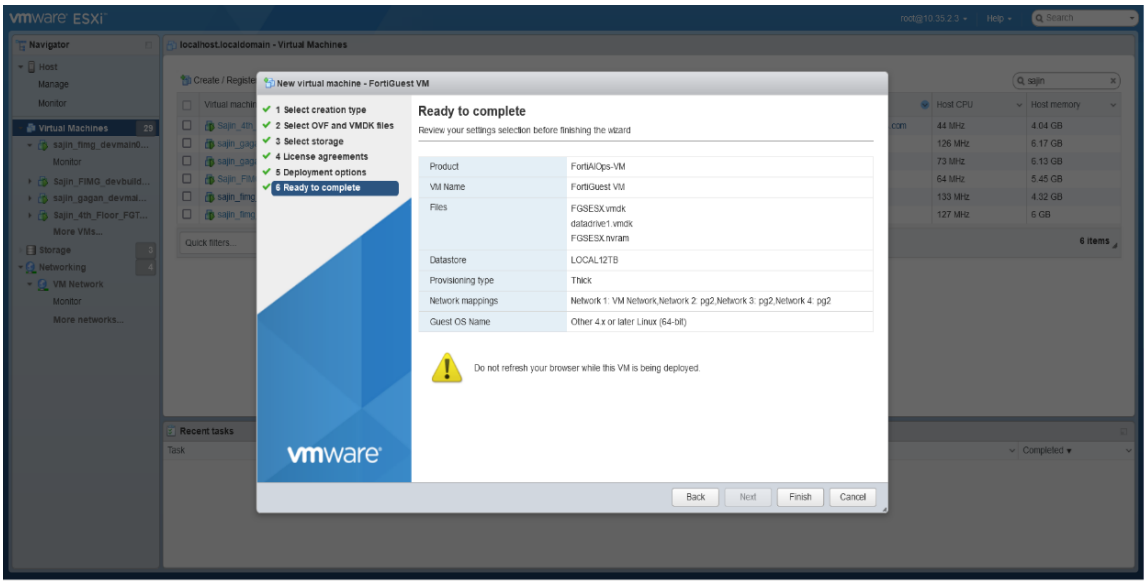
1. Download the FortiGuest *.ovf* zip installation file from the *Fortinet Support* website, for example, *FortiGuest_VM64_ESXi-v1.x.x-build01xx.ovf.zip*.
2. Unzip the downloaded file and extract the *.ovf*.
3. Log in to the VMware ESXi server and click **Create/Register VM**. Select **Deploy a virtual machine from an OVF or OVA file**.



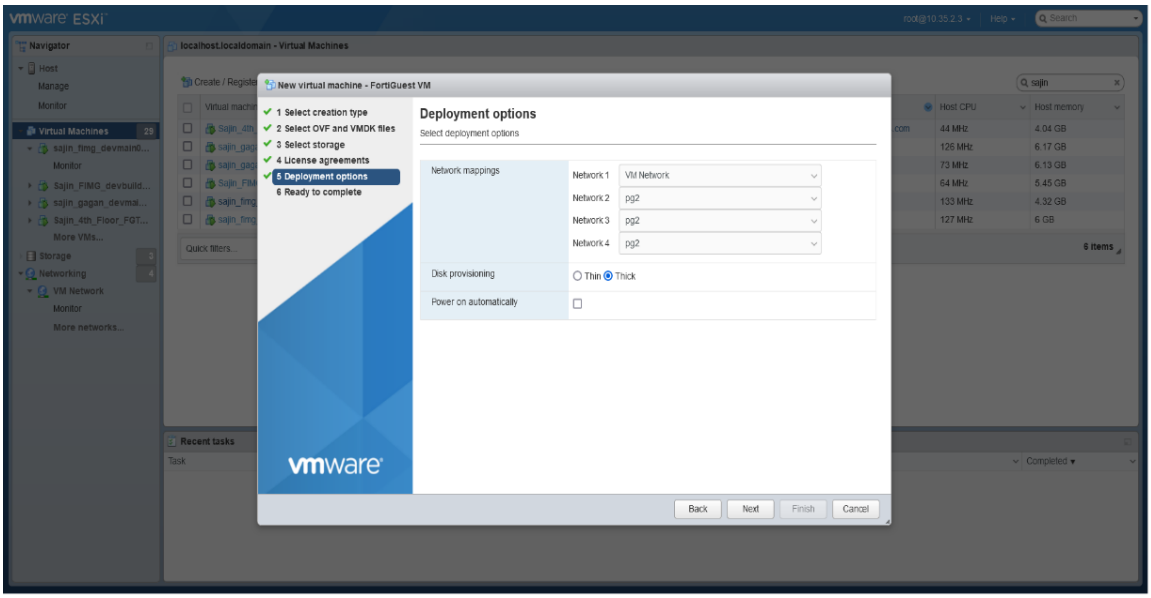
4. Enter a name for the new virtual machine. Browse and select the extracted *.ovf* files or drag and drop all the extracted files to new virtual machine window.



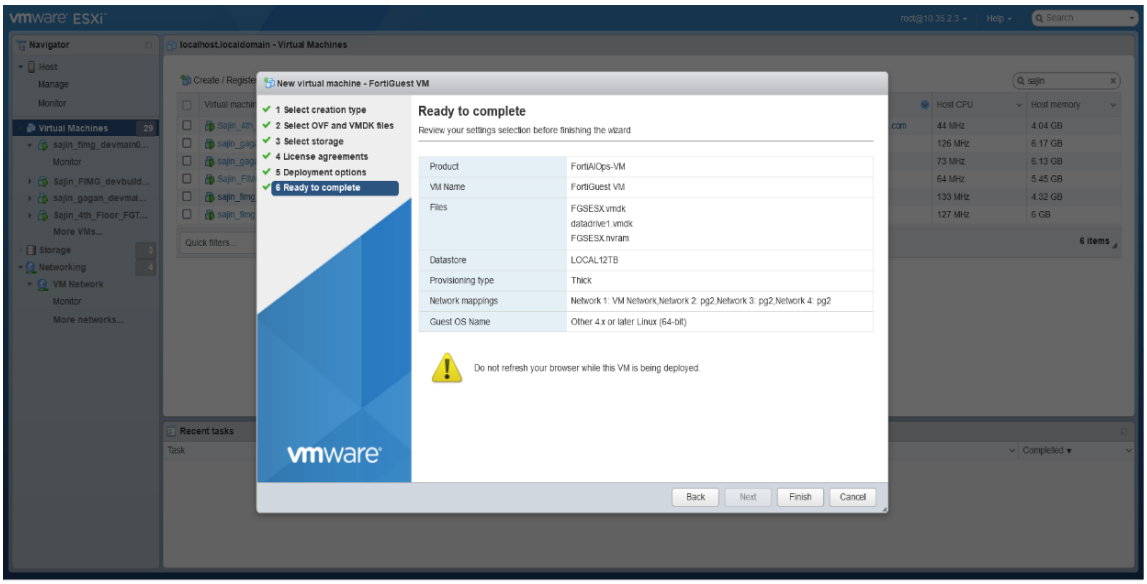
5. Optionally, modify the **Select Storage** settings.
6. Agree to the license agreement.



7. Select the appropriate **Network Mappings** for **Network 1** as per ESXi configuration and select **Thick** as the disk provisioning setting. Disable **Power on Automatically**.



8. Review the details and click **Finish** to create the FortiGuest VM instance.



Deploying FortiGuest on Linux KVM.

Follow this procedure to create and configure FortiGuest on the Linux KVM server.

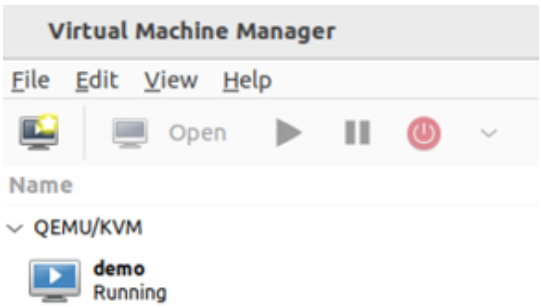
1. Download the FortiGuest *.kvm* zip installation file from the *Fortinet Support* portal, for example, *FortiGuest_VM64_KVM-v1.x.x-devmain00xx.kvm.zip*.
2. Run the `gunzip <FortiGuest Image>` command to extract the installation file.
3. Verify that the executable file **deploy_kvm** is present after extracting.

datadrive.qcow2	12-10-2023 06:36	QCOW2 File	193 KB
deploy_kvm	12-10-2023 06:36	File	4 KB
FGSKVM.qcow2	12-10-2023 06:36	QCOW2 File	5,08,160 KB
Fimg_VARS.fd	10-10-2023 05:45	FD File	528 KB
KVM.xml.tmpl	12-10-2023 06:36	TMPL File	3 KB
OVMF_CODE_4M.secboot.fd	10-10-2023 05:45	FD File	3,568 KB

4. Open terminal and navigate to the directory containing the unzipped installation files.
5. Run the `./deploy_kvm <name of machine>` command to deploy FortiGuest in virt-manager.

```
root@meru:/home/meru/Downloads# ./deploy_kvm demo
virsh define demo.xml
Domain 'demo' defined from demo.xml

Domain 'demo' started
```

6. Open the virt-manager window.

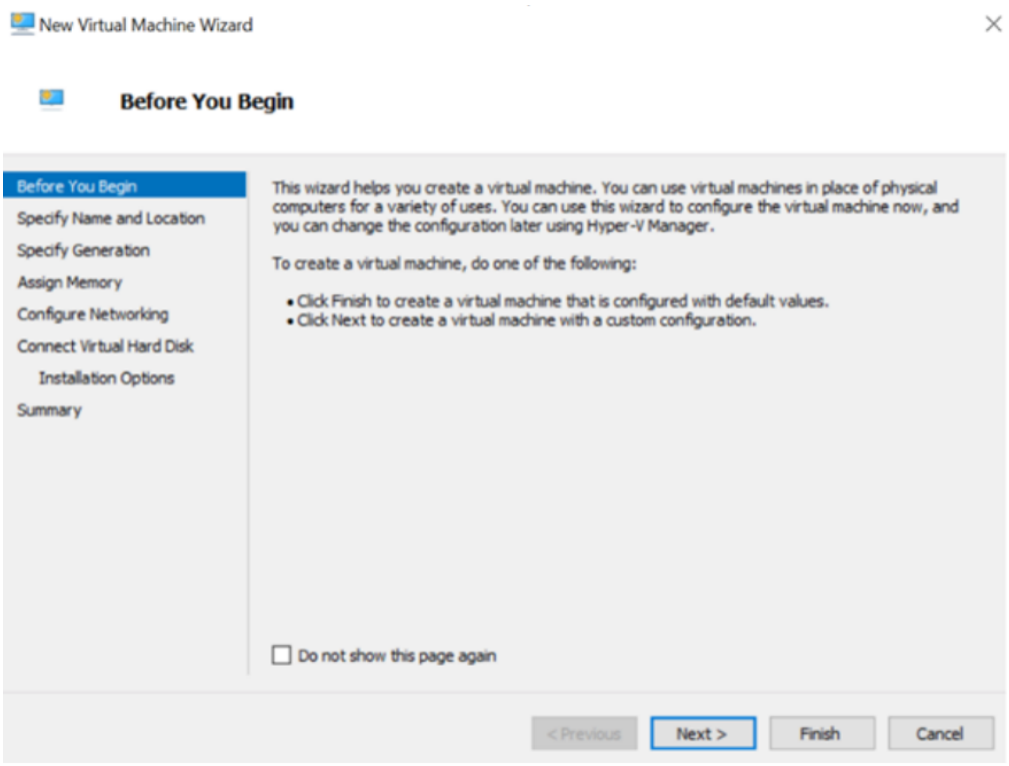


7. Click **Open** to launch the console after the virtual machine is in a running state.

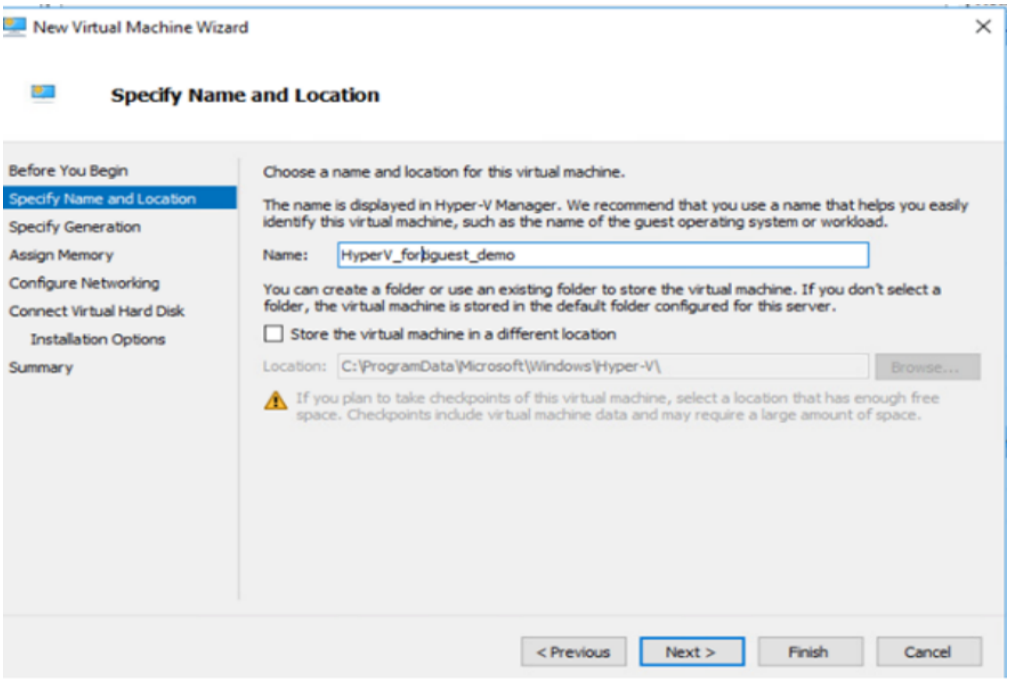
Deploying FortiGuest on Windows Hyper-V

Follow this procedure to create and configure FortiGuest on the Windows Hyper-V.

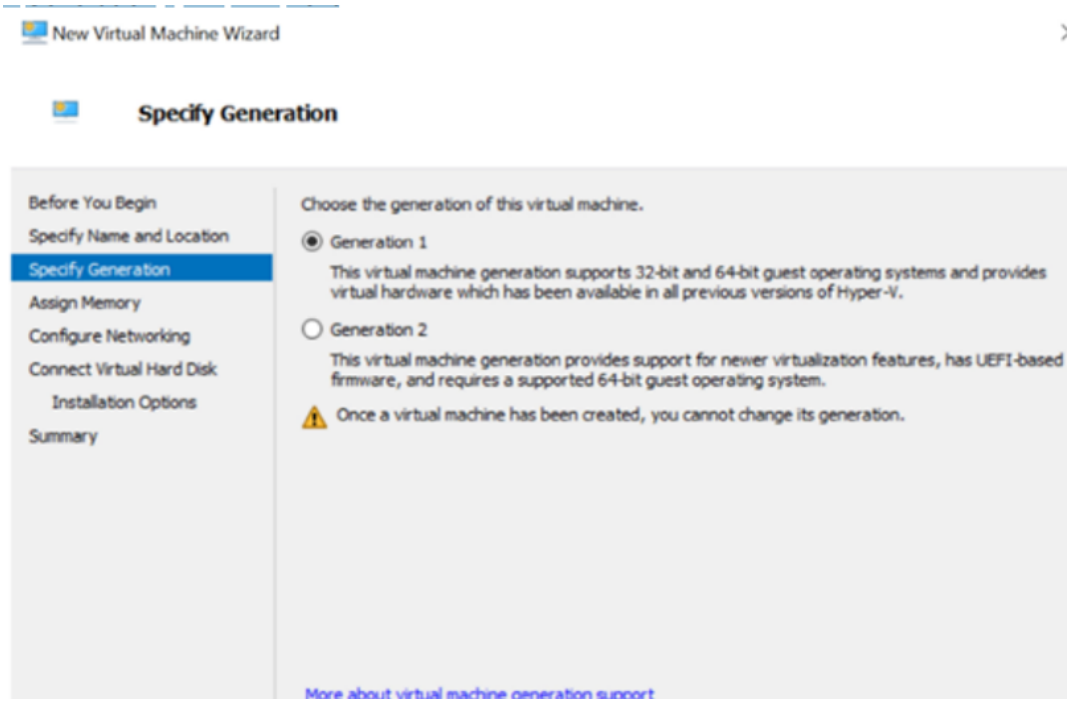
1. Download the FortiGuest *.hyperv* installation from the *Fortinet Support* portal, for example, *FortiGuest_VM64_HV-v1.x.x-devmain00xx.hyperv.zip*.
2. Extract the downloaded installation using any Windows extractor tools.
3. Verify that the *DATADRIVE* and *FGSWHV* files are present after extraction.
4. Open the Hyper-V Manager and in the **Actions** column, click **New** and then **Virtual Machine**.
5. Click **Next** to create a virtual machine with custom configuration.



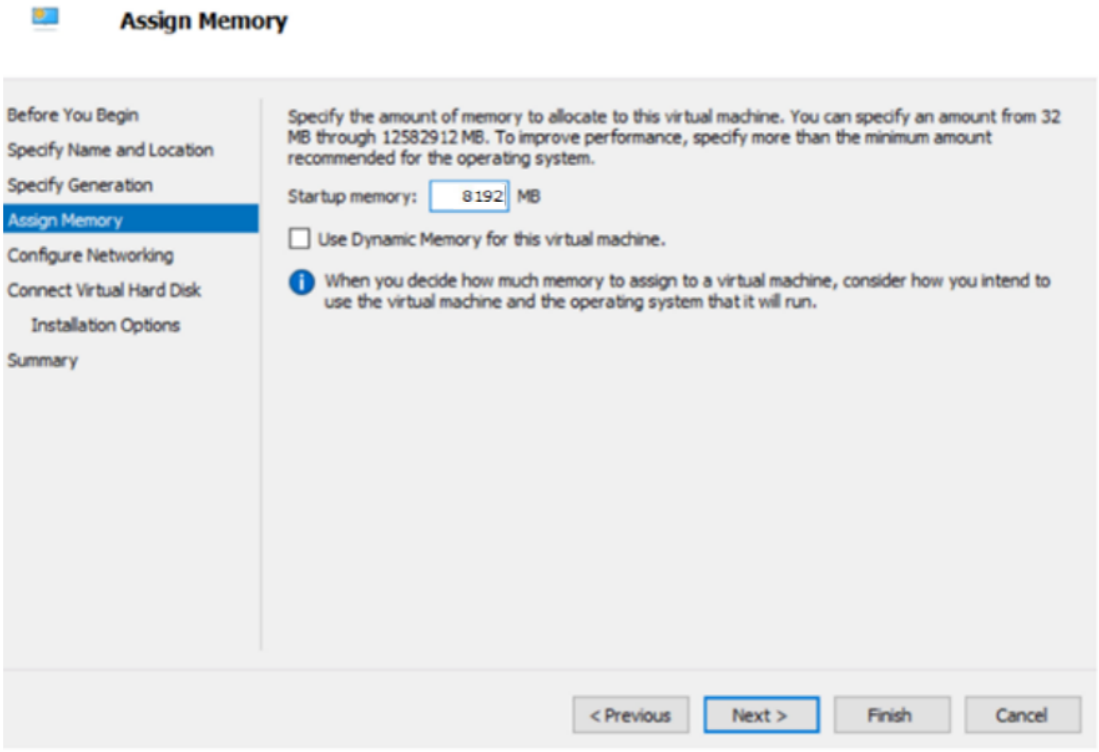
6. Enter a name and location for the virtual machine.



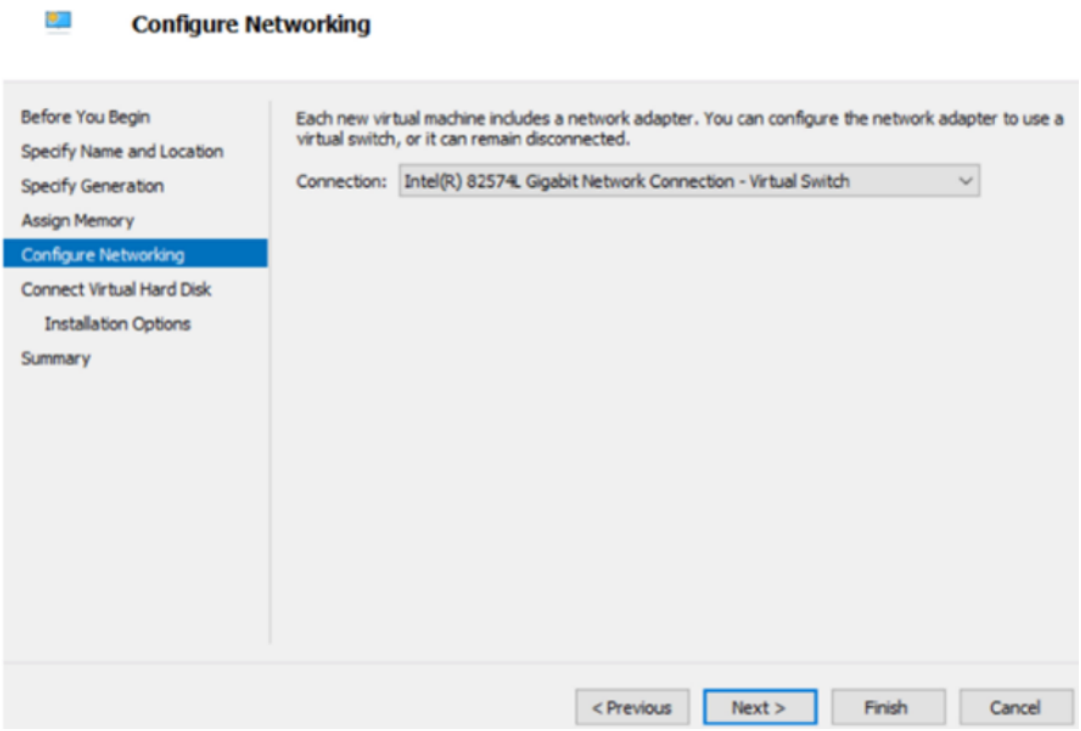
7. Select **Generation 1** and click **Next**.



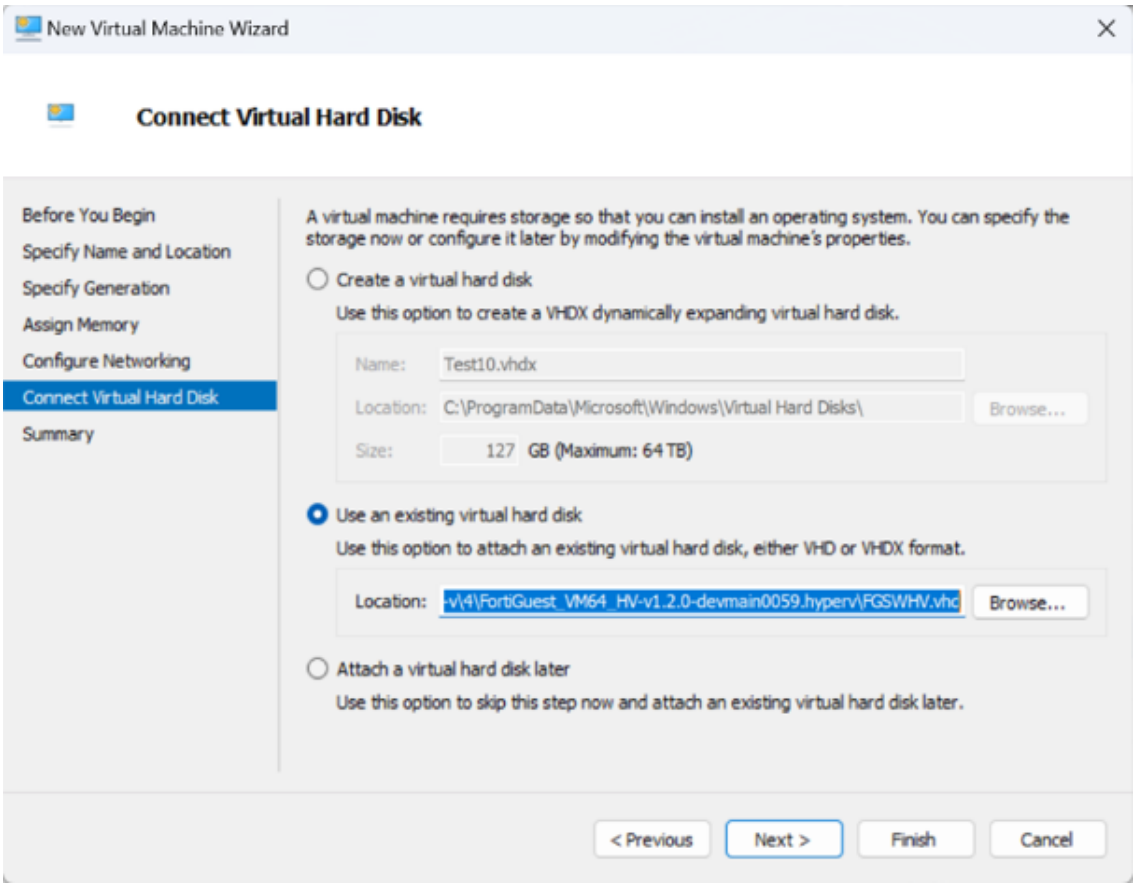
8. Select the amount of memory to allocate to the virtual machine, a minimum of **8 GB** is required. You can use dynamic selection for memory.



9. Select your default switch and click **Next**. You can also connect to any other switch configured in your network.

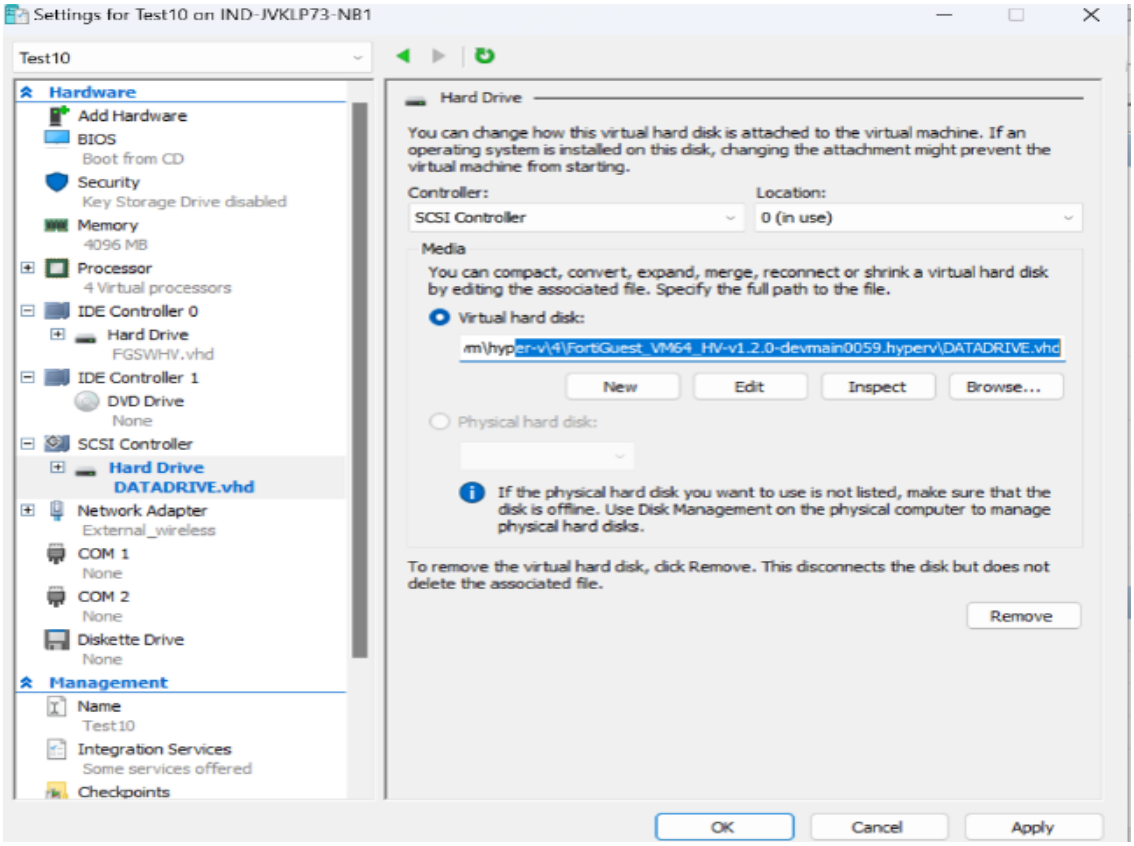


10. Select **Use an existing virtual hard disk** and navigate to the location of the extracted **FGSWHV disk (.vhd)** file and select it.



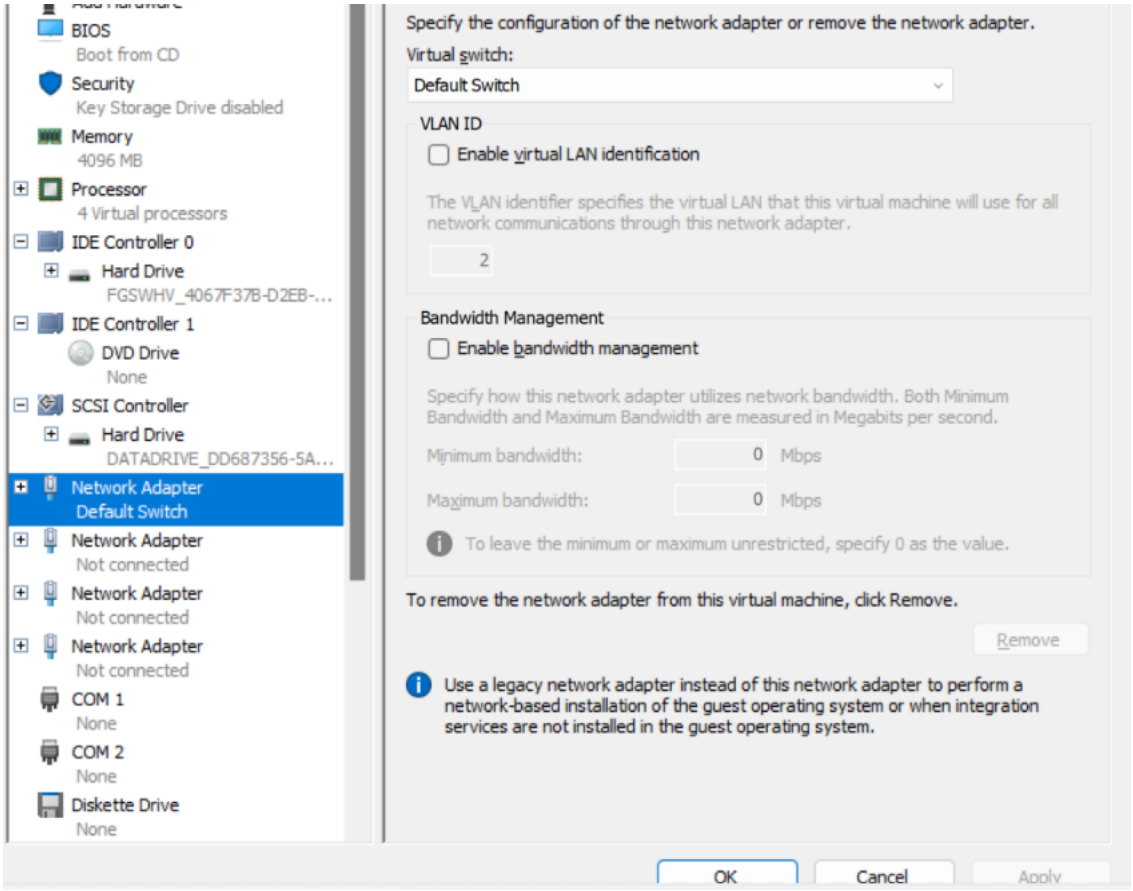
11. Review the details in **Summary** page and click **Finish** to create the new virtual machine.
12. Add the **DATADRIVE** hard drive.
    a. Right-click the FortiGuest virtual machine and select **Settings**.
    b. Click **SCSI Controller**, select **Hard Drive** in the right pane, and click **Add**.
    c. Browse to the extracted **DATADRIVE** file and click **Open**.

d. Click **Apply** and then **OK**.



13. Add four network adapters.
    a. In the Hardware pane, click **Add Hardware.**
    b. Select **Network Adapter** and click **Add.**
    c. Repeat steps 2 previous until you have added four network adapters.
    d. Click **Apply** to save your changes.

Note: Adding four network adapters is mandatory for Hyper-V deployment.

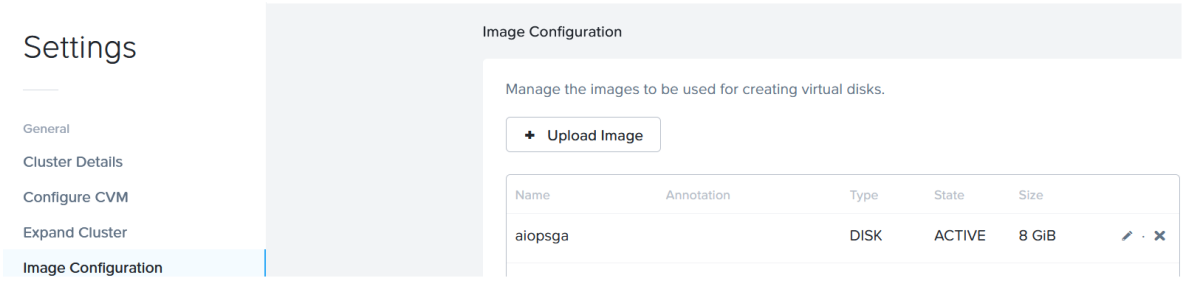


14. Right-click the FortiGuestVM and select **Start** to power-on the VM.
15. Verify the network connectivity and CLI.

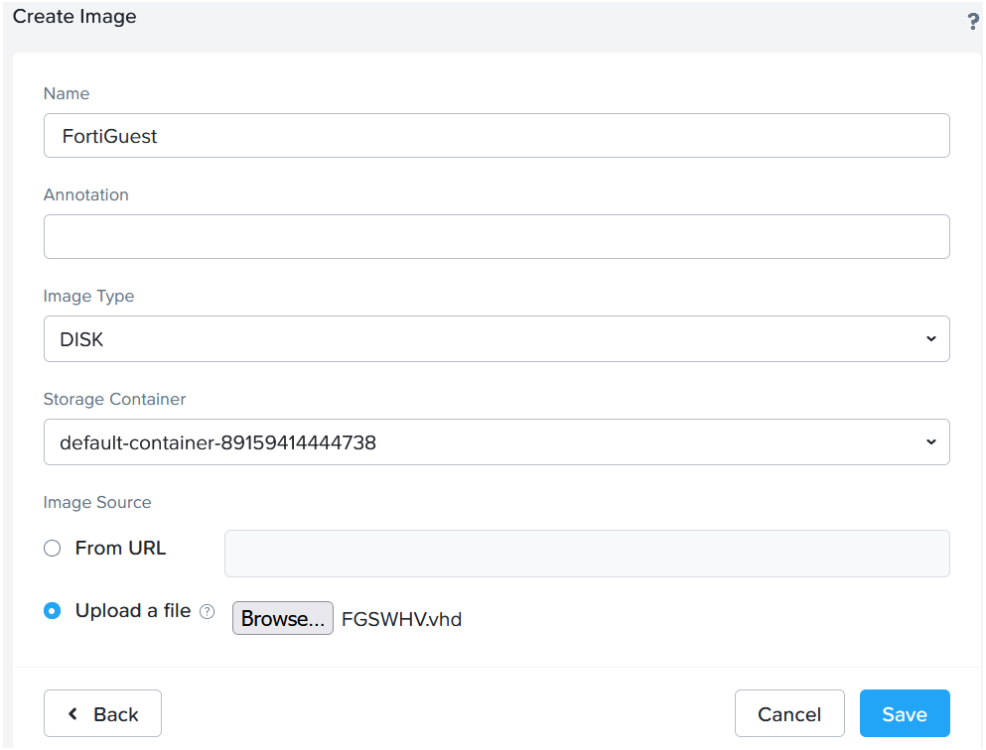
Deploying FortiGuest on Nutanix

Perform the following steps to deploy FortiGuest on Nutanix.

1. Obtain *FortiGuest_VM64_HV-v1.3.0-[build0xxx].hyperv.zip* from Fortinet and extract it to obtain the files *FGSWHV.vhd* and *DATADRIVE.vhd*.
2. Log in into the Nutanix Prism user interface and click the icon. Select **Image Configuration**.



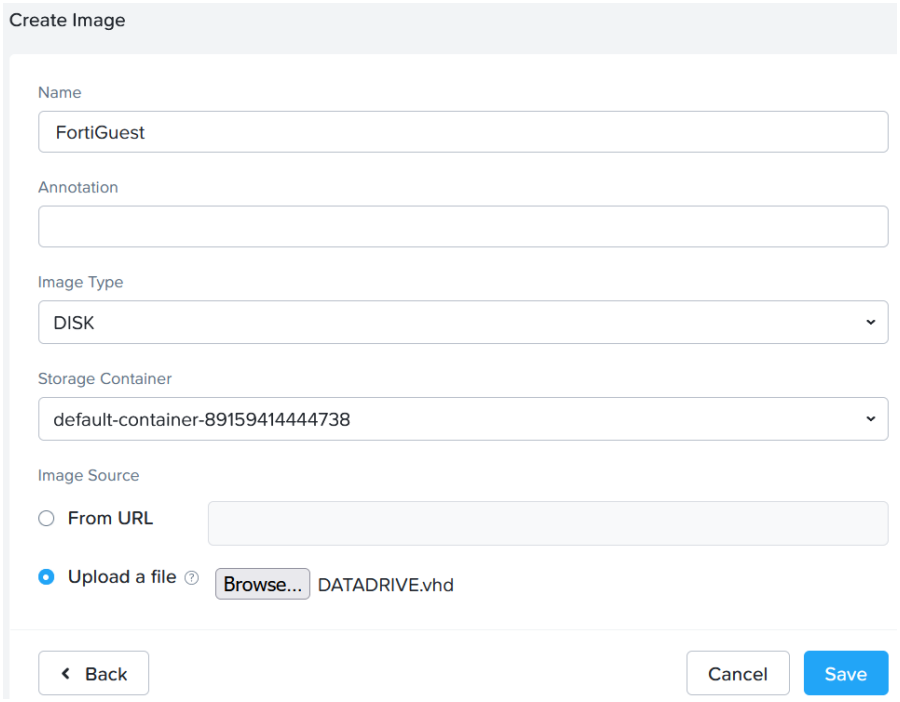
3. Upload both the *FGSWHV.vhd* and *DATADRIVE.vhd* files in the order as mentioned here. To upload *FGSWHV.vhd*, click **Upload Image** and update the following fields.



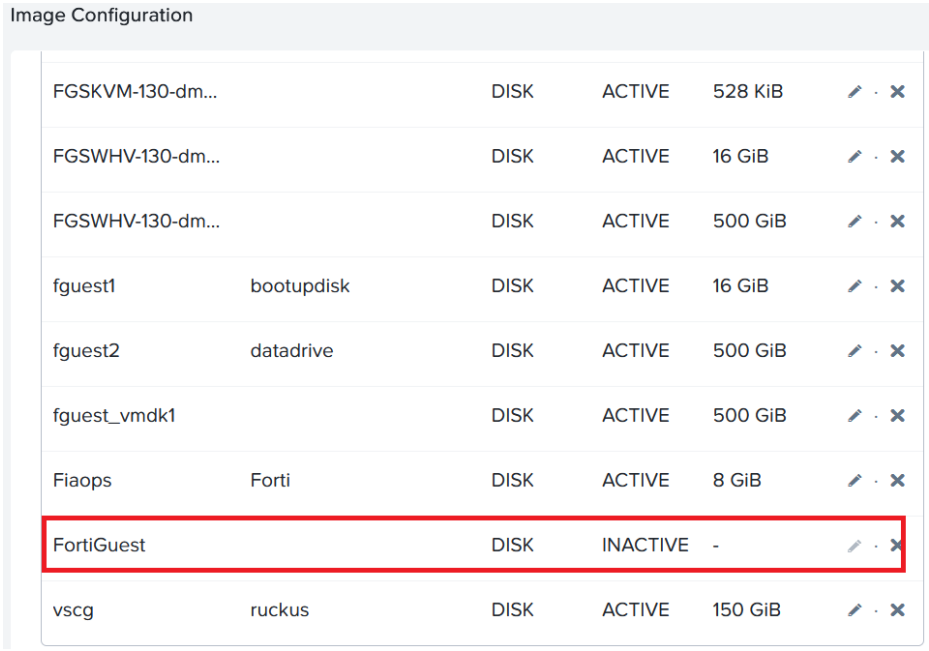
- Enter a **Name** for the FortiGuest image file.
- Select **Disk** in as the **Image Type**.
- Select the **Storage Container**.
- In the **Image Source** section, click **Upload a file** and browse to the FortiGuest image file *FGSWHV.vhd*

4. Click **Save**.

5. Repeat steps 3 and 4 to upload *DATADRIVE.vhd*.



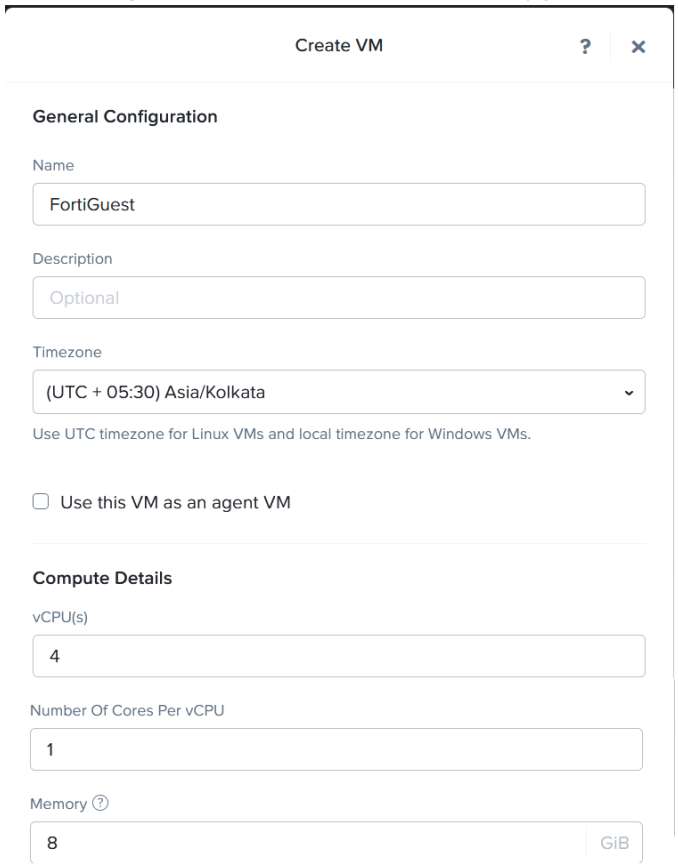
6. Refresh the browser after a few seconds and the newly created images are listed in the **Image Configuration** page.



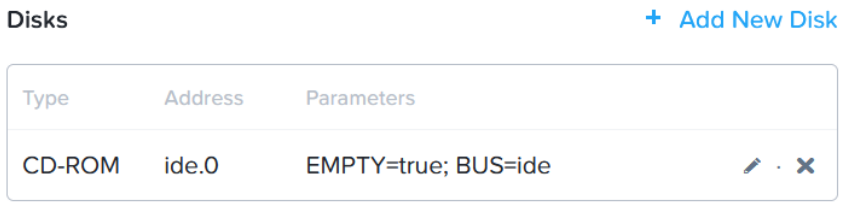
7. To create a VM, navigate to the VM dashboard and click **Create VM** and enter the following configuration.

- Enter a **Name** for the FortiGuest VM.
- Select your **Timezone**.

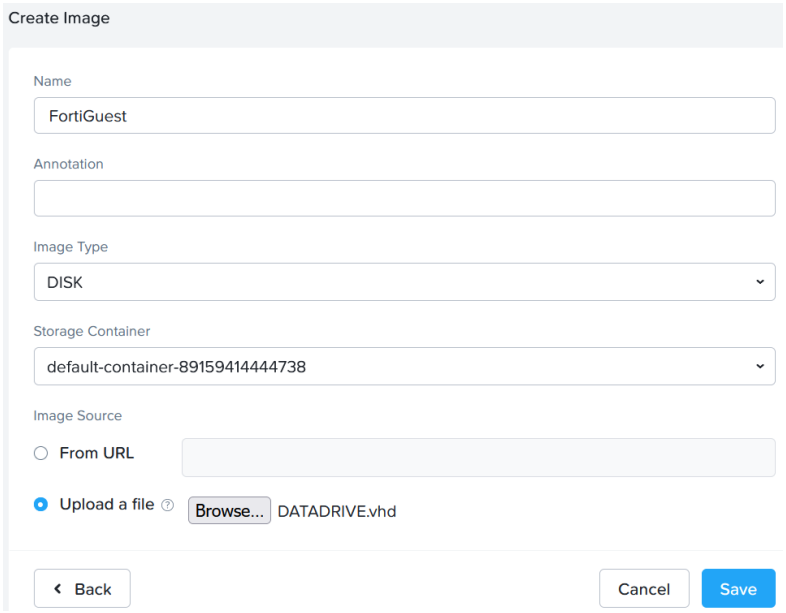
- In the **Compute Details** section, enter 4 **vCPU(s)** and 8 GB of **Memory**.



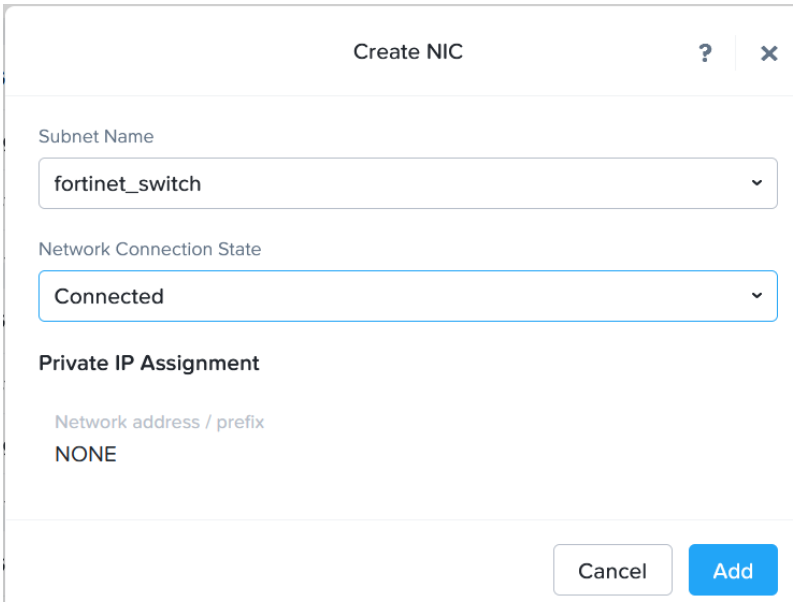
Note: By default, a CD-ROM is listed under **Disks**, delete this CD-ROM.



8. To create a new Boot disk, click **Add New Disk** and enter the following configuration.
   - Select **Clone from Image Service** as the **Operation** and the disk is cloned from the FortiGuest image files uploaded earlier in this procedure.
   - Select **SCSI** as the **Bus Type**.
   - Select the uploaded FortiGuest disk **Image** - *FGSWHV.vhd*.



9. Click **Add**.
10. Add another disk for *DATADRIVE.vhd* following the previous step.
    Note: Ensure to create a new disk for *FGSWHV.vhd* first and then for *DATADRIVE.vhd*.
11. Add 4 Network Adapters, click **Add New NIC**.
    Note: Adding four network adapters is mandatory for Nutanix deployment.

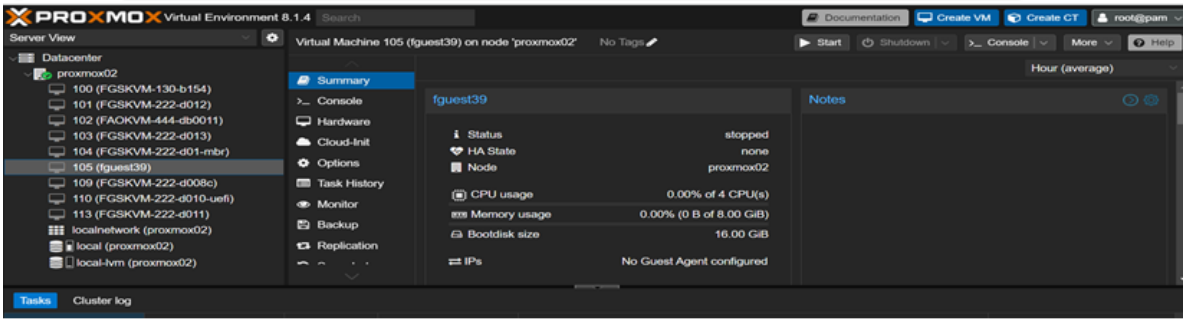


12. Configure the FortiGuest static IP address on starting the VM.

Deploying FortiGuest on Proxmox

Perform the following steps to deploy FortiGuest on Proxmox hypervisor platform.

1. Obtain *FortiGuest_VM64_KVM-v1.3.0-[build0xxx].kvm.zip* from Fortinet.
2. Use SCP to transfer this file to a Proxmox machine and extract it.
```
unzip FortiGuest_VM64_KVM-v1.3.0-[build0xxx].kvm.zip
-rw-r--r-- 1 root root 204608 Mar 27 15:08 datadrive.qcow2
-rwxr-xr-x 1 root root 4541 Mar 27 15:08 deploy_kvm
-rwxr-xr-x 1 root root 2264 Mar 27 15:08 deploy_pmx
-rw-r--r-- 1 root root 533463040 Mar 27 15:08 FGSKVM.qcow2
-rwxr-xr-x 1 root root 540672 Mar 27 14:17 Fimg_VARS.fd
-rw-r--r-- 1 root root 917504 Mar 27 15:08 Fimg_VARS.qcow2
-rw-r--r-- 1 root root 393194388 Apr 22 15:14 FortiGuest_VM64_KVM-v1.3.0-
[build0xxx].kvm.zip
-rwxr-xr-x 1 root root 2749 Mar 27 15:08 KVM.xml.tmpl
-rwxr-xr-x 1 root root 3653632 Mar 27 14:17 OVMF_CODE_4M.secboot.fd
```
3. Import the FortiGuest disk image manually in the Proxmox shell to create the VM.
```
./deploy_pmx -n <name> -v <volume> -b <bridge> [-i <vmid>] [-c <cores>] [-m
<memory>]
```
Where:
   - `<name>` is the name of the VM, for example, *fortiguest-1.3.0*.
   - <`bridge`> is the network bridge to use, for example, *vmbr0*.
   - <`vmid`> is the ID assigned to the new VM; the default is to use the next available free ID.
   - <`cores`> is the number of CPU cores to allocate; the default is 8.
   - <`memory`> is the amount of RAM to allocate (in MB); the default is 8192 MB.
4. The VM is now deployed, edit the settings and add 4 CPUs in the Proxmox user interface.



5. Configure the FortiGuest static IP address on starting the VM.

Note: The supported CPUs include Intel Core i5 and higher.

Specifications for Scale Deployments

The following minimum specifications are required for FortiGuest scale deployments.

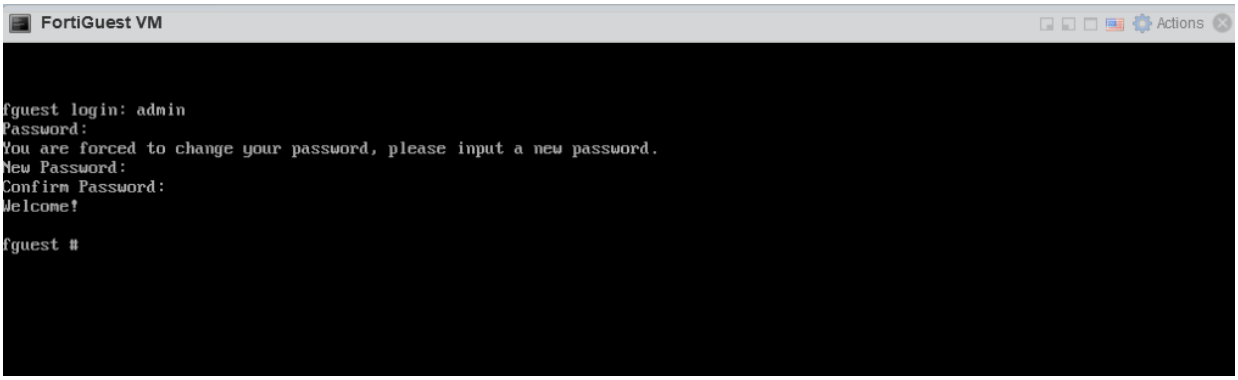
Specification Category	Requirements		
	CPU	Memory	Storage
Low	8 core	8 GB	1 TB

Specification Category	Requirements		
	CPU	Memory	Storage
Medium	16 core	16 GB	1 TB
High	24 core	64 GB	1 TB

Specification Category	Maximum Concurrent Sessions	RADIUS Performance	
		PAP / local database (authentications/sec)	PAP / AD / external database (authentications/sec)
Low	1000	266	161
Medium	10000	486	311
High	10000	653	-
	50000	451	217

Setting up Network IP configuration

Log in to the device from the console using the default username and password (*admin/no password*). Set up a new password and log in to the device using the new credentials.



- Viewing/ Updating Configuration
- Configuring IP Address
- Configuring Hostname
- Configuring NTP

Viewing/ Updating Configuration

Run the `show full-configuration` command to view all of the configured commands in FortiGuest. After making changes, run the `end` or `next` command to commit your changes and make them effective.

Configuring IP Address

Run the following commands to set the IP address.

```
fguest # config system interface
fguest (interface) # edit port1
fguest (port1) # set mode static
fguest (port1) # set ip <IP/CIDR>
fguest (port1) # end
```

Run the following commands to set the gateway.

```
fguest # config router static
fguest (static) # edit 1
fguest (1) # set gateway <your_gateway>
fguest (1) # set device port1 #Same as the port mentioned in interface.
fguest (1) # end
```

Run the following commands to configure the DNS server.

```
fguest # config system dns
fguest (dns) # set primary <Primary_DNS_Server>
fguest (dns) # set secondary <Secondary_DNS_Server>
fguest (dns) # end
```

Note: When a FortiGuest instance is configured, the default IP address is 192.168.1.99/24.

Configuring Hostname

Run the following commands to configure hostname.

```
fguest # config system global
fguest (global) # set hostname <hostname>
fguest (dns) # end
```

Configuring NTP

Run the following commands to configure NTP.

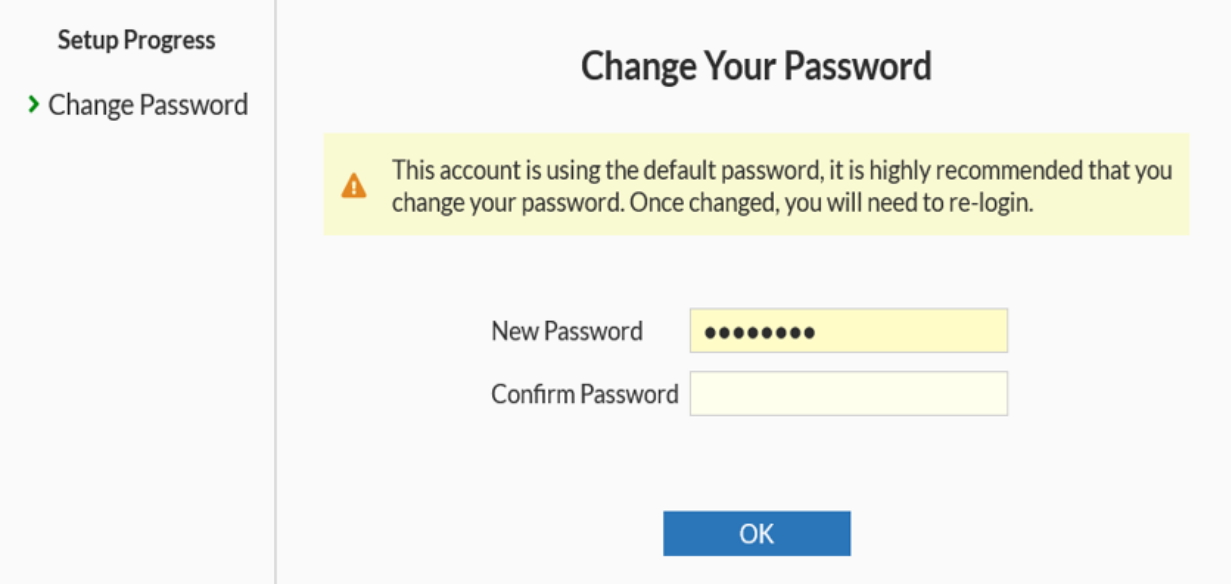
```
fguest # config system ntp
fguest (ntp) # set ntpsync enable
fguest (ntp) # set ntpserver 0.in.pool.ntp.org 1.in.pool.ntp.org
fguest (ntp) # set syncinterval 60
fguest (ntp) # end
```

For complete list of supported commands, see Command Line Interface (CLI) Reference.

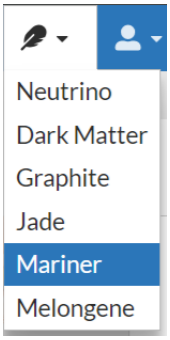
Accessing FortiGuest

After the network IP configuration is complete, log in into the FortiGuest VM as *admin* at *https://[server IP]/adminportal/auth/login* to access FortiGuest GUI, for example, *https://10.39.1.33/admin-portal/auth/login*. Password is not required at first login, you will be prompted to the set a new password.

Note: The GUI admin login and CLI admin login are different. You cannot use the same credentials for both methods.



The FortiGuest administrative portal supports multiple display themes for the user interface. The selected theme is saved in the browser per user, and the same theme is used on subsequent log-ins, unless it is changed. The default theme is *Mariner*.



Upgrading Firmware

Run the `execute restore image` command to upgrade the firmware. The firmware image is loaded from an FTP server or a TFTP server. For example, run `execute restore image ftp <FortiGuest Image location> <FTP Server IP> <username> <password>` command, where:

- `<FortiGuest Image location>` is the path to the FortiGuest firmware image on the FTP server.
- `<FTP Server IP>` is the IP address of the FTP server.
- `<username>` is the username for the FTP server.
- `<password>` is the password for the FTP server.

For complete list of supported commands, see Command Line Interface (CLI) Reference

You can also upgrade FortiGuest in GUI. See Firmware Upgrade.

Licensing

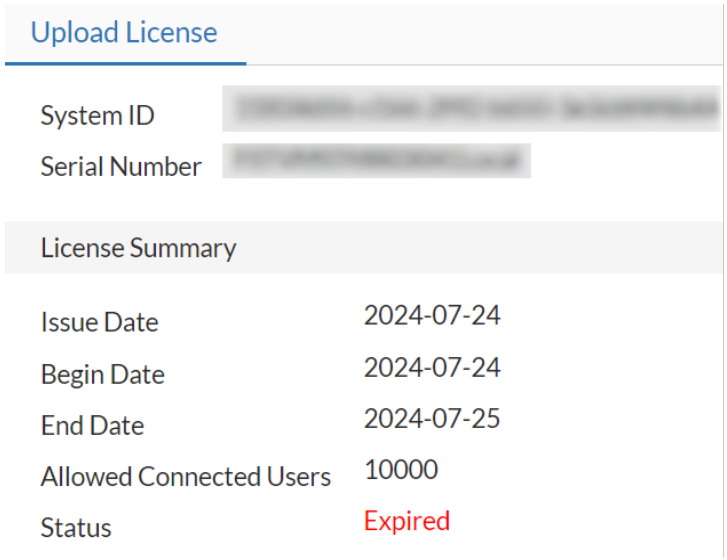
The **System > Licensing** page allows you to view and upload the FortiGuest license file. To obtain the license file, contact *Fortinet Customer Support*.

- Installing License
- License Utilization
- Configuration Restore
- License Expiry and Decrements
- Re-licensing

Installing License

To upload a license file navigate to **System > Licensing**.

1. Click **Upload License File**.
2. In the Upload License File window, click **+ Browse**.
3. Browse and select the license file.
4. Click **OK**.



Note: To renew the license subscription for FortiGuest (valid for one year) before the expiry, contact *Fortinet Customer Support*. The same license is updated and you are not required to procure a new license. You can now view the status of the FortiGuest license on this page, the **Status** is displayed as *Valid* or *Expired*.

License Utilization

Each account type has different license utilization guidelines.

Account type	Description
Guest	• FortiGuest will count the number of guest user accounts in the database, not the number of active connected sessions. • Expired, suspended, pending approval, and rejected accounts are not counted.
Remote	• When authenticating remote users, a corresponding local user account is created and counted.
Device	• Device account license count is independent of user account license count. The device account count is five times the user account count.

Configuration Restore

The following apply to the FortiGuest accounts when restoring configuration.

- If there are any accounts with status suspended, rejected, pending approval, or expired, the account will be imported into the new database as is, with no change in status.
- For accounts with status active or inactive, if the license count is less than the number of accounts being imported, FortiGuest will only restore the number of accounts permitted by the license count.
- Accounts with status active or inactive that were created most recently will be fetched first.
- The remaining accounts with status active or inactive that exceed the current license count will be marked as unlicensed. This allows the administrator to identify the unlicensed accounts on the user interface.

License Expiry and Decrements

When the license expires, FortiGuest performs the following actions.

- Un-license all active and inactive accounts in the database. Accounts with other statuses will remain as is.
- Display an error message in the system logs indicating that the license has expired. After a 24-hour grace period, the accounts will be unlicensed.

If the license count is decreased, FortiGuest will reduce the number of accounts in the database to match the new count.

Re-licensing

Re-licensing is applicable to accounts with the following conditions.

- Unlicensed during a database restore
- Unlicensed because of license expiry or decrements

The administrator can either choose to re-license the accounts individually or choose to re-license all the accounts, provided there is space for re-licensing the accounts.

Command Line Interface (CLI) Reference

You are required to set up a new password after logging in for the first time. The password must be 8-12 characters long. Open the CLI and log in as the admin user (admin). Change the password at the admin prompt and the CLI administration menu is displayed.

The following commands are supported for FortiGuest.

Configuration Commands

The following commands are available to configure FortiGuest.

Command	Parameters	Description
config system interface	?	Displays the various parameters available for this command.
	edit <interface port>	Edit the interface port and enter the port setting mode in the CLI.
	?	Displays the various parameters available for this command.
	abort	Aborts the port setting mode and exits.
	next	Returns to the interface configuration mode.
	set mode <static|DHCP>	Configure the port IP address mode; static or DHCP.
	set ip <IP/netmask>	Configure the port IP address (static).

Command	Parameters	Description
	`set allowaccess <ssh|https|http|ping>`	Configure the admin access type; SSH, HTTP, HTTPS, Ping, or SNMP.
	`unset ip`	Removes the configured IP address.
	`unset allowaccess <ssh|https|http|ping>`	Removes the specified admin access.
	`unset mode`	Sets the port IP addressing to default mode.
	`unset dns-server-override`	Sets the dns-server-override to default setting.
	`get`	Obtain the system information.
	`show`	Displays the current interface configuration details.
	`end`	Exit the port configuration mode; the configuration changes then take effect.
`config system`	`admin`	Configures admin users. `edit admin` - Edit admin user details. `set password` - Set the admin user password.
	`dns`	Configures DNS and enters the DNS configuration mode. `set primary` - Configures the primary DNS server.

Command	Parameters	Description
	`global`	Configures global settings and enters the global configuration mode.
	`interface`	Configures the system interface.
	`ntp`	Configures system NTP information. • `set ntpsync` - Enable/disable the system time by synchronizing with the NTP server. • `set ntpserver` - Configure the IP address or hostname of the NTP servers (up to 10).
config route	`static`	Edit the IPv4 static routing tables and enter route configuration mode.

Show Commands

The following commands can be used for viewing configuration information.

Command	Parameters	Description
`show`		Displays bootstrap configuration.
`show full-configuration`		Displays all configuration (includes defaults).

Diagnostic Commands

The following commands are used to diagnose and troubleshoot issues.

Command	Parameters	Description
diagnose	?	Displays the various parameters available for this command.
	hardware ?	Displays the various parameters available for this command.
	hardware deviceinfo disk	Displays information of all disks.
	hardware deviceinfo nic	Display the available list of NICs.
	hardware deviceinfo <nic name>	Displays information of a specific NIC.
	hardware lspci	Displays the PCI parameters.
	hardware lspci tree	Displays PCI bus tree.
	hardware lspci verbose	Displays detailed information about all devices.
	hardware sysinfo ?	Displays the various parameters available for this command.
	hardware sysinfo cpu	Displays detailed information for all installed CPU(s).
	hardware sysinfo interrupts	Displays details of system interruptions.
	hardware sysinfo iomem	Displays the memory map of I/O ports.
	hardware sysinfo ioports	Display the address list of I/O ports.
	hardware sysinfo memory	Displays the system memory details.
	hardware sysinfo mtrr	Displays the memory type range register.
	hardware sysinfo slab	Displays the memory allocation information.
diagnose service	log	Displays service logs.
	start	Starts the specified service.
	status	Displays the status of service.

Command	Parameters	Description
	`stop`	Stops the specified service.
diagnose debug cache	`get`	Displays the Redis cache.
	`hget`	Displays the Redis cache.

Management Commands

The following enable some management and other operations in FortiGuest.

Command	Parameters	Description
`execute`	`?`	Displays the various parameters available for this command.
	`date <YYYY-MM-DD>`	Set the date in the *YYYY-MM-DD* format.
	`time <HH:MM:SS>`	Set the time in the *HH:MM:SS* format.
	`factoryreset`	Resets all the three data disks to the factory default settings and reboots the device.
	`formatlogdisk`	Formats the log disk and reboots the device.
	`ping <destination>`	Ping the host name or IPv4 address.
	`traceroute <destination>`	Traceroute of the host name or IPv4 address.
	`reboot`	Reboot the system.
	`shutdown`	Shut down the device.
	`sysctl sh`	Enter shell environment.
	`backup config ftp <filepath> <ftp server>[:port] [ftp_ user] [ftp_passwd]`	Creates a remote backup of the configuration file using FTP.
	`backup config tftp <filename> <tftp server>`	Creates a remote backup of the configuration file using TFTP server.
	`restore config ftp <filepath> <ftp server>[:port] [ftp_ user] [ftp_passwd]`	Restores the configuration file from an FTP server using specific details.

Command	Parameters	Description
	`restore config tftp <filepath> <tftp server>`	Restores the configuration file from a TFTP server.
	`restore image ftp <filename string> <ftp server>[:port] [ftp_user] [ftp_passwd]`	Restores the firmware image from an FTP server using specific details.
	`restore image tftp <filename string> <tftp server>`	Restores the firmware image from a TFTP server.

System Information

The following commands information related to the system configurations.

Command	Parameters	Description
`get system`	`?`	Displays the various parameters available for this command.
	`status`	Displays system status, such as, version, serial number, BIOS details, time stamp, hostname, and so on.
	`admin`	Displays the configuration details of the admin users.
	`admin <username>`	Displays the configuration details of a specific admin user.
	`dns`	Displays the DNS configuration.
	`global`	Displays the configuration details of global attributes.
	`interface`	Displays the interface details, status, and IP address.
	`interface <port>`	Displays the port details, status, and IP address.
	`ntp`	Displays the configuration details and status of NTP server.

User and Device Accounts

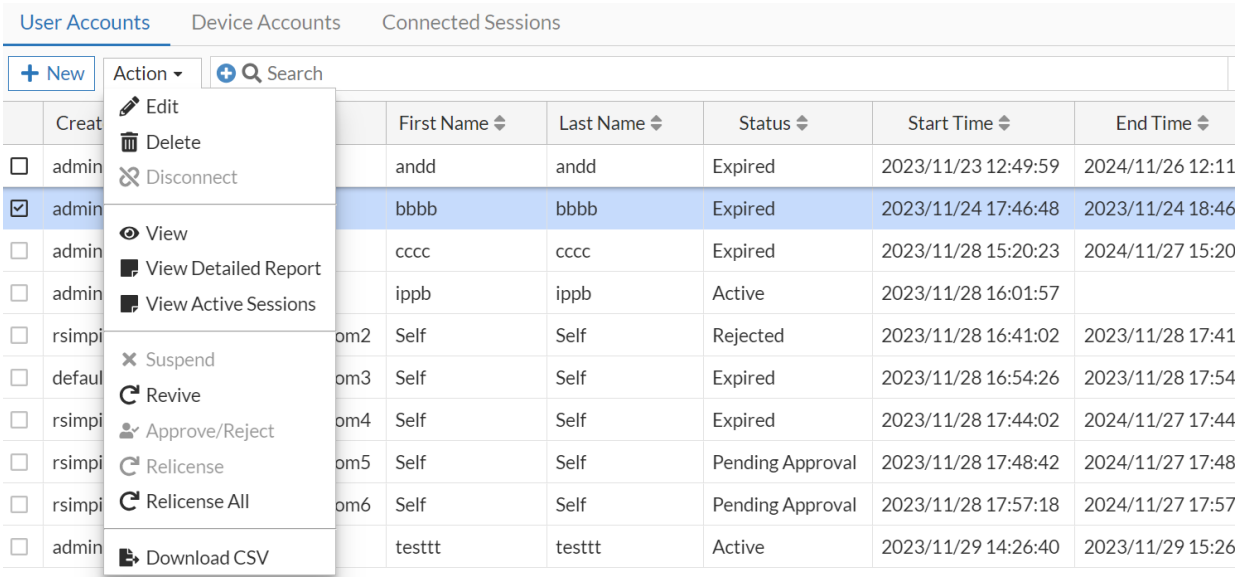
FortiGuest allows you to create network access accounts for your users, visitors, contractors or anyone who needs to access the network. You can create and manage guest user accounts and device accounts that connect to the network.

Note: Prior to creating user accounts, ensure that email notifications are enabled and configured at Email NotificationsThe user credentials are sent only via email.

- Creating and Managing User and Device Accounts
- Creating and Managing Account Batches

Creating and Managing User and Device Accounts

To create and manage user and device accounts, navigate to **Accounts > Manage Accounts**. Select an account and click **Actions** to perform any of the following supported operations.

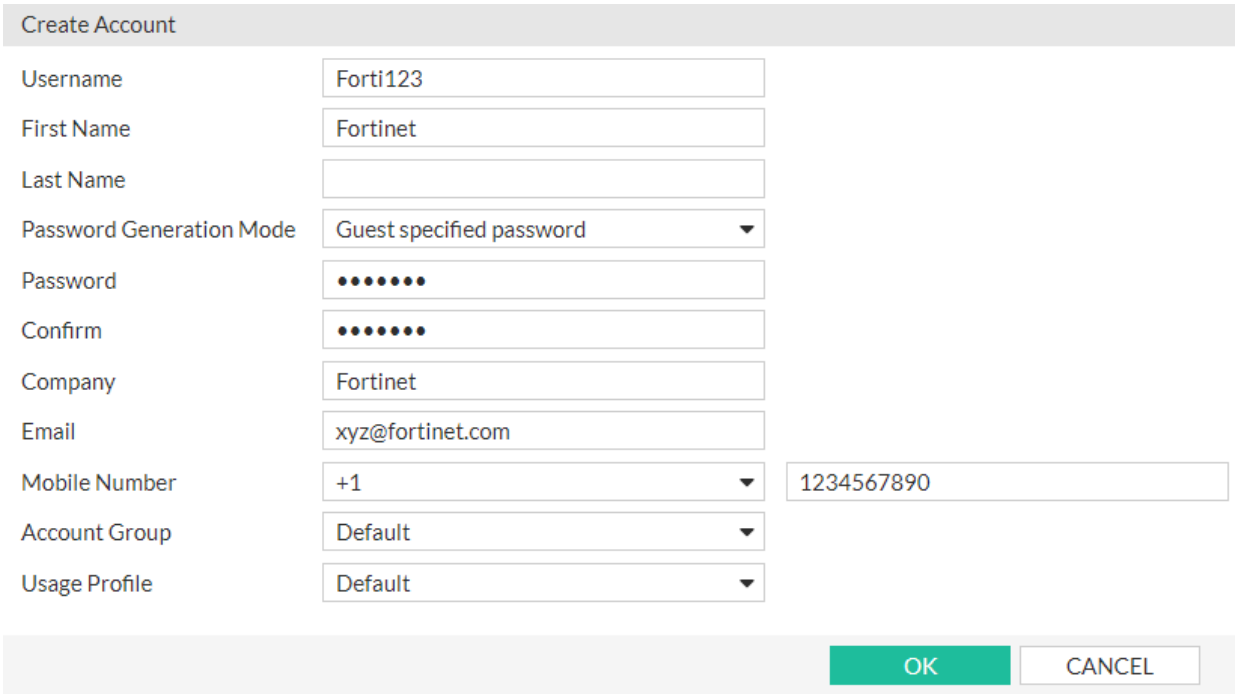


- **Download CSV** - Download the account details in a *.csv* format.
- **View** - View the account details. You can print the account details, suspend the account, or reset the password.
- **View Detailed Report** - View the audit and accounting logs for the selected account.
- **View Active Sessions** - View connected sessions individually for an account.
- **Edit** - Edit the selected account details.
- **Delete** - Delete the selected account.
- **Suspend** - Suspend the selected account to deactivate it temporarily. The account is removed from the list and the user cannot access it anymore. You can revive a suspended account.
  Note: Account suspension works only if FortiGate supports *Change of Authorization*.
- **Disconnect**- Disconnect the selected account to prevent access. You can revive a disconnected account.
  Note: Account disconnection works only if FortiGate supports *Change of Authorization*.

- **Revive** - You can revive a suspended or disconnected account anytime.
  Note: While reviving an account with a new usage profile, ensure that the time zone matches the previous usage profile applied on the account.
- **Approve/Reject** - A sponsor can approve/reject the account before it is activated.
- **Relicense** and **Relicense All** - The administrator can either re-license a selected account or re-license all the accounts, provided there is space for re-licensing the accounts. See Licensing.

Creating User Account

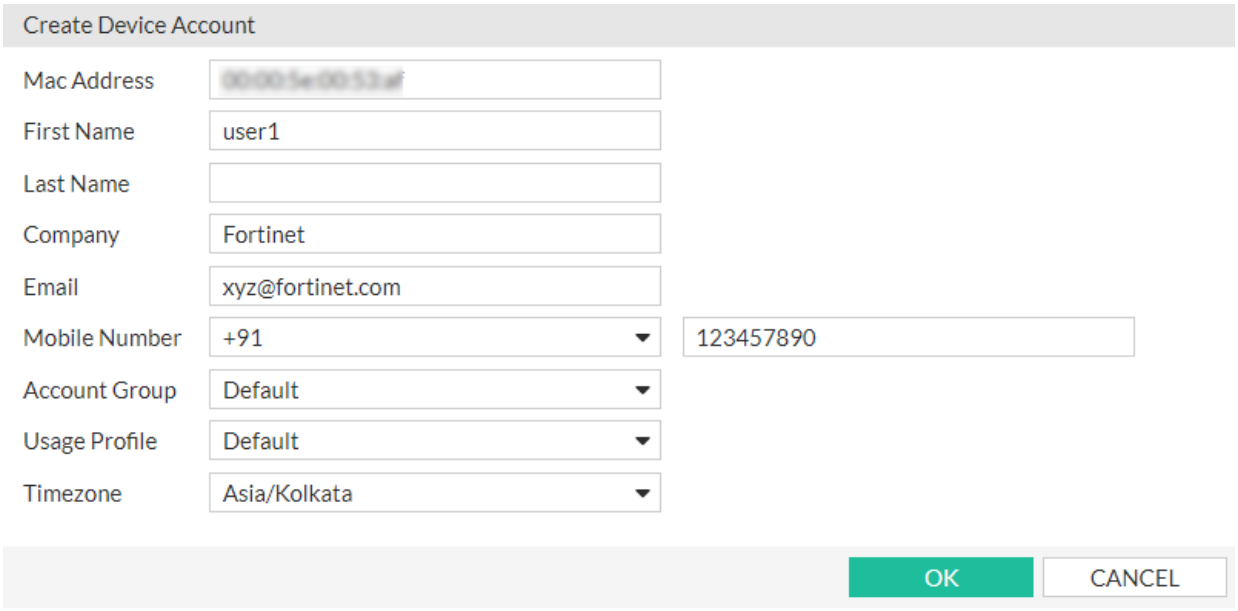
To create a new user account the following user details. The options available to create a user account are as per the configured Policy Details.



- The **Username** of the account.
- The **First Name** and the **Last Name** of the user.
- The **Password Generation Mode**. You can allow the admin to set the password (**Admin specified password**) or enableFortiGuest to generate a password automatically (**Auto generated password**). When the password is admin specified, it must match the password complexity configured in Password Policy.
- The **Password** to access the user account. The password must contain at least 2 characters, 2 numbers and 1 symbol (*!$^()-_=+{}[];:@#~,<>?*).
- The **Company** or organization of the user.
- The user **Email** address.
- The **Mobile Number** of the user.
- Select the associated **Account Group** and **Usage Profile**.

Creating Device Accounts

To create a new device account, provide the following user details.

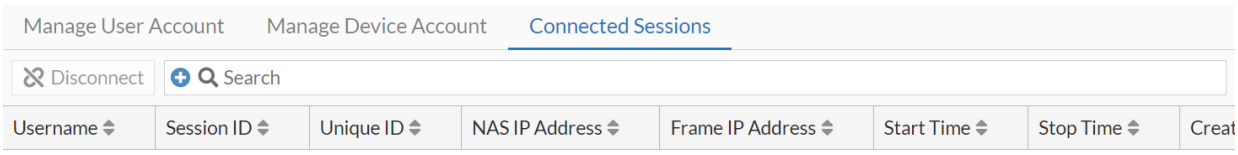


Update the following user details requesting the device be added on to the network.

- The **MAC Address** of the device.
- The **First Name** and the **Last Name** of the user.
- The **Company** or organization of the user.
- The user **Email** address.
- The **Mobile Number** of the user.
- Select the associated **Account Group** and **Usage Profile**.
- Select the **Timezone** relevant to the user.

Connected Sessions

The FortiGuest admin can view all the active and connected sessions You can disconnect one or multiple sessions, select a connected session and click **Disconnect**.



The guest users can now see and manage all sessions (if logged in from multiple devices) of a specific user and disconnect them as required. The guest can either disconnect from an already authenticated device or from a new device, when the concurrent connection limit is exceeded. You can enable session management for a portal in post-auth settings in **Guest Portal > Portals > Settings**, see Settings.

Creating and Managing Account Batches

To create and manage user and device accounts, navigate to **Accounts > Manage Accounts Batches**. Select an account and you can perform any of the following supported operations.

The **Manage Account Batches** page lists all the user and device account batches. You can select any to view the details, optionally, you can also create new batches. Click **New** and you are redirected to the respective user account and device account batch creation page.

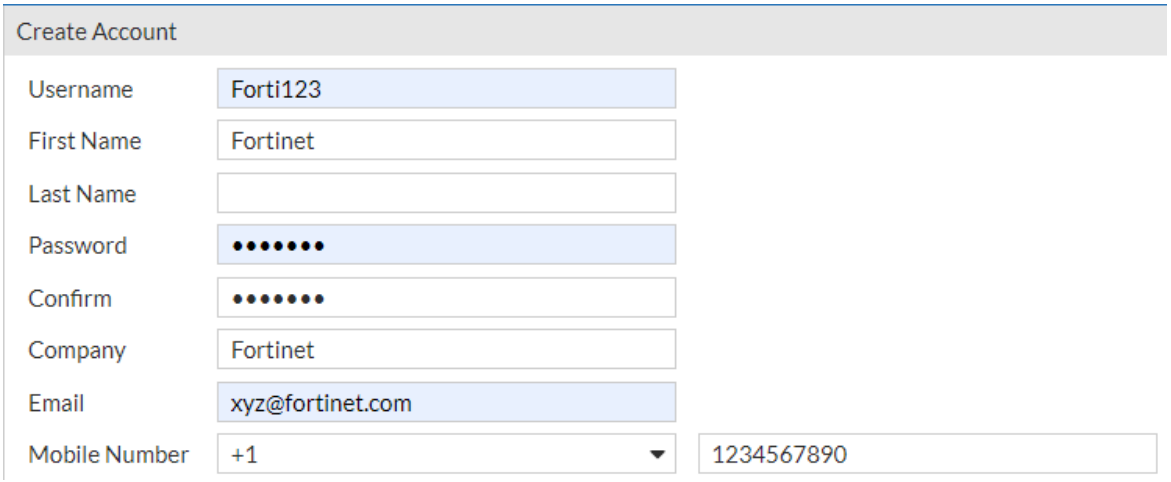
Creating User Account Batch

The FortiGuest allows you to create multiple user accounts at the same time. You can create multiple accounts manually or import from a *.csv* file.

Account Batch

Perform the following steps to create an account batch.

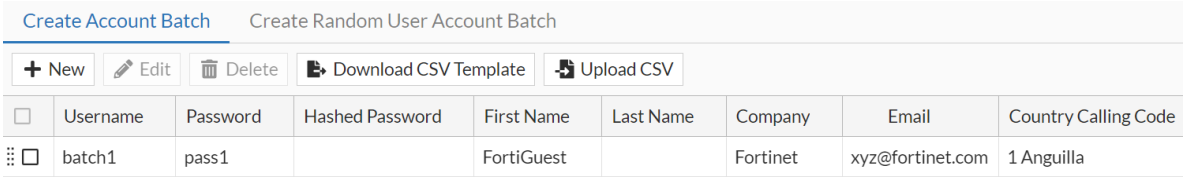
1. Navigate to **Accounts > Create Account Batch** and click **New** to create an account. Update the following user details.



   - The **Username** of the account.
   - The **First Name** and the **Last Name** of the user.
   - The **Password** to access the user account. The password must contain at least 2 characters, 2 numbers and 1 symbol (*!$^()-_=+{}[];:@#~,<>?*).
   - The **Company** or organization of the user.
   - The user **Email** address.
   - The **Mobile Number** of the user.
2. You can import the user account details in a *.csv* format. Click **Download CSV Template** and populate the required fields in the template file. After the template file is updated with user details, click **Upload CSV** to upload it. You can import users with encrypted passwords along with clear text passwords, and upload the same *.csv* to import users into another system.

Note: You cannot import more than 3700 local user accounts using the *.csv* template, at a given time. Currently, multiple iterations are required to import larger number of accounts.

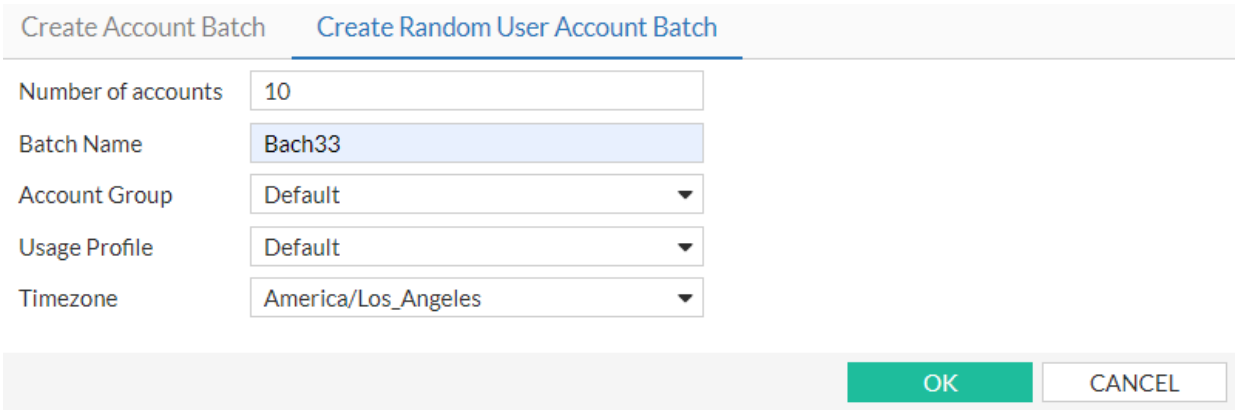
3. You can create an account batch after the user account details are created/imported as described in the previous steps. Update the following details.



- The **Batch Name**.
- Select the associated **Account Group** and **Usage Profile**.
- Select the **Timezone** relevant to the users.

Random User Account Batch

You can create a random user account batch when you need to hand out details to visitors, but do not have access to a computer at a given point in time to create and provide the accounts to users. This feature allows you to create accounts in advance and record the details for correlation at a later time.



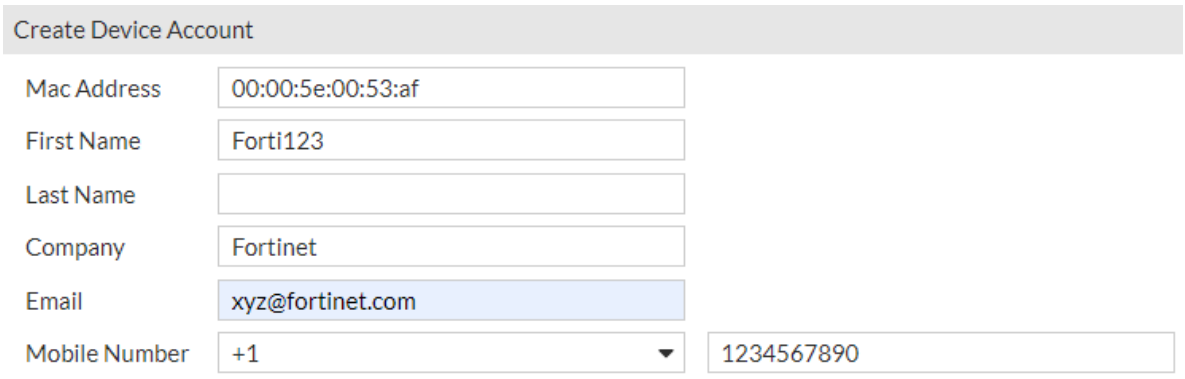
Click the **Create Random User Account Batch** tab and update the following details.

- The **Number of accounts** that you want to generate in this batch.
- The **Batch Name**.
- Select the associated **Account Group** and **Usage Profile**.
- Select the **Timezone** relevant to the user.

Creating Device Account Batch

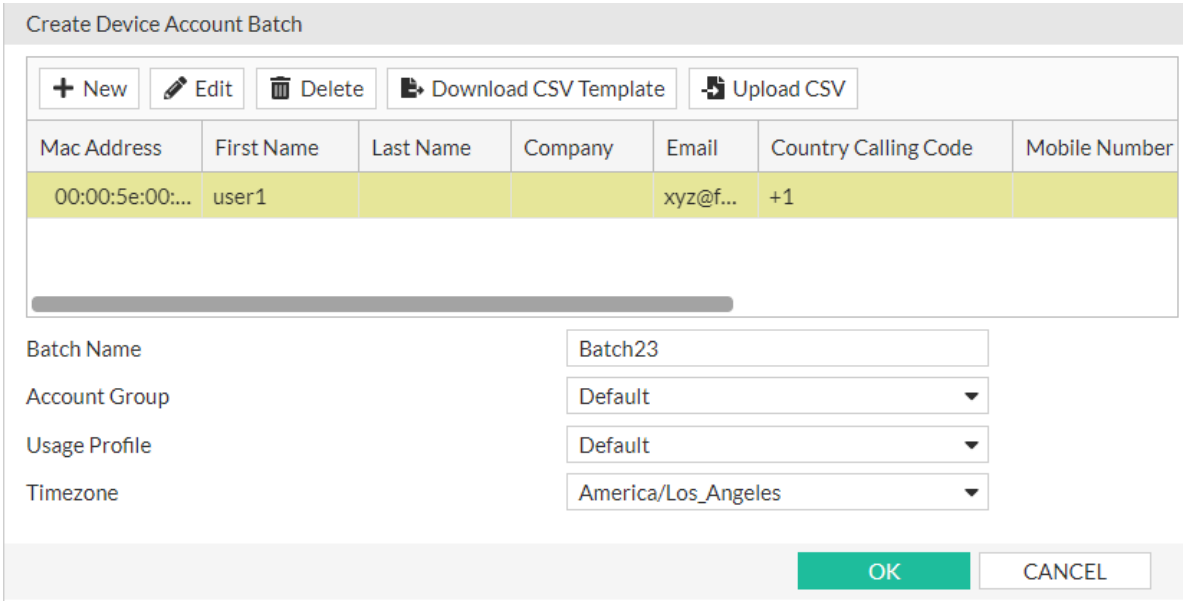
The FortiGuest allows you to create multiple device accounts at the same time. You can create multiple device accounts manually or import from a *.csv* file.

1. Navigate to **Accounts > Create Device Account Batch** and click **New** to create an account. Update the following user details requesting the device be added on to the network.



- The **MAC Address** of the device.
- The **First Name** and the **Last Name** of the user.
- The **Company** or organization of the user.
- The user **Email** address.
- The **Mobile Number** of the user.

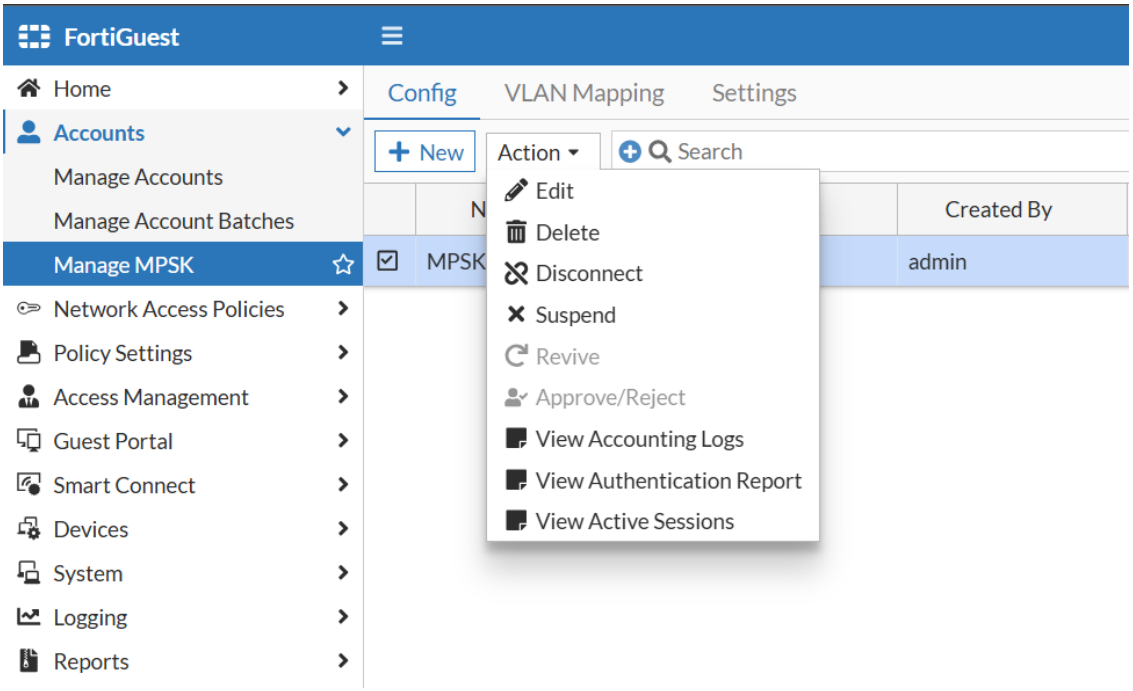
2. You can import the device account details in a *.csv* format. Click **Download CSV Template** and populate the required fields in the template file. After the template file is updated with device/user details, click **Upload CSV** to upload it.
3. You can create an account batch after the device accounts are created/imported. Update the following details.



- The **Batch Name**.
- Select the associated **Account Group** and **Usage Profile**.
- Select the **Timezone** relevant to the user.

Creating and Managing MPSK

To create and manage Multiple Pre-Shared Key (MPSK), navigate to **Accounts > Manage MPSK**. Select an account and click **Actions** to perform any of the following supported operations.



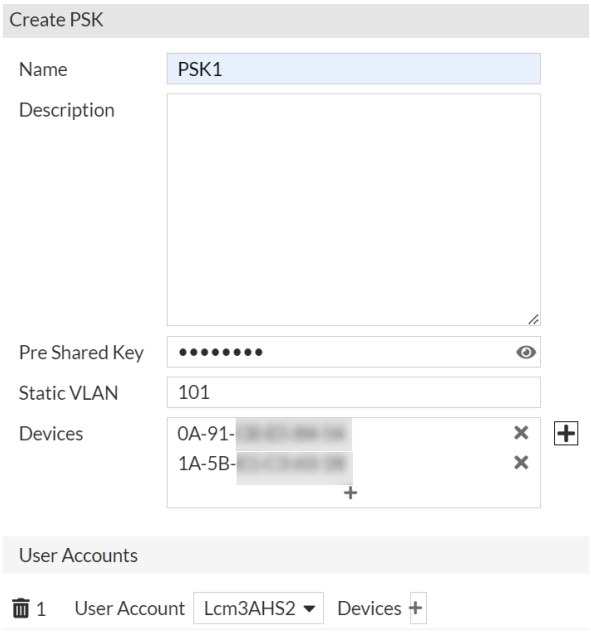
- **Edit** - Edit the selected MPSK profile.
- **Delete** - Delete the selected MPSK profile.
- **Disconnect**- Disconnect clients connected to selected MPSK profile.
- **Suspend** - Suspend the selected MPSK profile to deactivate it temporarily. The profile is removed from the list and the user cannot access it anymore.
- **Revive** -You can revive a suspended or disconnected MPSK profile.
- **View Accounting Logs**-View accounting logs for the selected MPSK profile
- **View Authentication Report** - Displays the successful or failed RADIUS authentications for the selected MPSK profile
- **View Active Sessions**-View connected session individually for the selected profile.
- **Approve/Reject** - A sponsor/administrator can approve/reject the MPSK profile before it is activated.

MPSK accounting features such as suspend, disconnect, and delete require FortiOS version 7.6.3 GA.

Creating PSKs

The administrator can create, update, and delete PSKs in this page. You can create a single or multiple PSKs, each PSK is assigned a single VLAN and one/multiple user accounts and devices. Navigate to **Accounts >**

Manage MPSK and select **Config**. On successful guest portal authentication, the guests can view and use the administrator created PSK or can create their own as described in Guest Portal Device Registration.



- **Name** – Enter a unique name for the PSK
- **Description** – Enter a description/purpose for the PSK.
- **Pre Shared Key** – Create a PSK.
- **Static VLAN** - A static VLAN can be configured per PSK. The VLAN value can be from 1-4095.
- **Device** – Select the client device to associate the PSK with. Optionally, you can create a new device account here. If you select a device that is already linked to a PSK then this new PSK is applied to that device. Only unlimited device accounts of guest are displayed here.
- **User Accounts** – Assign one/multiple user accounts and associated devices to the PSK.
  You can tag device accounts to user accounts when creating a PSK.

A device can use an administrator created PSK, even if it not registered or registered but not tagged with that PSK. When such a device uses the PSK, it is automatically registered in the **Accounts > Manage MPSK** page and a related device account is created.

To use another PSK for your device, you must remove the device from the existing PSK and associate it with a different PSK on the **Accounts > Manage MPSK** page.

Notes:

- The administrator receives an email alert when a new MPSK profile is created using a device account and the guest receives an email alert when the PSK is changed on the guest portal.
- If the admin deletes a PSK tagged to a device, then the PSK-device account association is removed.
- You can configure the maximum number of devices that are allowed to get tagged to a PSK (valid range is 1 - 50) and the maximum number of PSKs allowed per guest (valid range is 1 - 10), in **Accounts > Manage MPSK >Settings**. See MPSK Settings.

VLAN Mapping

FortiGuest provides secure network access by supporting both static and dynamic VLAN mapping when authenticating a guest. You can view the free and occupied VLANs at **Accounts > Manage MPSK > VLAN Mapping**. Select the RADIUS client and all VLANs currently mapped to the PSK associated with the particular RADIUS client are displayed. If both static and dynamic VLANs are configured, then the dynamic VLANs are assigned first, if the dynamic VLAN is not available, then FortiGuest assigns the configured static VLAN.

FortiGuest handles VLAN mapping differently for guest accounts that are tagged to the PSK vs guest accounts not tagged to the PSK. Consider the following, if a guest account is *NOT* tagged to a PSK.

- If a static VLAN is configured then it is used and if a static VLAN is not configured then VLAN 0 is used.
- Dynamic VLAN is *NOT* used in this scenario.

For PSKs with guest accounts tagged to them, the behaviour described in Dynamic VLAN Mapping is applied.

Dynamic VLAN Mapping

Dynamic VLAN mapping is used when a PSK is authenticating via a RADIUS client. Each PSK/per RADIUS client is assigned one VLAN even if that PSK is used by multiple devices, as long as it authenticates via the same RADIUS client. Consider the following example where the VLAN is assigned per RADIUS client.

VLAN pools *pool1* and *pool2* are configured on the RADIUS client.

- If a device *Mobile1* with a PSK, *PSK-auth*, logs in through a RADIUS client, *Client1*, then VLAN ID *xx* is assigned to it.
- If another device, *Mobile2* with the same PSK, *PSK-auth*, logs in through the same RADIUS client, *Client1*, then it is also assigned VLAN ID *xx*.
- But if a device if *Mobile3* with the same PSK *PSK-auth* logs in through a different same RADIUS client, *Client2*, then a different VLAN ID *yy* is assigned. Likewise, if *Mobile3* with a different PSK *PSK-auth12* through the same RADIUS client, *Client1*, then also a different VLAN ID *yy* is assigned.

The following behaviour applies while managing dynamic VLANs.

- The admin is allowed to configure *n* number of VLANs/VLAN ranges separated by commas.
- If the admin adds/deletes the VLAN Mapping on a RADIUS client, then all existing mappings including those currently assigned to PSKs are deleted and re-configured again with the new VLANs.
- If a RADIUS client is deleted then all VLAN mappings associated with it are also deleted.
- If the VLAN pool is exhausted for a RADIUS client, then the static VLAN is assigned. If no static VLAN is configured, then VLAN 0 is assigned.

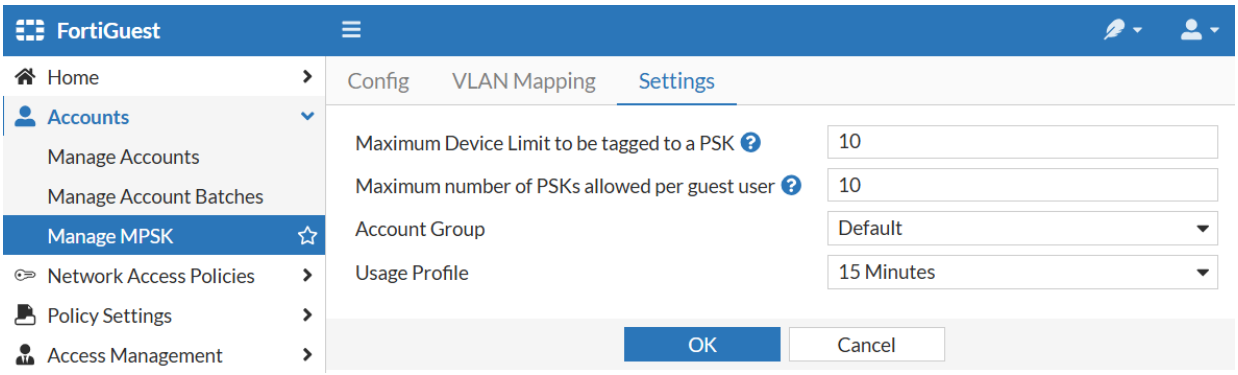
To enable dynamic VLAN mapping, see PSK Authentication.

Static VLAN Mapping

A static VLAN can be configured per PSK. The VLAN value can be from 1-4095. To configure static VLAN, see Creating PSKs.

MPSK Settings

You can configure account group, usage profile and PSK limits in Settings page.



- **Maximum Device Limit to be tagged to a PSK** - Set the maximum number of devices that are allowed to get tagged to a PSK (valid range is 1 - 50).
- **Maximum number of PSKs allowed per guest user** - Set the maximum number of PSKs allowed per guest (valid range is 1 - 10).
- **Account Group** - Select the account group to be used.
- **Usage Profile** - Select the usage profile to be used.

Network Access Policies

Using the FortiGuest network access policies, you can configure pre-defined settings and rules that allow you to define criteria-based authentication and authorization of users, to connect to the network with certain conditions. You can create and assign the following network access policies.

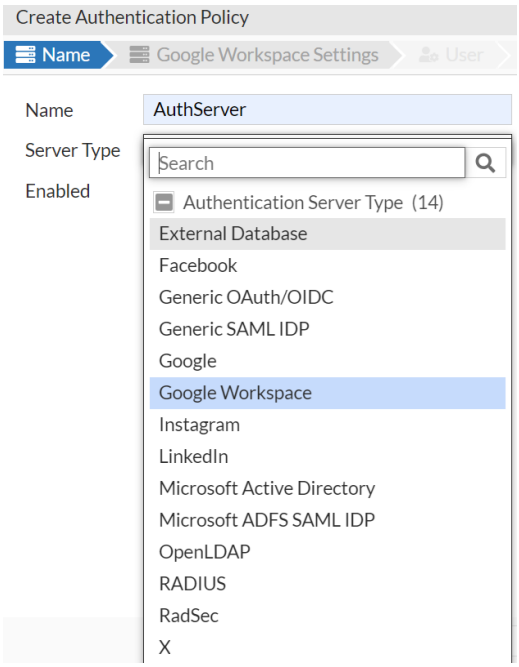
- Authentication Policies
- Authorization Policies
- Authorization Profiles
- Usage Profiles
- Account Groups
- RADIUS Attribute Placeholder

Authentication Policies

FortiGuest allows user authentication via the internal user database or an external authentication server. For an authentication attempt against FortiGuest each server is tried in order against the relevant domain. If an external server rejects the authentication attempt then the user is rejected by FortiGuest. If a server does not respond the next server in the realm is tested.

With an external authentication server, the sponsors need not have another set of user names and passwords to authenticate. The existing server user credentials are used for authentication. It also enables the administrator to quickly roll out user access because there is no need to create and manage additional local sponsor accounts.

Navigate to **Network Access Policies > Authentication Policies** and click **New**. Enter a **Name** for the authentication policy and select the authentication **Server Type**. Based on the selected authentication server, update the subsequent settings/parameters to create an authentication policy. You can **Clone** the authentication policy to reuse configurations.

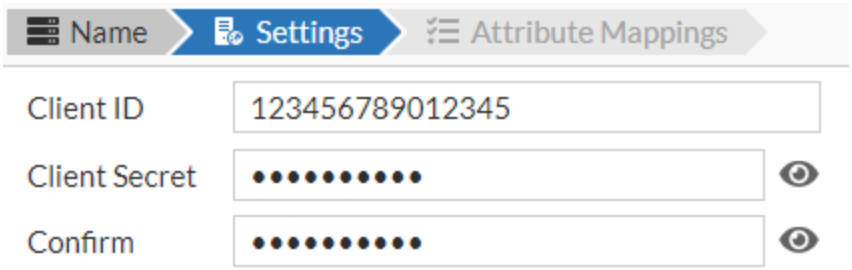


The external servers authenticate sponsors using their existing server credentials. It also enables the administrator to quickly roll out user access because there is no need to create and manage additional local sponsor accounts.

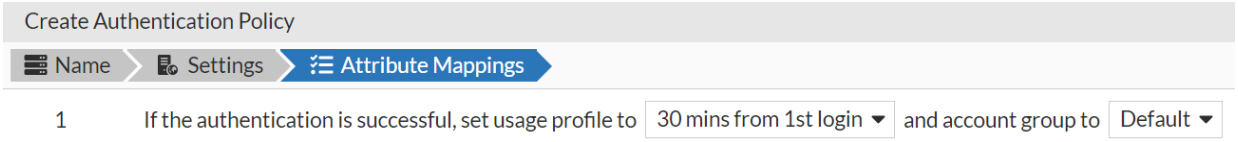
- Facebook/Google/X/Instagram/LinkedIn
- Google Workspace
- Microsoft Active Directory
- External Database
- Open LDAP
- Generic OAuth/OIDC
- RADIUS
- Security Assertion Markup Language (SAML) Support
- RadSec Authentication
- Adding RADIUS and RadSec for Eduroam

Facebook/Google/X/Instagram/LinkedIn

To authenticate sponsors, enter the **Client ID** and **Client Secret** generated on the respective developer's console for these applications.

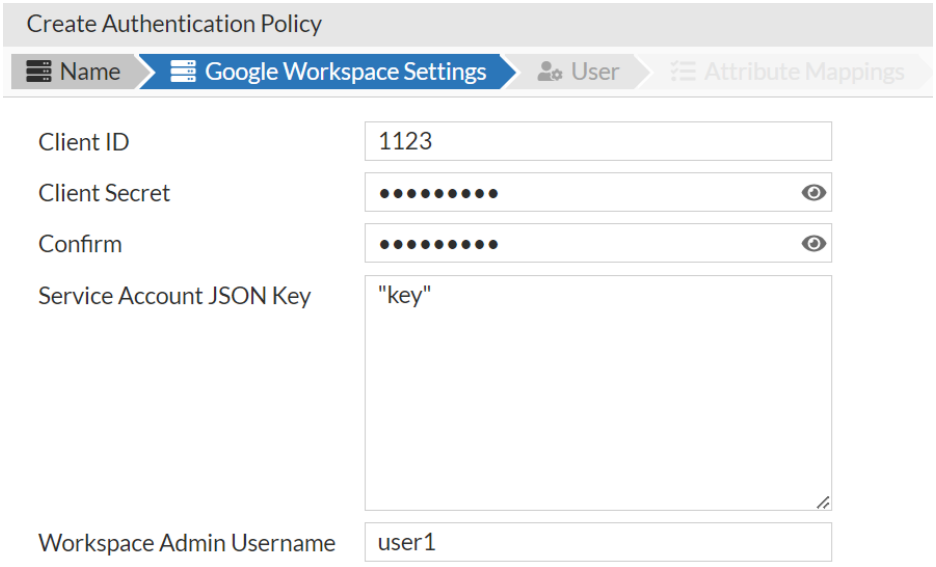


Enter any **Attribute Mappings** required for the server and then map them to the usage profile you require and also set the **Account Group**. Click **Add Mapping** to configure the rules for the policy.

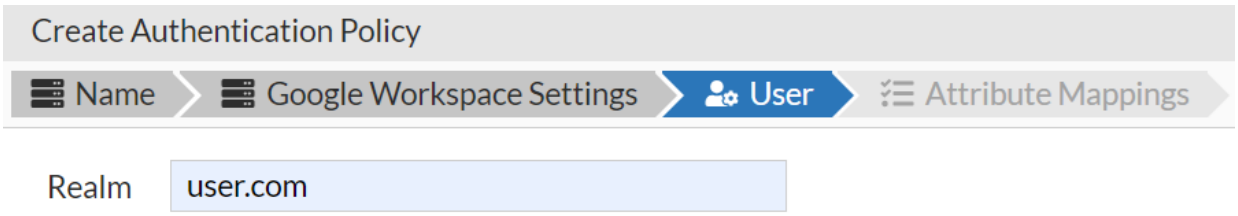


Google Workspace

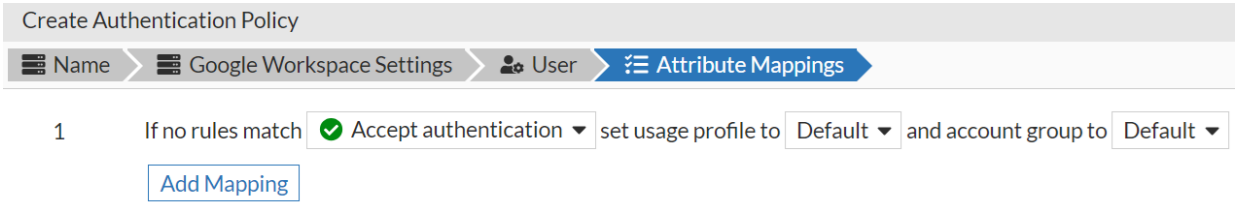
Enter a **Name** for the authentication policy and select the authentication **Server Type**. For authentication, enter the **Client ID** and **Client Secret** generated on the Google Workspace developer's console. Additionally, enter the JON key and the administrator username.



The **User** is the realm/domain to which the user belongs.



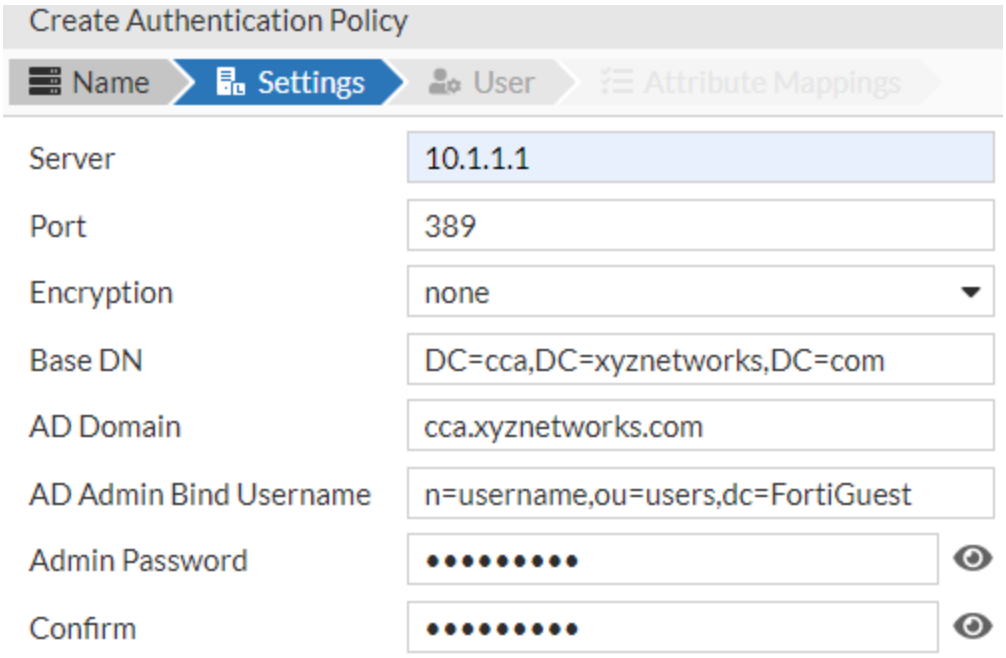
Enter any **Attribute Mappings** required for the server and then map them to the usage profile you require and also set the **Account Group**. Click **Add Mapping** to configure the rules for the policy.



Microsoft Active Directory

Supports authentication against multiple domain controllers that can be a part of the same Active Directory to provide resilience, or they can be in different Active Directories. FortiGuest can authenticate users from separate domains, even where no trust relationship is configured. All Active Directory authentications are performed against individual domain controller entries. FortiGuest attempts to authenticate users against each domain controller entry according to the authentication order specified in the authentication settings.

The user list may appear empty if users are not assigned to any Active Directory groups. This is because the query relies on AD group membership. To resolve this, create a dedicated group in Active Directory and add the relevant users as members. If the group already exists, ensure the group name is added in the format *CN=GroupName* in the AD group within FortiGuest. Additionally, verify that all users have an email address configured.



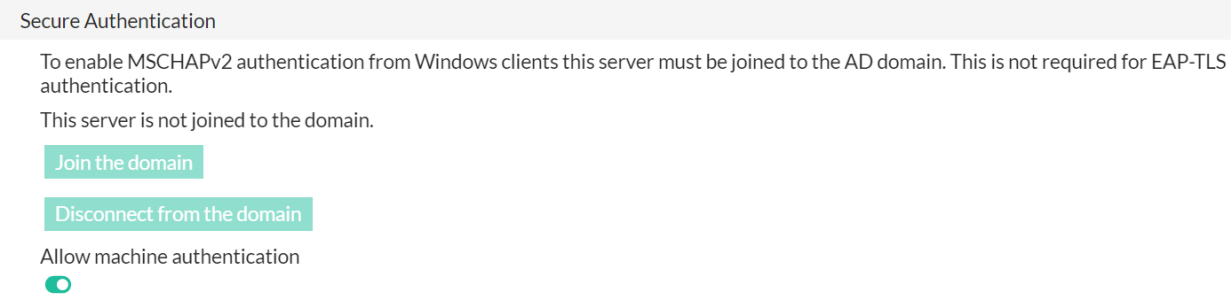
Note: In case the following security settings are configured in the domain controller, then the encryption type should not be *None*.

- Domain controller - LDAP server signing requirements are set to **Require Signing**.
- Network security - LDAP client signing requirements set to **Negotiate signing** or **Require signing**.

Configure the following fields to enable Active Directory authentication.

- **Server** - The Hostname or IP address of the Active Directory server.
- **Port** - The port number of the Active Directory server.
- **Encryption** - The desired encryption method of the Active Directory server.
- **AD Domain** - Enter the domain name of the Active Directory.
- **Base DN** - This is the *Distinguished Name* of the domain controller. It is the name of the root of the directory tree and informs FortiGuest where to start the group searches from. For example, the base DN for the domain *cca.xyznetworks.com* is *DC=cca,DC=xyznetworks,DC=com*.
  Note: The **AD Domain** and **Base DN** are populated when you enter the Active Directory **Server** details.
- **Admin Bind DN** and **Admin Password** - To authenticate a user account the client must bind to the Active Directory server using the bind DN and password of the user account. A Bind DN example is, *cn=username,ou=users,dc=FortiGuest*, where username is that of the user account.

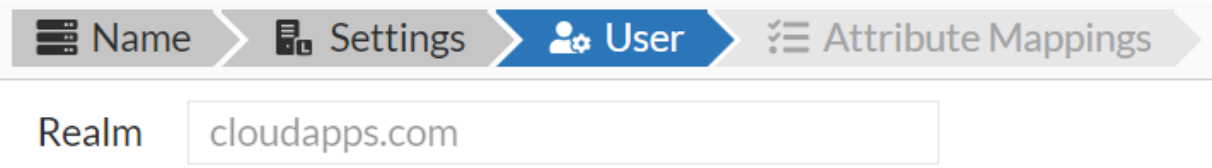
FortiGuest supports MSCHAPv2 authentication to enable a Windows client to connect to a controller that uses FortiGuest as a RADIUS server, that in turns authenticates against an MS Active Directory server. FortiGuest supports authentication from users in domains that are trusted by the domain that it is joined to, for example, if *Domain A* trusts *Domain B*, then users from *Domain B* can also be authenticated to FortiGuest.



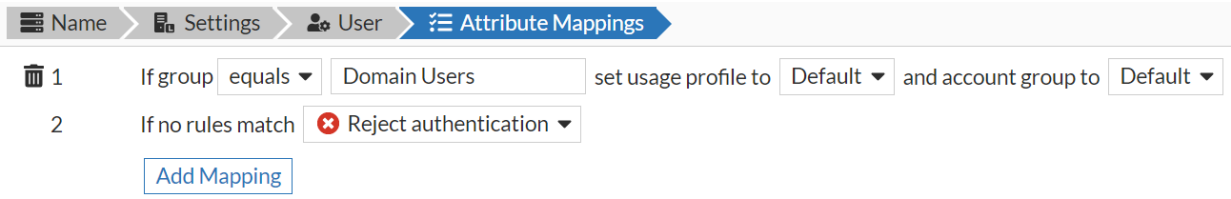
Notes:

- FortiGuest can join only one domain at a time for MSCHAPv2 support.
- You have to re-join the domain after an upgrade/reboot.

The **User** is the realm/domain to which the user belongs.

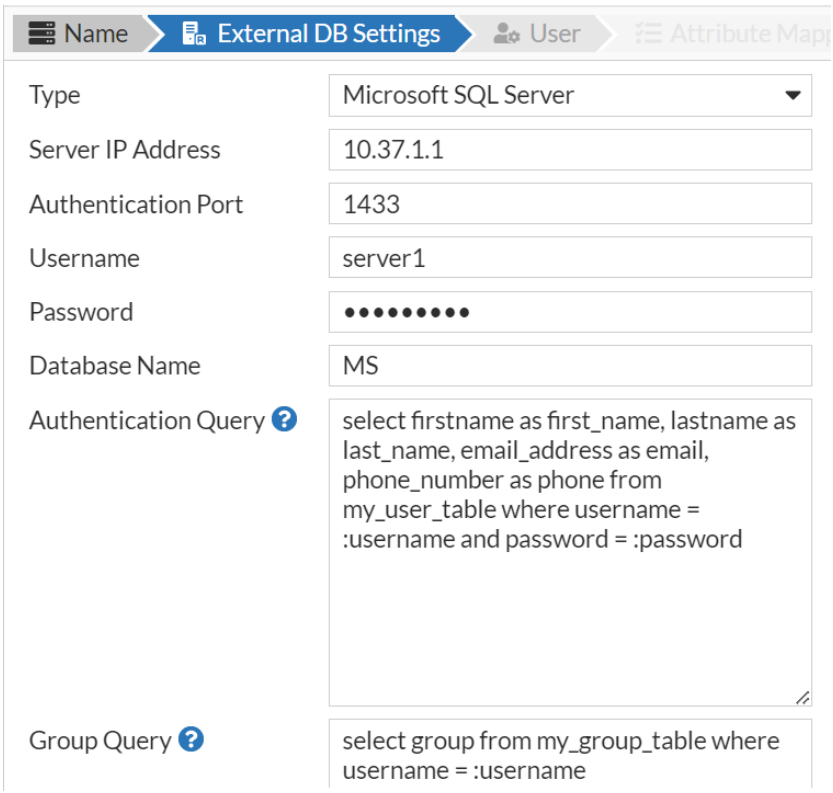


Enter any **Attribute Mappings** required for the server and then map them to the usage profile you require and also set the **Account Group**. Click **Add Mapping** to configure the rules for the policy.



External Database

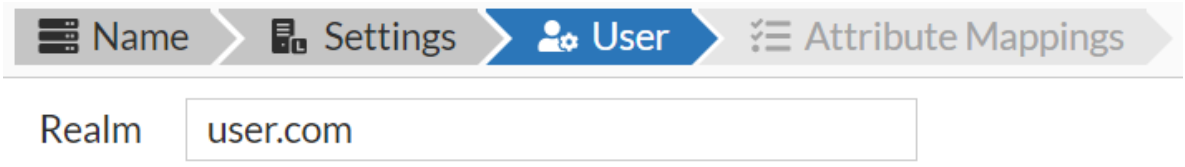
FortiGuest allows an external database to be configured for external authentication.



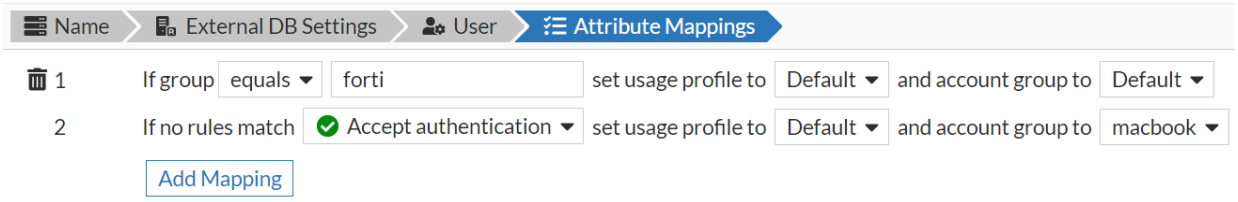
- **Type** - Select the type of external database, the supported databases are, MySQL, MS-SQL, and PostgreSQL.
- **Server IP Address** - Enter the IP address for the server.
- **Authentication Port** - Enter the required port number, leave blank to use the selected types default port
- **Username** and **Password** - Enter the required username and password.
  Note: The username should have only select permissions (Drop, Delete or Truncate should not be allowed for this user).
- Define the **Authentication Query** and **Group Query** required to get user groups from the database.
  Consider the following authentication query example.
  select firstname as first_name, lastname as last_name, email_address as email, phone_number as phone from my_user_table where username = :username and password = :password
  - A user is authenticated if the authentication query returns a row.
  - If any of the following columns are set in that row, then they are applied to the generated account: *first_name, last_name, email, phone*.
  - The *:username* and *:password* parameters are required in the authentication query.

  Consider the following group query (optional) example.
  select group from my_group_table where username =: username
  - This query returns rows with a single column containing the group name.
  - The groups are passed to the group mappings, to determine the user's usage and authorization profiles.
  - The *:username* parameter is required in the group query.

Configure the **User**, that is, the realm/domain to which the user belongs.

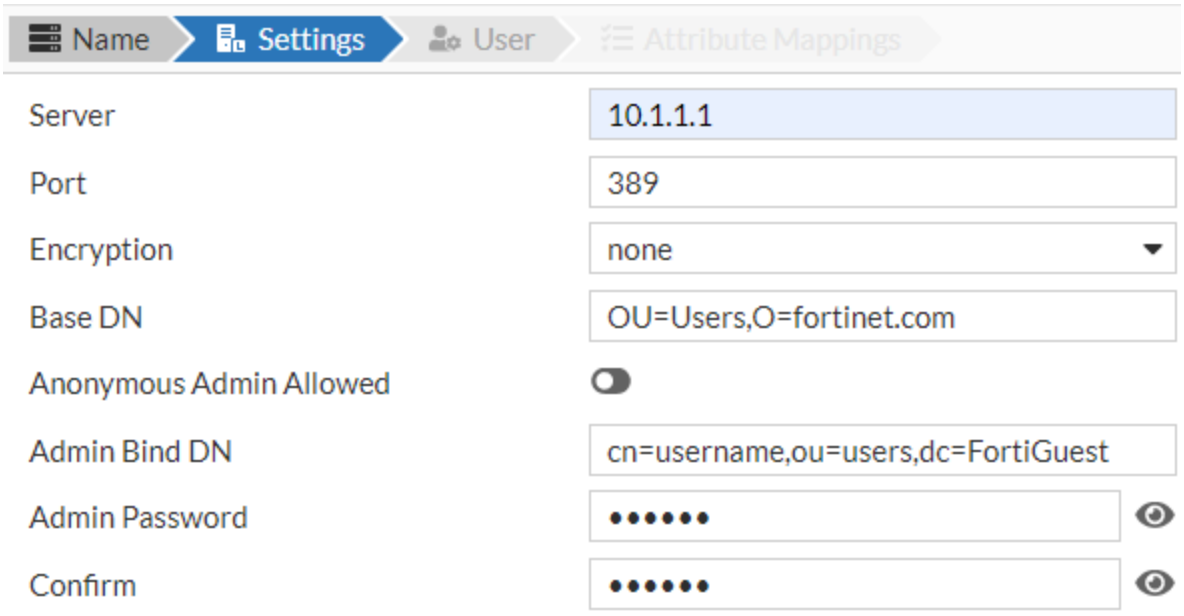


Enter any **Attribute Mappings** required for the server and then map them to the usage profile you require and also set the account group. Click **Add Mapping** to configure the rules for the policy.



Open LDAP

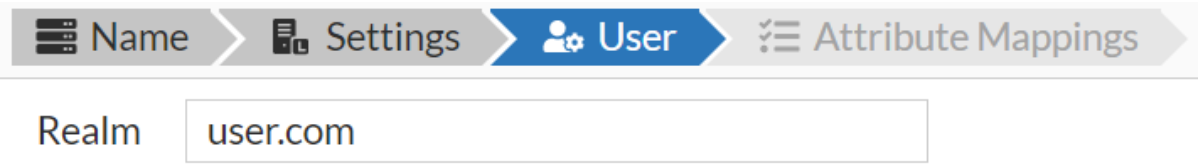
LDAP authentication supports authentication against multiple open LDAP Servers. LDAP authentication allows FortiGuest to authenticate users using their existing LDAP user accounts.



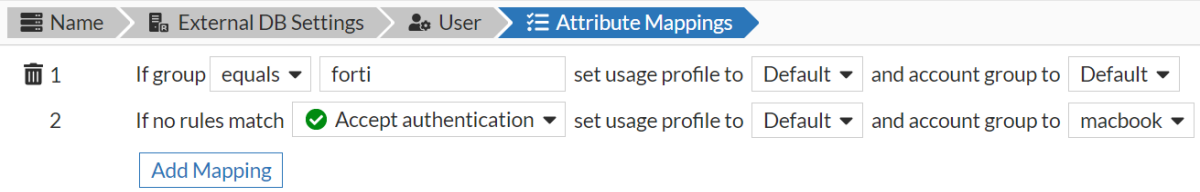
- **Server** - The IP address of the LDAP server.
- **Port** - The port number of the LDAP server.
- **Encryption** - Select the encryption method for the LDAP server, the supported methods are TLS and LDAPS.
- **Base DN** - This is the *Distinguished Name* of the container object from which an LDAP search to find the user is started, enter the desired Base DN, for example, *OU=Users,O=fortinet.com* or *OU=Engineering,O=fortinet*.
- **Anonymous Admin Allowed** - Allow anonymous administrators to authenticate using the LDAP server.

- **Admin Bind DN** and **Admin Password** - To authenticate a user account the client must bind to the LDAP server using the bind DN and password of the user account, for example, *cn=username,ou=users,dc=FortiGuest*, where username is that of the user account.

Configure the **User**, that is, the realm/domain to which the user belongs.



Enter any **Attribute Mappings** required for the server and then map them to the usage profile you require and also set the account group. Click **Add Mapping** to configure the rules for the policy.



Generic OAuth/OIDC

FortiGuest leverages the OAuth 2.0 and OpenID Connect (OIDC) protocols for secure communication. OAuth is an open standard for authorization. It provides third-party applications with limited access to secure resources without compromising the user's data or credentials. OIDC is an authentication protocol that verifies a user's identity when a user tries to access some resources. OIDC was developed to work together with OAuth by providing an authentication layer to support the authorization layer provided by OAuth.

FortiGuest obtains the OAuth access token and OIDC ID token from the specified OIDC authorization endpoint. The access token generated by OAuth is used to authorize access to resources, such as applications and servers, on a limited basis. The OIDC ID token enables authentication to OAuth, which is issued as a JSON Web Token (JWT). ID tokens are the defining component of the OIDC protocol.

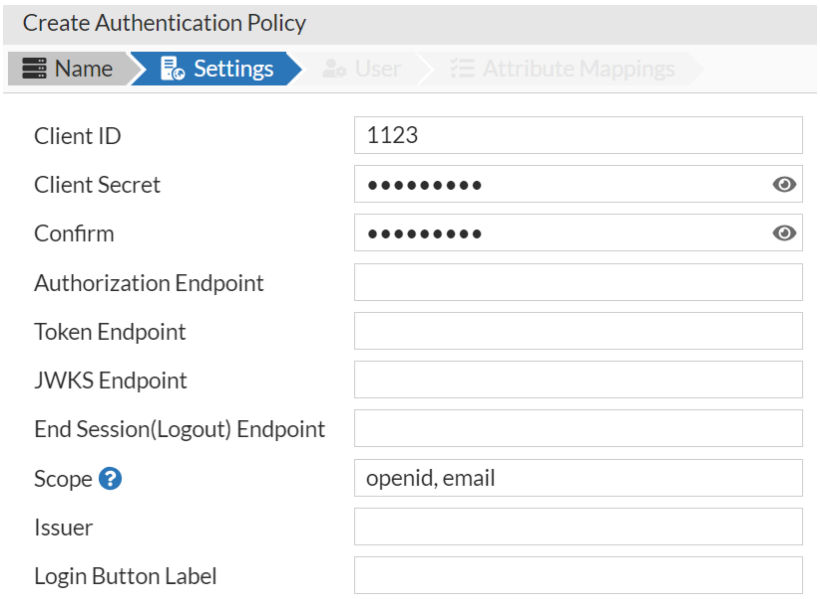
When the OAuth/OIDC server is configured for authentication, an icon is displayed on the captive portal home page. On successful login into the captive portal, the guest clicks on this icon and is directed to the IdP to authenticate with this server.

The following are the supported callback URLs for authentication.

- Admin portal - *https://{FortiGuest FQDN}/api/v1/oauth/oidc_callback*
- Guest portal - *https://{FortiGuest FQDN}/cp/portal/v1/cp/oidc/callback*

The following are the supported callback URLs for logout.

- Admin portal - *https://{FortiGuest FQDN}/api/v1/oauth/oidc/logout_callback*
- Guest portal - *https://{FortiGuest FQDN}/cp/portal/v1/cp/oidc/logout_callback*



The FortiGuest user interface allows administrators to add custom OAUTH2/OpenID Connect IdPs, select **Generic OAuth/OIDC** as the **Server Type** and update the following settings.

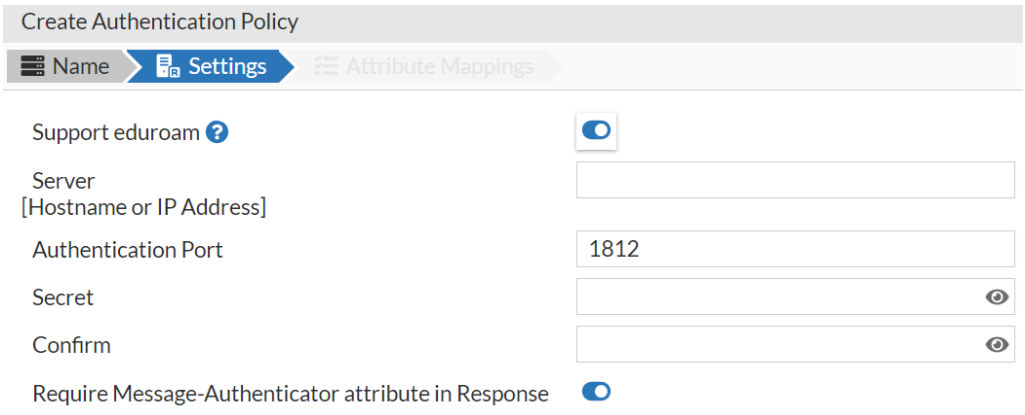
- **Client ID** and **Client Secret** - The client ID and secret required for authentication.
- **Authorization Endpoint** - The public URL of the OIDC authorization endpoint.
- **Token Endpoint** - The public URL of the OIDC token endpoint.
- **JWKS Endpoint** - The public URL of the OIDC JWKS endpoint.
- **End Session Endpoint** - The public URL of the session logout.
- **Scope** - The scope admin wants to request from the user during login. Multiple scopes are allowed as comma-separated strings, for example, *openid, email, profile*.
  Note: Ensure to include **openid** in the scope.
- **Issuer** - This is the public URL of the IdP.
- **Login Button Label** - The label (text) to appear on the login button.

Optionally, you can specify some additional attributes that FortiGuest uses to verify authentication attempts. Configure your IdP to include them as OIDC attributes.

Note: Ensure to include **oidc** as realm in the guest portal's **Realm Policy**.

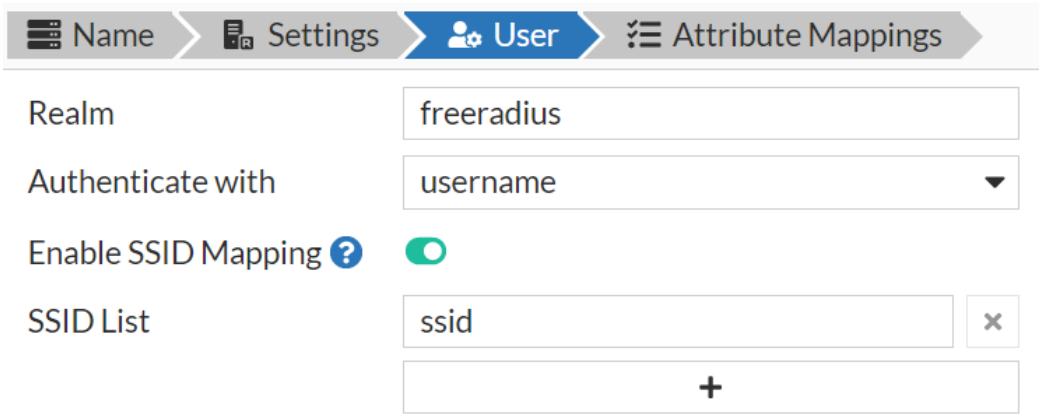
RADIUS

RADIUS authentication allows FortiGuest to authenticate users using their existing RADIUS user accounts.

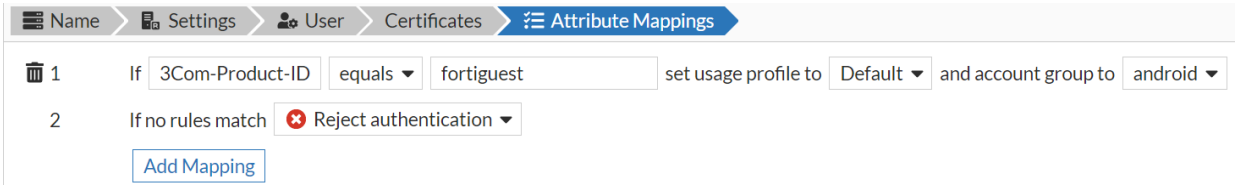


- **Support eduroam** - Enable/disable Eduroam support with the RADIUS server. See Adding RADIUS and RadSec for Eduroam.
- **Server IP Address** - The IP address of the RADIUS server.
- **Authentication Port** - The authentication port number of the RADIUS server.
- **Secret** - The shared secret for the RADIUS client. This must match the shared secret specified in the configuration of the RADIUS client.
- **Message-Authenticator attribute** - You can enable/disable sending the message authenticator attribute to the server when configuring the RADIUS client.

Configure the **User**, that is, the realm/domain to which the user belongs. This option is not available if eduroam support is enabled. You can enable SSID mapping and add the SSIDs that will use the configured authentication policy, if there is no realm in the RADIUS request. Ensure that the *Called-Station-ID* attribute contains the SSID as part of the authentication request.



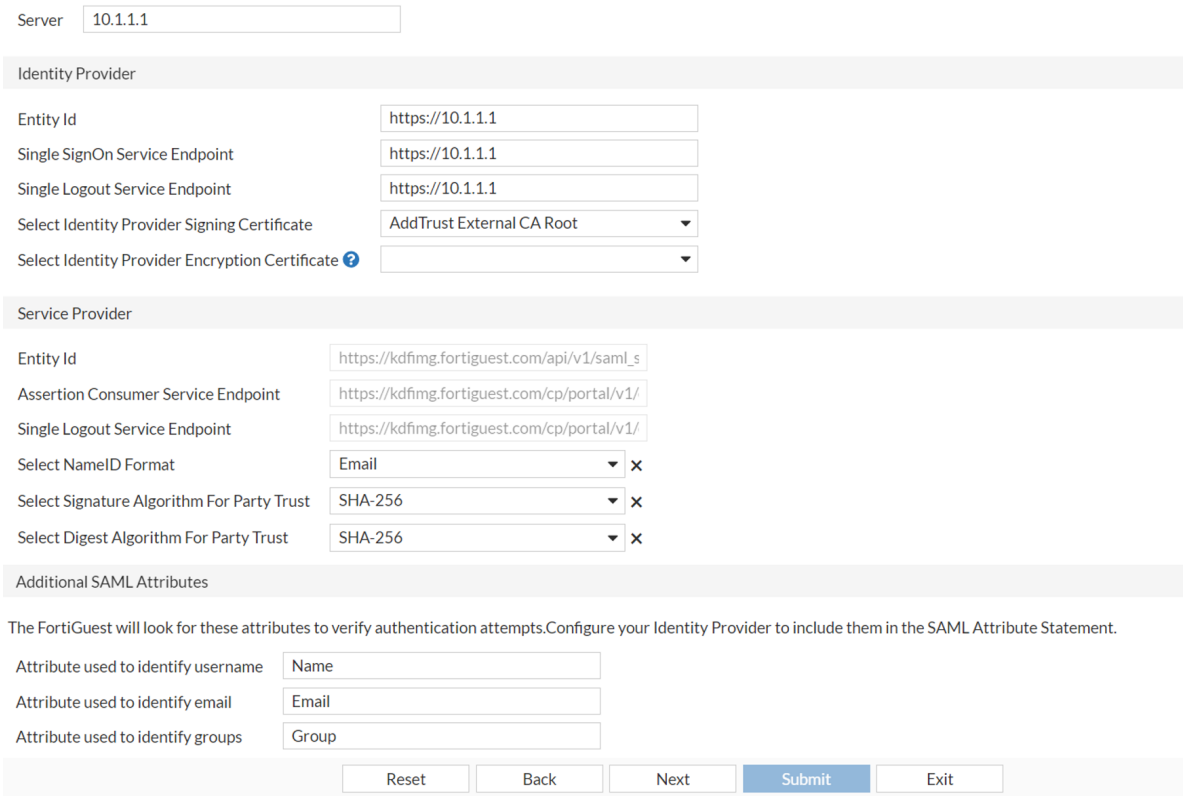
Enter any **Attribute Mappings** required for the server and then map them to the usage profile you require and also set the account group. Click **Add Mapping** to configure the rules for the policy.



Security Assertion Markup Language (SAML) Support

You can configure an authentication server that supports the SAML protocol to access FortiGuest. A SAML supporting authentication server is the *Identity Provider* and FortiGuest is the *Service Provider*. When the SAML authentication server is configured, the FortiGuest login page provides an option to login using SAML. Users can authenticate to the captive portal using their SAML credentials from a trusted IDP.

1. Select **Microsoft ADFS SAML** or **Generic SAML IDP** as the **Server Type**.
2. Configure the SAML settings for the **Identity Provider**.



These settings configure the data that FortiGuest requires to connect to the authentication server.

Field	Description
Server	The IDP server hostname or IP address.
Entity ID	The identifier of the IDP server.
Single SignOn Service EndPoint	The target URL where authentication request from FortiGuest is sent.
Single LogOut Service EndPoint	The URL where log out request from FortiGuest is sent.

Field	Description
Select Identity Provider Signing Certificate	SAML response validators issued by the IDP servers. To use the signing certificate for encryption, do not updated the **Select Identity Provider Encryption Certificate** field.
Select Identity Provider Encryption Certificate	

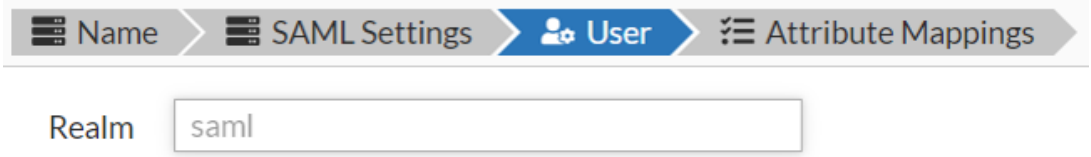
3. Configure the SAML settings for the **Service Provider**. These settings configure the data that the IDP requires to connect to FortiGuest.

Field	Description
Entity ID	The identifier of the FortiGuest.
Assertion Consumer Service Endpoint	The target URL of FortiGuest server to which the IDP will send the SAML response or SAML assertion after authentication.
Single Logout Service Endpoint	The target URL of FortiGuest server to which the IDP will send the SAML log out response.
Select NameID Format	The name identifier of the user.
Select Signature Algorithm For Party Trust	The signature algorithm user in the sign-on process.
Select Digest Algorithm For Party Trust	The digest algorithm used in the digest process.

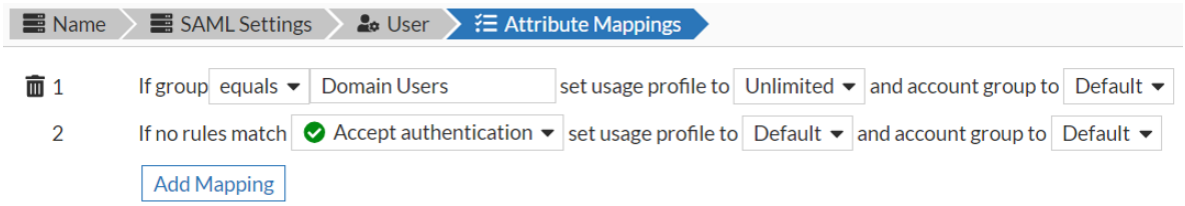
4. Configure additional SAML attributes. FortiGuest looks for these attributes to verify authentication attempts.
   a. Specify the additional attributes that you want to authenticate against.
   b. Configure your Identity Provider to include them in the SAML attribute statement.
   c. Map the attributes from your IDP to the attributes in your SAML profile on FortiGuest.

Field	Description
Attribute used to identify username	The username attribute.
Attribute used to identify email	The email attribute.
Attribute used to identify groups	The groups attribute.

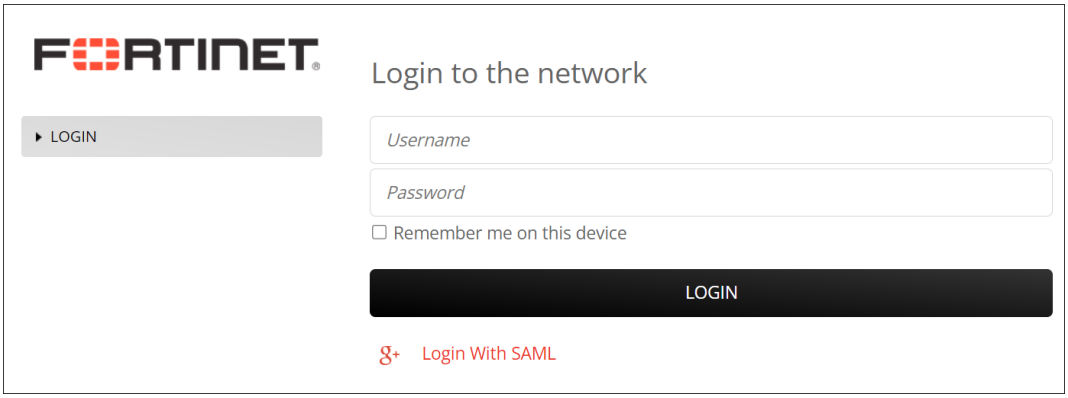
5. Once SAML server is added, select a user realm and click **Next**.



6. Add mapping rules to accept or refuse connection, assign usage profile and account group based on the group attribute values.



To add SAML authentication to the guest portal, configure the SAML server in the Realm policy, see Realm Policy. Preview the portal and ensure that **Login with SAML** option is enabled.



Note: Navigate to the **SAML Settings** to export the meta data file after adding the SAML server.

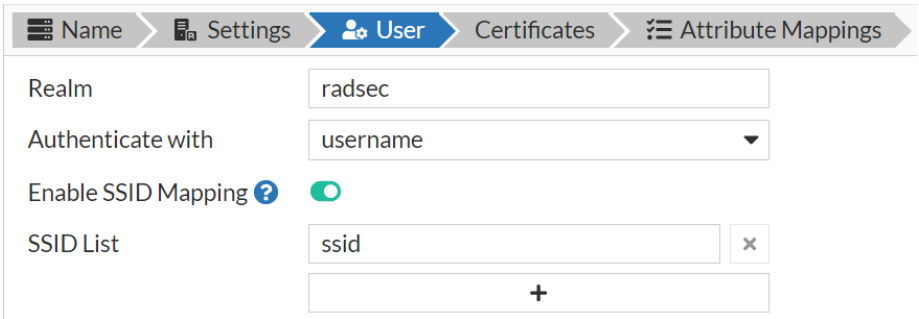
RadSec Authentication

FortiGuest allows user authentication via RadSec, this authentication secures communication between RADIUS/TCP peers on the transport layer. This is particularly useful in roaming environments where RADIUS packets are transferred through different administrative domains and untrusted, potentially hostile networks.

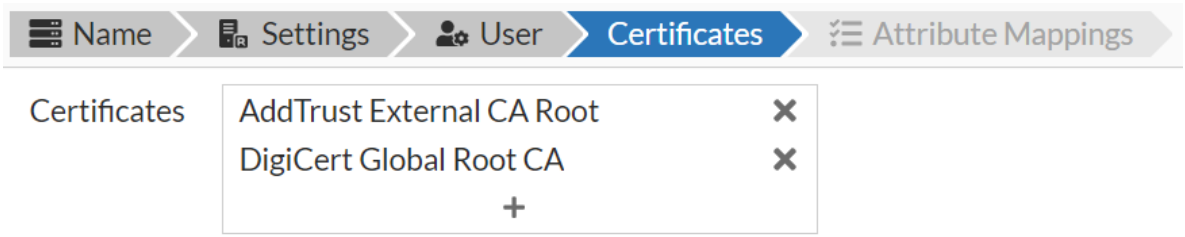
1. Select **RadSec** as the server type and update the following fields in the **Settings** tab.

- **Support eduroam** - Enable/disable Eduroam support with the RadSec server. See Adding RADIUS and RadSec for Eduroam.
- **Verify SSL Certificate CN** - To enable verification, select this option.
- **RadSec Type** - Select TLS or DTLS as the RadSec type.
- **Server IP Address** - Enter the hostname or IP address of the server.
- **Authentication Port** - Enter the authentication port number.
- **Secret** - Enter and then confirm the shared secret.
- **Message-Authenticator attribute** - You can enable/disable sending the message authenticator attribute to the server when configuring the RADIUS client.

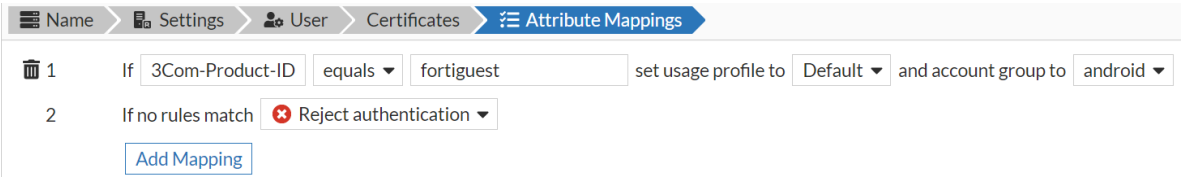
2. Configure the **User**, that is, the realm/domain to which the user belongs. This option is not available if eduroam support is enabled. You can enable SSID mapping and add the SSIDs that will use the configured authentication policy, if there is no realm in the RADIUS request. Ensure that the *Called-Station-ID* attribute contains the SSID as part of the authentication request.



3. FortiGuest allows you to upload trusted CA certificates to validate your server, select a listed certificate or click **Create** to upload a new certificate.



4. Enter any **Attribute Mappings** required for the server and then map them to the usage profile you require and also set the account group. Click **Add Mapping** to configure the rules for the policy.



Note: To enable external RadSec authentication, a server certificate should be for both SSL client and server.

Adding RADIUS and RadSec for Eduroam

Eduroam (education roaming) is the secure, world-wide roaming access service developed for the international research and education community. Eduroam allows students, researchers and staff from participating institutions to obtain internet connectivity across campus and when visiting other participating institutions by simply opening their laptop. RADIUS and RadSec authentication servers can be added to support this feature.

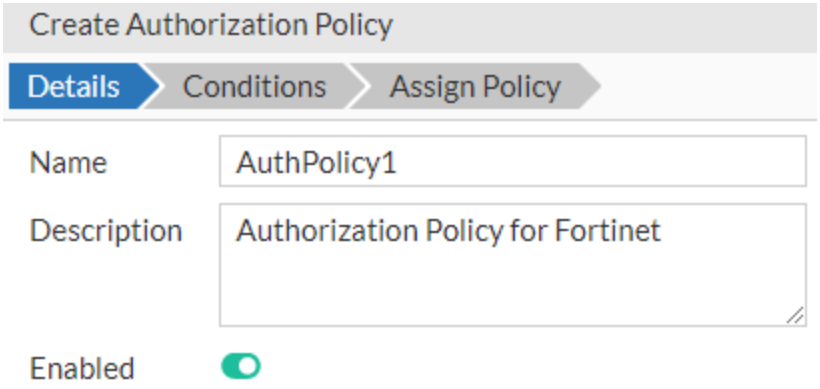
Notes:

- You can configure only one authentication server for Eduroam support.
- Eduroam realm is not displayed under the realm policy for guest portal. It is used only for 802.1x authentication.

Authorization Policies

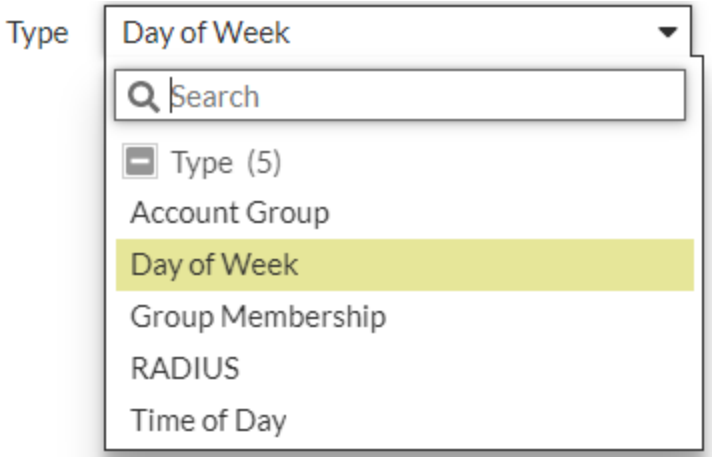
The *Authorization Policy* enables different authorization to users on different devices. For example, allowing users on corporate devices to access internal resources, while giving users on personal devices less access to sensitive data, for example, allowing access only to the internet. For example, administrators can add devices to a list using their MAC address as the identifier and then write a policy so that upon a RADIUS authentication the system can assign a different authorization if the calling-station-id (MAC Address) is in the admin defined list. An authorization policy assigns an authorization profile for any successfully authenticated user based on the conditions configured. You can **Clone** the authorization policy to reuse configurations.

1. Enter a **Name** and **Description** for your authorization policy.



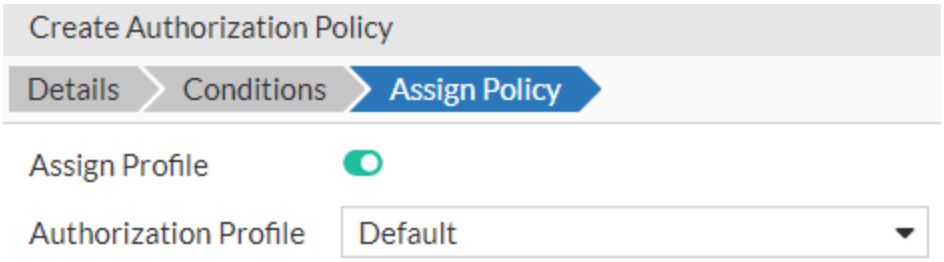
2. Set access conditions based on the available attribute types.

The access rule conditions configured here are matched to assign the appropriate **Authorization Profile**.



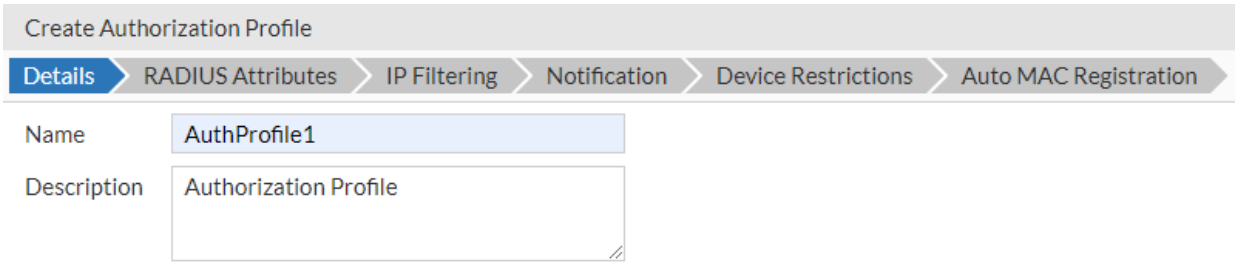
- Day of Week
- Group Membership
- RADIUS
- Time of Day

3. Select an **Authorization Profile** you want to assign to the users/devices that matches configured the authorization rule conditions.



Authorization Profiles

The authorization profiles enable different levels of access to different accounts. For example, to assign different RADIUS attributes or to only allow access to users from certain IP address ranges. You can **Clone** the authorization profile to reuse configurations.



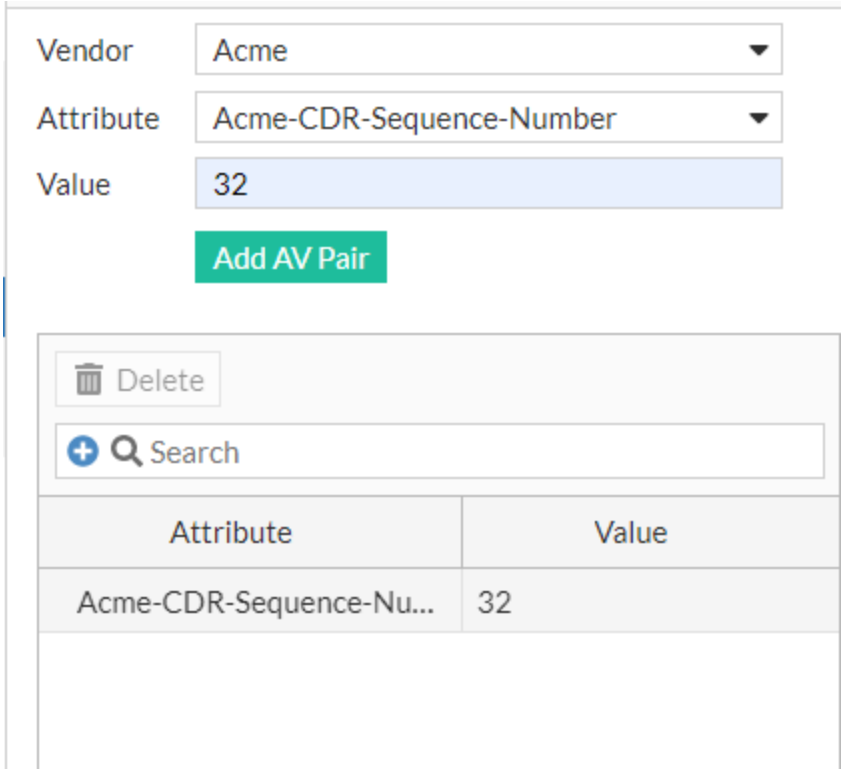
1. Navigate to **Network Access Policies > Authorization Profiles** and enter a **Name** and **Description** for your profile.

2. An authorization profile implements various restrictions and attributes for a user account. Configure the following in your authorization profile.
   - RADIUS Attributes
   - IP Filtering
   - Notification Settings
   - Device Restrictions
   - Auto MAC Registration

RADIUS Attributes

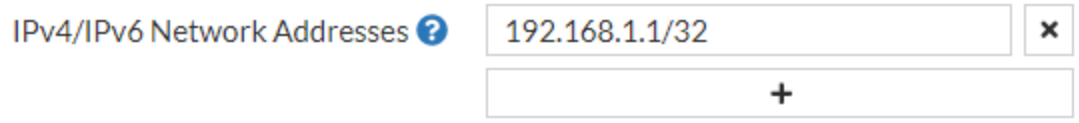
FortiGuest sends these RADIUS attributes to the enforcement device. If a user authenticates using a RADIUS client device such as a FortiGate controller, then for each role you can define additional vendor specific RADIUS attributes that are sent upon successful authentication. Click **New** and select a **Vendor** to add an **Attribute-Value** pair.

Note: **IETF** and **Fortinet** are displayed as the suggested vendors for RADIUS attributes.



IP Filtering

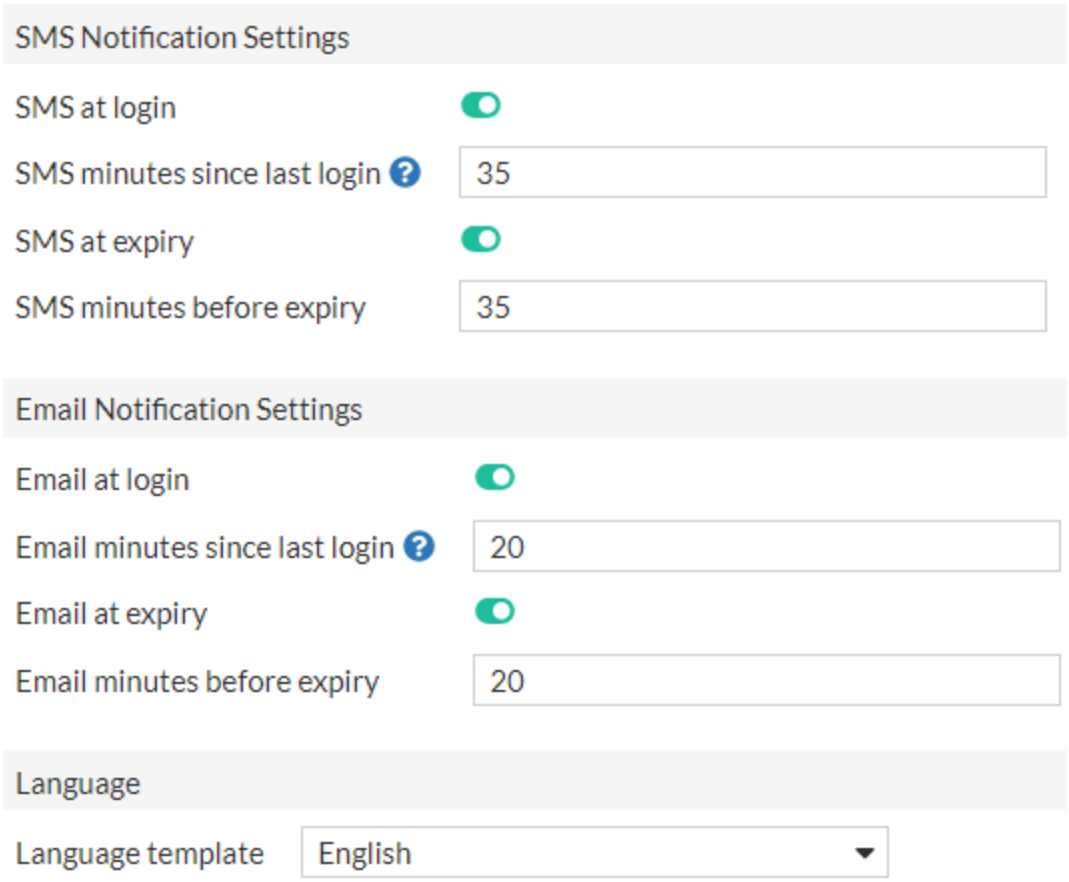
If a user authenticates using a RADIUS client device, then you can specify from which IP address ranges the user is allowed to authenticate for each profile. This enables you to specify profiles based upon location so that users assigned to a specific profile can only log in from locations that you specify. Enter the IPv4/IPv6 network address with the appropriate prefix length, the host addresses must be specified using a /32 prefix for IPv4.



Note: This feature only works when the RADIUS client sends the user IP address in the RADIUS authentication and the IP address is contained in the *Framed-IP-Address* attribute.

Notification Settings

You can configure to send an email and SMS notifications upon user account log in and expiry.



- **SMS Notification Settings** - Enable SMS notifications for user account log in and then specify how often you wish to send notifications. Leave the field empty to send an SMS at every log in.
- **Email Notification Settings** - Enable email notifications for user account log in and then specify how often you wish to send notifications. Leave the field empty to send an email at every log in.
- Specify the **Language template** to use for email and SMS notifications.

Device Restrictions

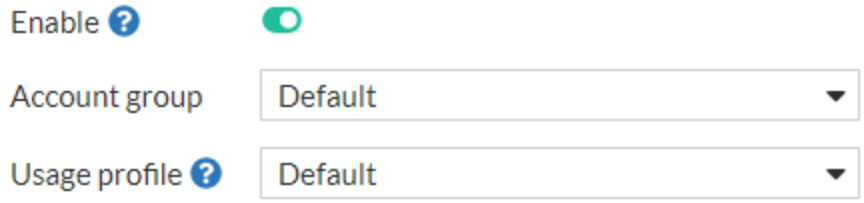
You can configure the user profile to restrict log in to a certain amount of permissible users/devices within a specific time period.

- Enter the **Max devices per user** to configure the maximum number of devices allowed per users. Leave the field empty to allow an unlimited number of devices per user.
- Enter the **Max users per device** to configure the maximum number of users to access a device. Leave the field empty to allow an unlimited number of users per device.
- The **Duration** is the period for which these restrictions apply. For example, if the maximum limit is 2 devices per user then this limit applies only for the time period configured in the **Duration** field.

Note: FortiGuest enforces device restrictions only if *Radius Accounting* is enabled with interim updates on the NAS server, and the *Accounting-interim-update* attribute is added in the RADIUS client.

Auto MAC Registration

You can enable this setting to register MAC addresses, so that when a device is used to login it is remembered on the network. If this is enabled, a device account is automatically created for a user device when they login via a portal. Automatic device registration is subject to the limit set in **Policy Settings > Account Groups**. Select the **Account Group** and **Usage Profile** used to create the device.



Usage Profiles

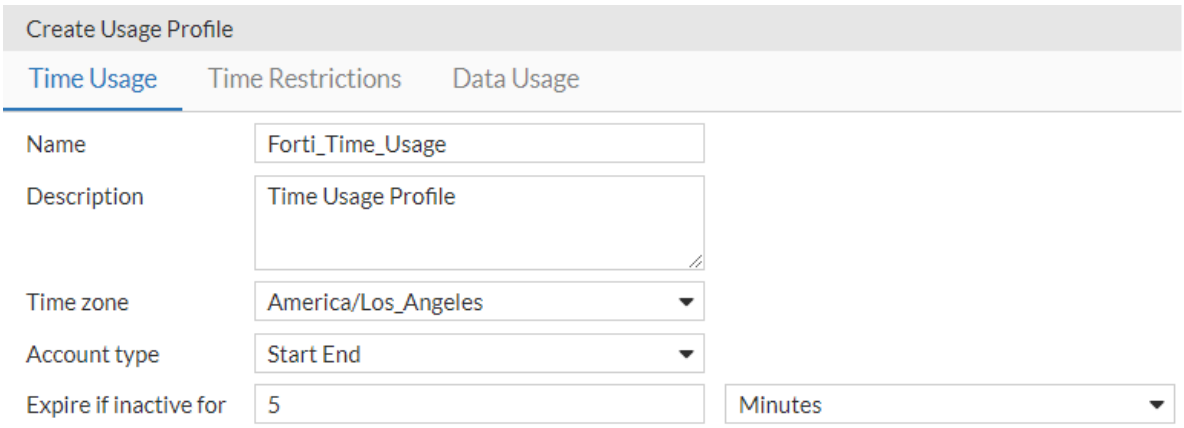
The *Usage Profiles* allow you to provide levels of time access/data usage to different user accounts. For example, you can assign a usage profile that allows access during a working week day and not on a weekend. After usage profiles are created, you must change the sponsor user group to allow sponsors in that group to be able to provision accounts to the appropriate usage profiles created. Navigate to **Network Access Policies > Usage Profiles** and update the following configurations. You can **Clone** the usage profile to reuse configurations.

- Time Usage
- Time Restrictions
- Data Usage

Time Usage

Configure the time usage profile for user accounts access restrictions.

1. Enter the **Name** and **Description** of the new time profile; select the **Timezone** to which any account restrictions apply.

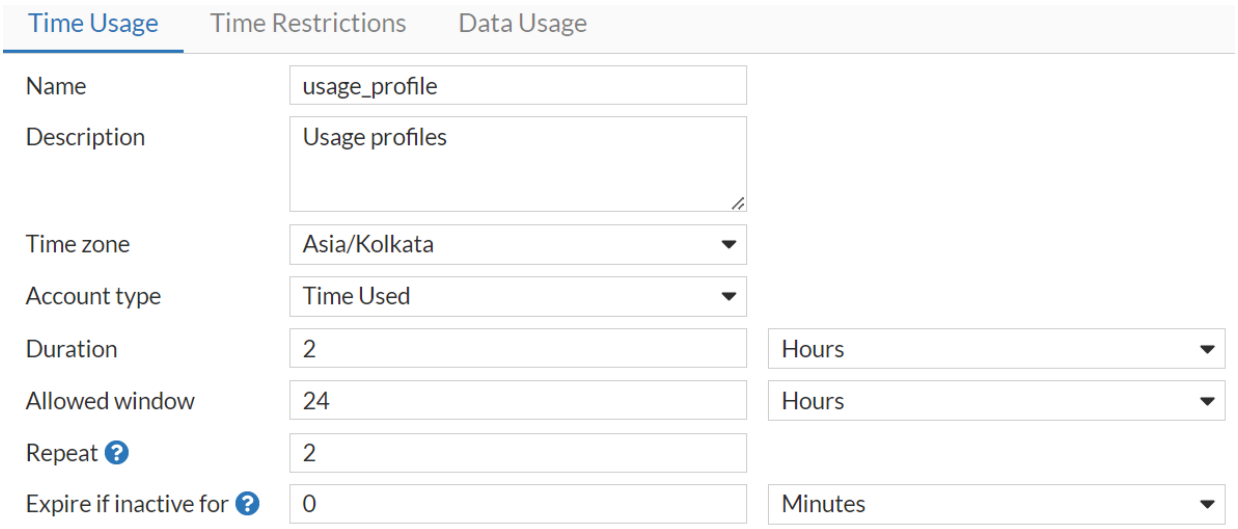


2. Select any of the following available **Account type** options.
   - **Start End** - Allows sponsors to define start and end times for account durations, from when the user first logs in.
     Note: Do not use the **Start End** usage profile for any accounts that are created on the fly, such as, accounts created against a backend authentication like *AD/LDAP/RADIUS/AUTH/SAML* and accounts created via captive portal like *Self Service/CC BILLING/PMS BILLING/CLICK THROUGH/AUTO LOGIN*. Use the **Start End** only for user accounts created by admin/sponsor.
   - **From First Login** - Allows sponsors to define a length of time for user access from their first login.
   - **From Creation** - Allows sponsors to define a length of time for user access from the moment of account creation.
   - **Time Used** - Allows sponsors to create a time period during which the user can log in. For example, account can be valid for 2 hours and usable for any time within 24 hours from first log in. The following fields are additionally required to configure this option. See User Scenario.
     - **Duration** - The time for which a guest user can log in within the specified **Allowed Window**.
     - **Allowed Window** - This parameter should be greater than or equal to **Duration**.
     - **Repeat** - The number of times the configured **Allowed Window** and **Duration** parameters are repeated.
   - **Unlimited** - Unlimited time profiles.
3. The **Expire if inactive for** option allows the admin to specify the time period after which an account with this usage profile should be considered inactive.

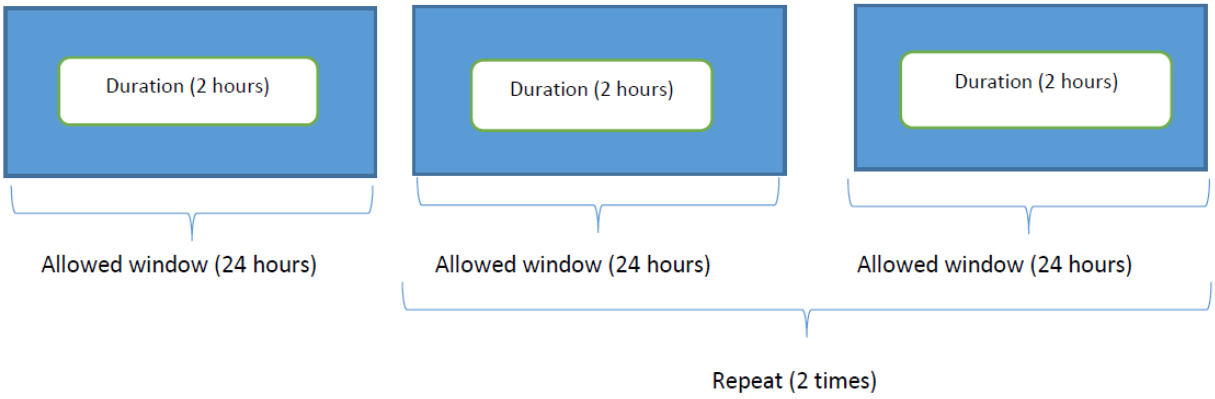
Note: In case of a usage profile with the account type as **Start End**, ensure that the time zone defined here is the same as that in the account creation page that is associated with this profile.

User Scenario

Consider the following use cases for configuring the time usage profile and how it works with FortiGuest. In the following example, **Duration** is set to 2 hours, the **Allowed Window** is 24 hours, and **Repeat** cycle is 2 times.



With this usage profile, the account is valid for 2 hours and usable for any time within 24 hours from the first user login. Since the **Repeat** is set to 2, the account end time is 72 hours from the first login; during which a user can log in for 2 hours, in a window of 24 hours and this cycle can be repeated twice.

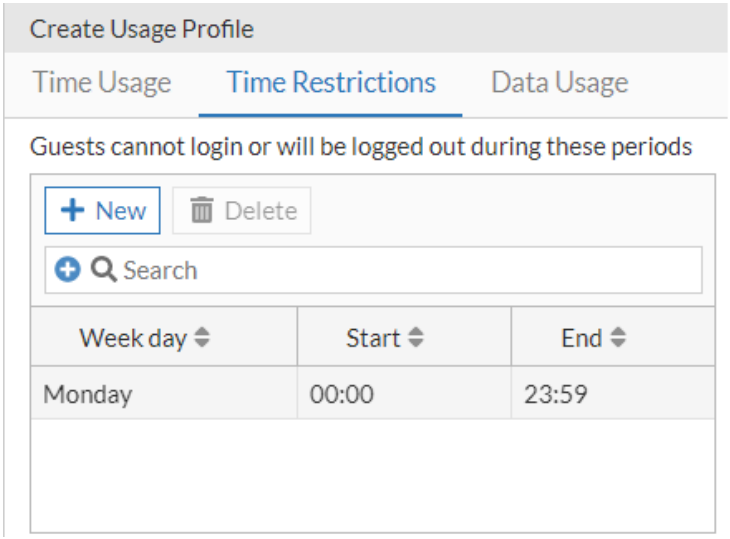


Now, consider the following use cases.

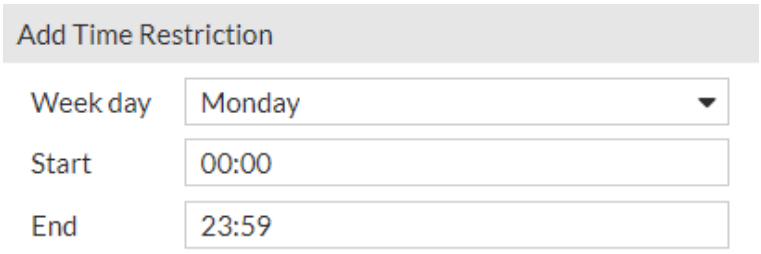
- **Use Case 1** - When a user logs in for the first time, FortiGuest grants a session timeout of 2 hours, based on the configured **Duration** of 2 hours. If the user disconnects after 1 hour and logs in again within the same 24 hour window, then the session timeout is only for the remaining 1 hour.
  Note: User can re-connect any number of times. The timeout is based on the configured duration and allowed window.
- **Use Case 2** - Consider that the user logs for the first time within the allowed window, that is expiring in 30 minutes, then the user is granted access for 2 hours and 30 minutes. This includes 30 minutes of the remaining allowed window and 2 hours from the next allowed window (since **Repeat** is set to 2).
- **Use Case 3** - If the user logs in at the end of the last allowed window. For example, if the user logs in when the last allowed window is expiring in 30 minutes, then FortiGuest grants access for just 30 minutes, the allowed window expires after that.

Time Restrictions

You can implement account restrictions in the *Time Restrictions* section. Guests cannot log in or are logged out during these periods.

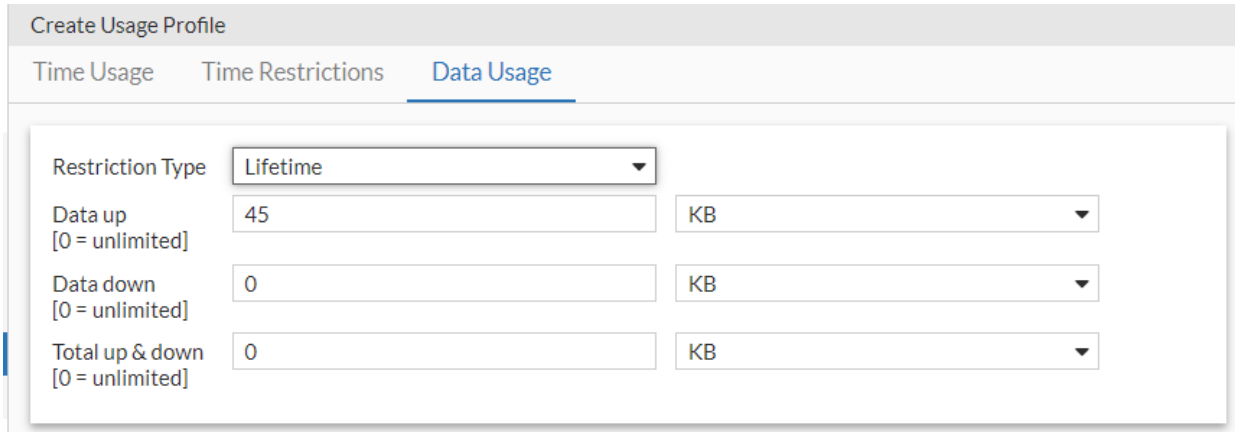


Select the week day and specify the **Start** and **End** time to restrict guest access.



Data Usage

You can also add data usage restriction on the account based on time periods. The data restriction is configured either for a lifetime or is periodic.



- **Lifetime** - This restriction applies to the full lifetime of the account, after which the account expires. A user cannot connect back until the admin revives the account.
- **Periodic** - This restriction applies to a set period of time, after which the account access is restricted until the next time period begins. A user can connect back again only after the current restriction for data is over and the new time period begins.
  - **Daily** - This restriction applies as per the user's time zone, that depends on the usage profile that is applied.
  - **Weekly** - This restriction applies from Monday-Sunday, as per the user's time zone.
  - **Monthly** - This restriction applies from the 1st of a month to its last day, as per the user's time zone.

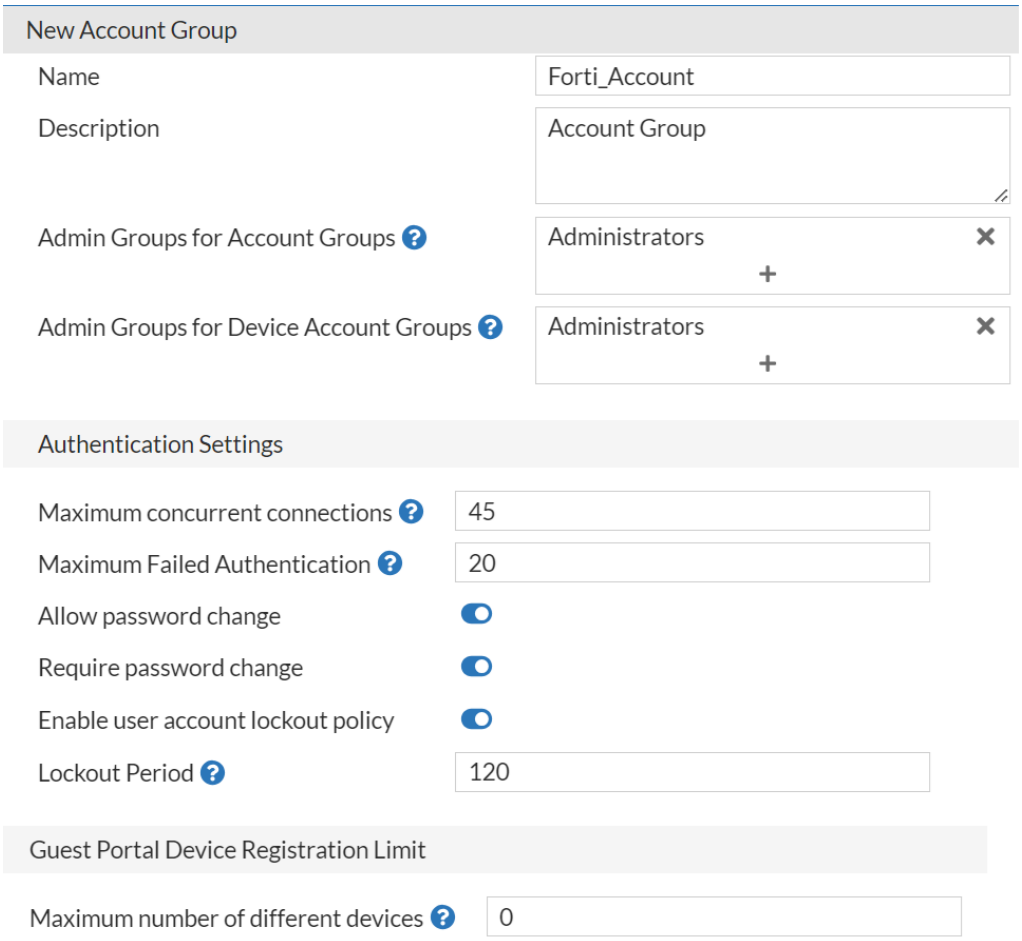
From the available options, determine whether to apply the following.

- **Data Up** - Apply a data usage up restriction to your profile in KB, MB or GB.
- **Data Down** - Apply a data usage down restriction to your profile in KB, MB or GB.
- **Total Up & Down** - Apply a total data usage restriction to your profile in KB, MB or GB.

Note: FortiGuest enforces these restrictions only if *Radius Accounting* is enabled with interim updates on the NAS server, and the *Accounting-interim-update* attribute is added in the RADIUS client.

Account Groups

The *Account Groups* are used to group user and device accounts and are assigned at the point of account creation. If no additional account groups are created, then user and device accounts are assigned to the default account group. An *Authorization Profile* is assigned via the *Authorization Policy* which may reference an account group as part of its mapping criteria. You can **Clone** the account group to reuse configurations.

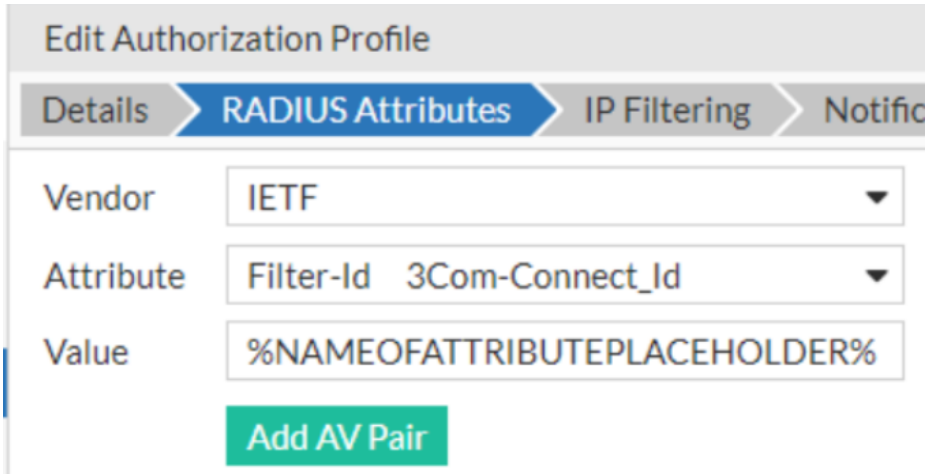


1. Navigate to **Network Access Policies > Account Groups** and click **New**.
2. Enter a **Name** and **Description** for the account group and configure the following options.
3. Configure the following **Authentication Settings** for member accounts.
   - **Maximum concurrent connections** - Specify the maximum number of concurrent connections allowed for each member account. A value of 0 implies an unlimited number of concurrent connections.
     Note: FortiGuest enforces this restriction only if *Radius Accounting* is enabled with interim updates on the NAS server, and the *Accounting-interim-update* attribute is added in the RADIUS client.
   - **Maximum failed authentications** - Specify the maximum number of failed authentication attempts allowed for each member account. A value of 0 implies an unlimited number of failed authentication attempts.
   - **Allow password change** - Select to allow member accounts to modify the configured passwords.
   - **Require password change** - Select to mandate password changes for member accounts.
     Note: Password change is not applicable on external user accounts. The account passwords should be reset on the respective database.
   - **Enable user account lockout policy** - Configure an account lockout period in case an existing user enters an incorrect password. The user can log in again after the lockout period is over.
   - **Lockout Period** - The valid range for the lockout period is 120 - 86400 seconds, the default is 120 seconds.
     When an account is locked, the status of the account appears *Locked out* in the **Manage Accounts** session.

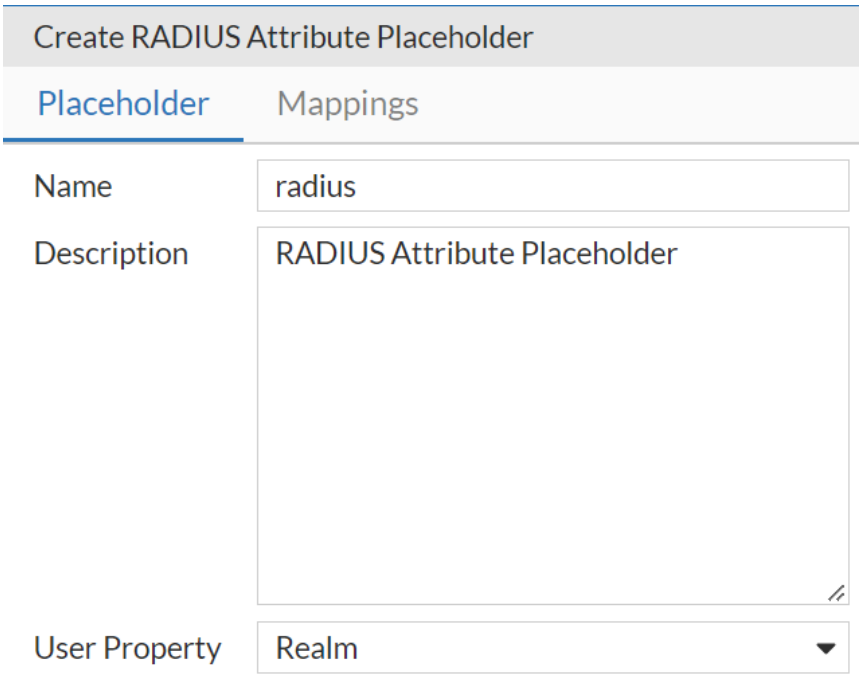
4. Specify the **Maximum number of different devices a user can register**, that is, the maximum number of different devices a user can register for guest portal access. A value of 0 implies an unlimited number of device registrations.

RADIUS Attribute Placeholder

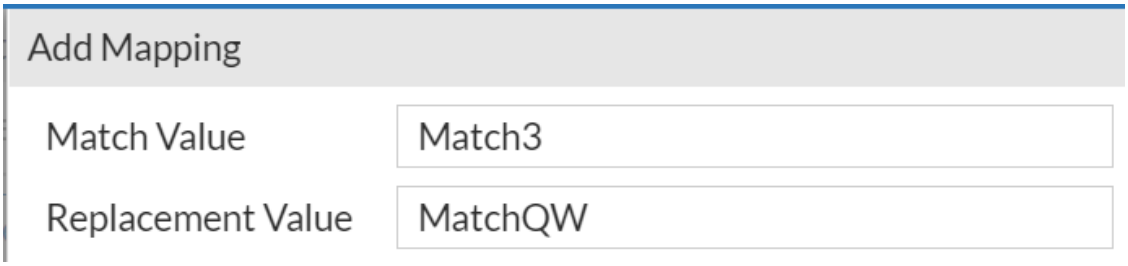
You can dynamically change the RADIUS attributes returned on authentication. The RADIUS attributes are defined in **Devices > RADIUS Clients** (RADIUS Clients) and **Network Access Profiles > Authorization Profiles** (Authorization Profiles). To dynamically replace these attributes with the RADIUS placeholder, define the value in the format, *%NAMEOFTHERADIUSPLACEHOLDER%*. You can **Clone** these placeholders to reuse them.



You can add, edit and delete the RADIUS placeholder attributes.



The RADIUS placeholder is added. In the **Mappings** tab create any number of mappings for the placeholder.



Note: If no mappings are defined for a RADIUS attribute placeholder, then the user property value is returned as the value of the RADIUS attribute.

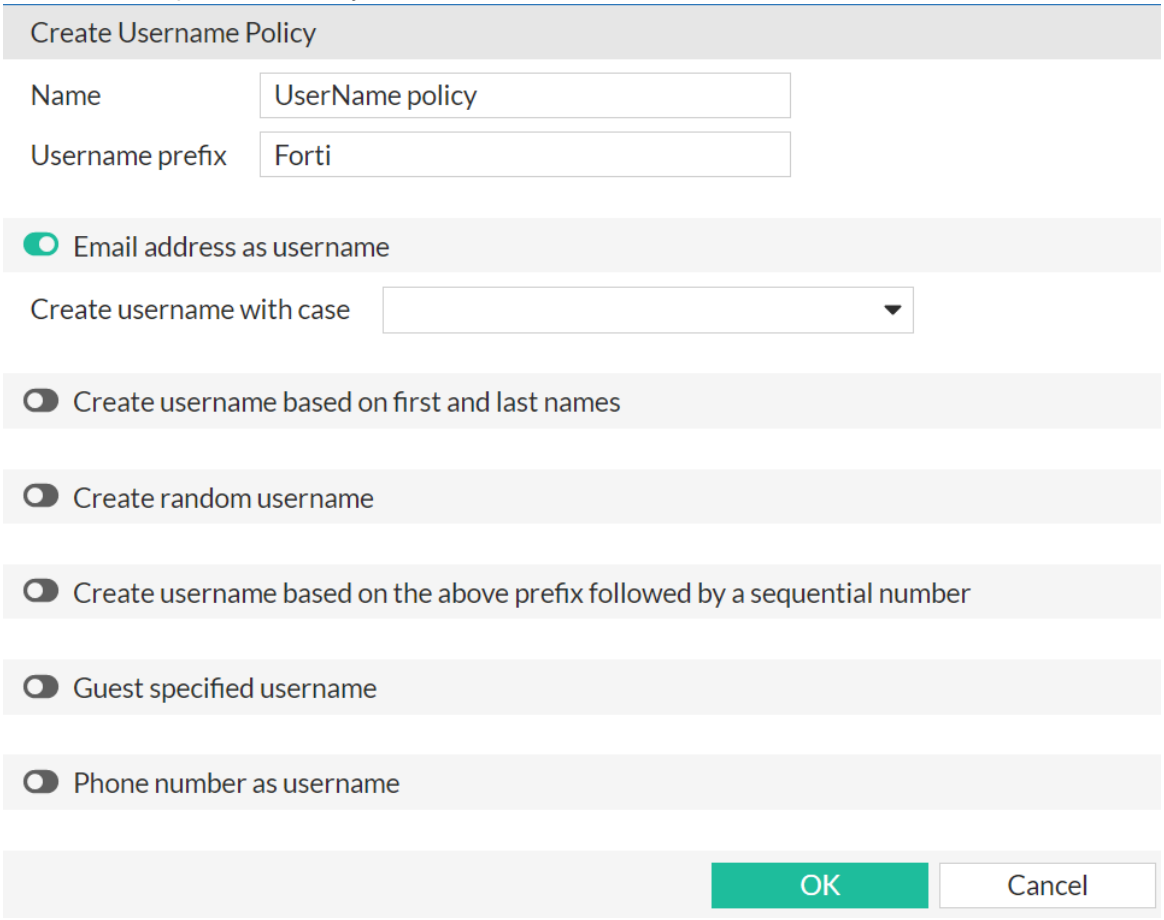
Policy Settings

Organizations commonly have policies in place for creating accounts for their users and systems, such as the format or length of the username and/or complexity of password. FortiGuest allows you to configure username and password creation policies to match your organization's policy. You can configure multiple policies and set any policy as the default; the default policy is for admin/sponsor created user accounts.

Username Policy

The account *Username Policy* determines how to create usernames for all guest accounts. You can **Clone** the username policy to reuse configurations.

1. Navigate to **Policy Settings > Username Policy** and click **Standard Accounts** tab. All generated usernames are prefixed with any text/number entered as the **Username Prefix**.

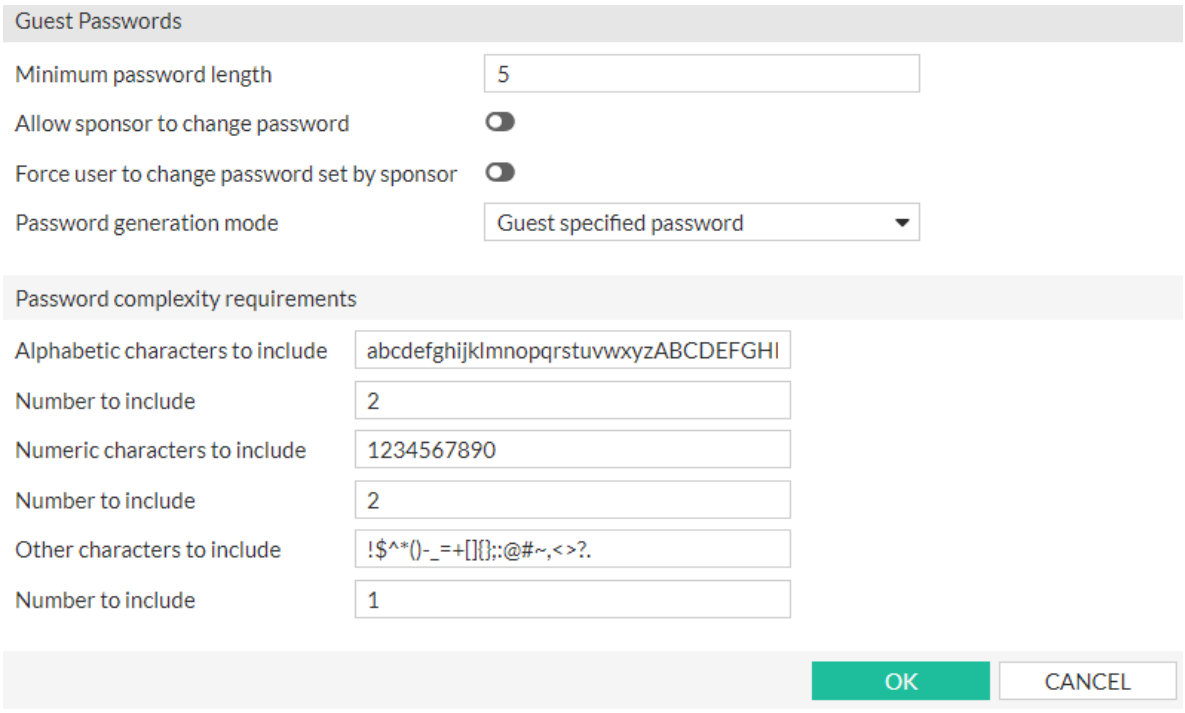


2. Create accounts based on any of the following user name policy criteria.
   - **Email address as username** - You can specify the *email address* as username, if an overlapping account with the same email address exists, a random number is added to the end of the email address to make the username unique. Overlapping accounts are accounts that have the same email address and are valid for the same period of time. With the **Create Username With Case** option, you can determine the case of the username created by the sponsor.
     - **Case entered by sponsor** - The username remains in the same case set by the sponsor.
     - **Uppercase** - The username is forced into uppercase after it is set by the sponsor.
     - **Lowercase** - The username is forced into lowercase after it is set by the sponsor.
   - **Create username based on first and last names** - Create a username based on combining the first and last names of the user. You can set a **Minimum username length** for this username from 1 to 20 characters (default is 8). Usernames shorter than the minimum length are padded up to the minimum specified length with a random number. The **Create Username with separator** option allows you to create usernames using some keyboard separators (_|-|,|:|.). With the **Create Username With Case** option, you can determine the case of the username created by the sponsor.
     - **Case entered by sponsor** - The username remains in the same case set by the sponsor.
     - **Uppercase** - The username is forced into uppercase after it is set by the sponsor.
     - **Lowercase** - The username is forced into lowercase after it is set by the sponsor.
   - **Create random username** - You can create a *random username* with a combination of alphabetic, numeric, and special characters. Insert the characters permissible in the randomly generated username and select the allowed number to use from each set of characters. You can determine the alphabetic, numeric, and other characters to include in the username.
     - **Alphabetic characters to include** - The permissible alphabetic characters that the username can include.
     - **Number to include** - The maximum number of alphabetic characters allowed in a username. The limit is 20 characters.
     - **Numeric characters to include** - The permissible numeric characters (numbers) that the username can include.
     - **Number to include** - The maximum number of numeric characters allowed in a username. The limit is 20 characters.
     - **Other characters to include** - The permissible other (special) characters that the username can include
     - **Number to include** - The maximum number of other characters allowed in a username. The limit is 20 characters.
   - **Create username based on the above prefix followed by a sequential number** - You can create username with the specified username prefix (**Username Prefix**) followed by a randomly generated sequential number.
   - **Guest specified username** - You can allow a guest specified username, that is, guests can create a username at account creation. Select the **Minimum username length** the guest must use; the permissible minimum length is 20.
   - **Phone number as username** - You can allow the guest to use their phone number as the username.

Password Policy

The account *Password Policy* determines how to create the password for all guest accounts. You can **Clone** the password policy to reuse configurations.

1. Navigate to **Policy Settings > Password Policy**. You can specify the following fields for the allowed password creation.



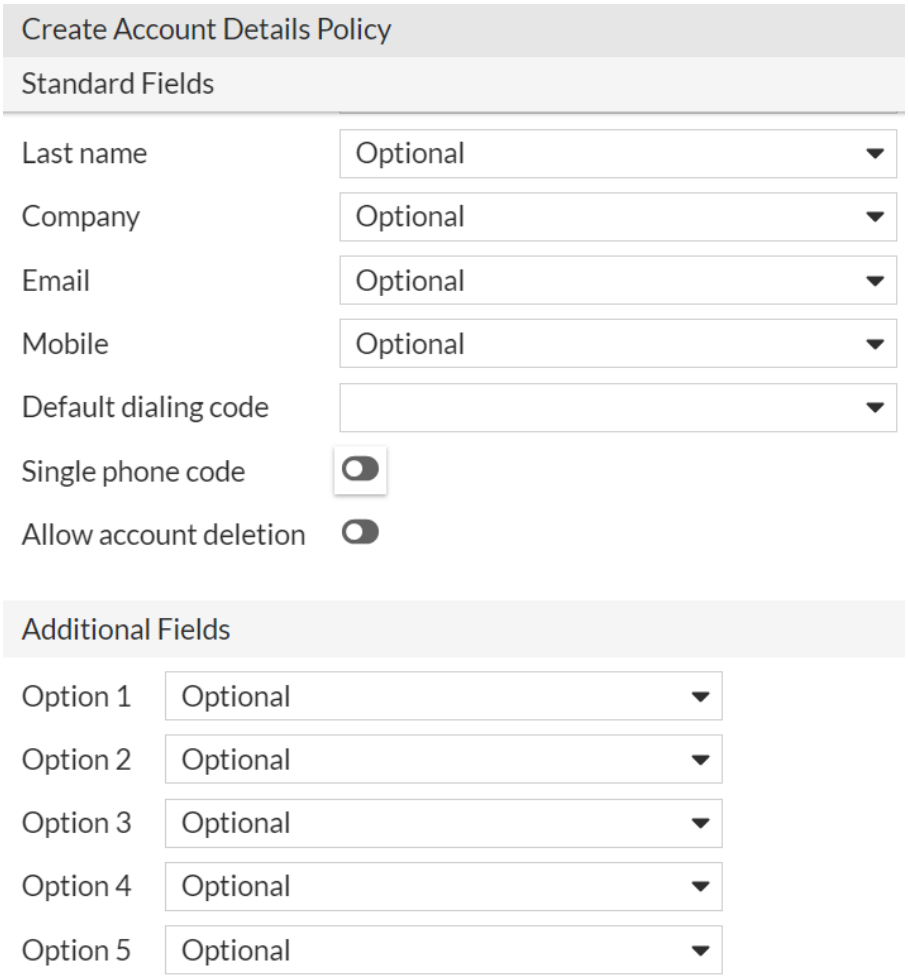
- **Minimum password length** - The required minimum password length for guests; the allowed minimum limit is 20.
- **Allow sponsor to change password** - Grant sponsors the permission to modify the guest password.
- **Force user to change password set by sponsor** - Allow the users to modify the guest password set by the sponsors.
- **Password generation mode** - FortiGuest automatically generates (**Auto generated password**) the guest password based on the configurations in this page, you may also allow the guest to specify a password (**Guest specified password**).

2. You can set the following password complexity parameters.
   - **Alphabetic characters to include** - The permissible alphabetic characters that the password can include.
   - **Number to include** - The maximum number of alphabetic characters allowed in a password. The limit is 20 characters.
   - **Numeric characters to include** - The permissible numeric characters (numbers) that the password can include.
   - **Number to include** - The maximum number of numeric characters allowed in a password. The limit is 20 characters.
   - **Other characters to include** - The permissible other (special) characters that the password can include
   - **Number to include** - The maximum number of other characters allowed in a password. The limit is 20 characters.

Policy Details

The *Policy Details* policy determines the data the sponsor needs to enter to create a guest account. Navigate to **Policy Settings > Policy Details**. The **Standard Fields** displayed are, **First name, Last name, Company,**

Email, **Mobile**, the **Default dialing code** of the country, usage of **Single phone code**, and **Allow account deletion**. You can **Clone** the policy settings to reuse configurations.



For each of these, you can specify one of the following three settings.

- **Required** - If a field is set to required it is mandatory for the user to complete.
- **Optional** - If a field is set to optional the user can choose not to complete the field.
- **Unused**—If a field is set to unused then no value is required.

You can use the **Additional Fields** to add any additional information that you require sponsors to fill out when creating guest accounts. There are five additional fields described as option 1 to option 5. Fortinet recommends customizing the text that is shown to the sponsor by editing the templates.

Access Management

Access Management allows an admin to define multiple admins with different set of privileges and their authentication mechanism. Admins can be authenticated against a local database or an external database/authenticator. You can configure multiple authentication servers in FortiGuest for administrator authentication.

- Administrator Authentication
- Admin Groups

Administrator Authentication

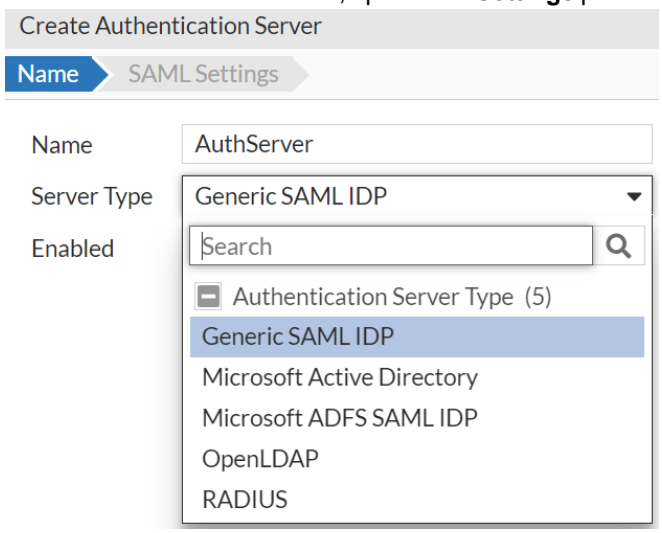
You can configure FortiGuest to authenticate administrators using external servers. FortiGuest has a default administrator account, called *admin*, in this section, you can create additional administrator accounts.

- External Authentication Servers
- Adding Administrator

External Authentication Servers

You can authenticate sponsors against the following external authentication servers. The external servers authenticate sponsors using their existing server credentials. It also enables the administrator to quickly roll out user access because there is no need to create and manage additional local sponsor accounts. You can create **Group Mappings**' rules to map the sponsor to a group based on information returned from the authentication server, see Admin Groups. You can **Clone** the authentication policy to reuse server configurations.

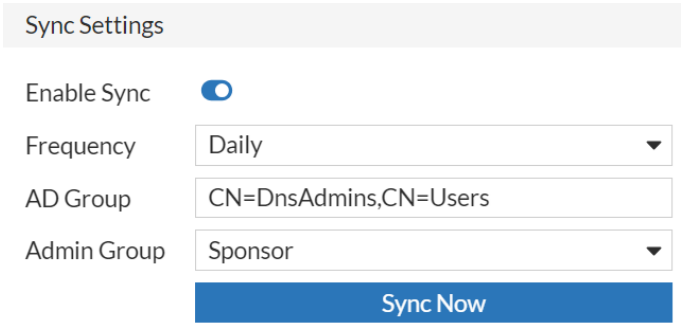
1. Navigate to **Access Management > Authentication > Authentication Servers** and click **New**.
2. Enter a **Name** for the authentication server and select any of the authentication **Server Type**. Based on the selected authentication server, update the **Settings** parameters to create an authentication policy.



The following external servers are supported for authentication.

- **Microsoft Active Directory** - See section Microsoft Active Directory.
- **OpenLDAP** - See section Open LDAP
- **RADIUS** - See section RADIUS.
- **Generic SAML IDP** and **Microsoft ADFS SAML IDP** - See Security Assertion Markup Language (SAML) Support on page 69.

Administrators can synchronize users and also configure the synchronization frequency when editing the Microsoft AD authentication servers. Edit an existing authentication server to use this feature.



Notes:

- For authentication with external servers like Active Directory and LDAP, ensure that the remote user is part of at least one group. For RADIUS authentication, the server needs to respond back with a class attribute. If there is no class attribute from a RADIUS server or a group returned from LDAP, the authentication fails.
- For authentication with external servers, if the group mapping does not match then the sponsor is mapped to the sponsor group that is already defined on portal.

Adding Administrator

You can create additional multiple admin accounts directly on FortiGuest.

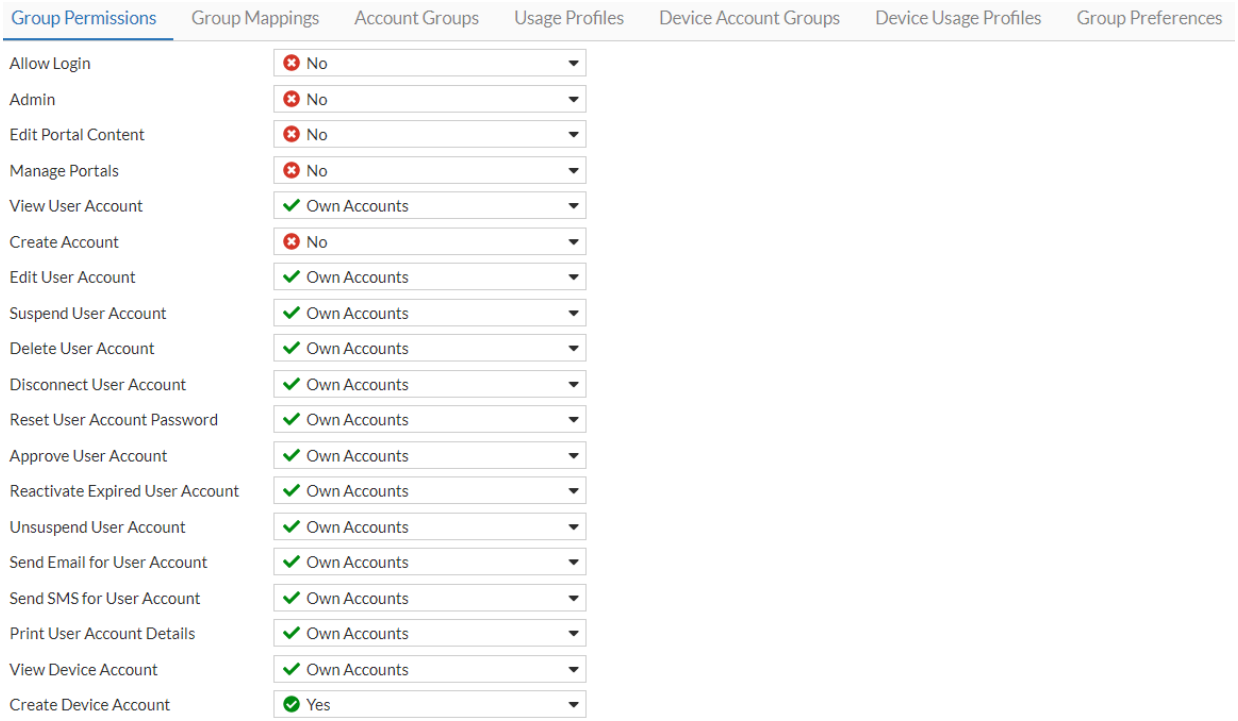
1. Navigate to **Access Management > Authentication > Admin Users**.

2. Update the following Sponsor credentials.
   - **Username** - Enter the administrator username.
   - **Full Name** - Enter the first and last name of the administrator.
   - **Email** - Enter the administrator email address.
   - **Password** - Enter the administrator user password.
   - **Confirm** - Confirm the configured password.
   - **Group** - Select the group for administrator account.

Admin Groups

Admin groups allow you to assign permissions to the sponsors. You can set role-based permissions for sponsors to allow or restrict access to different functions, such as creating accounts, modifying accounts,

generating reports, and sending account details to users via email or SMS. Navigate to **Access Management > Admin Groups** and update the following settings. You can **Clone** the admin group to reuse configurations.



Update the following user group settings in the subsequent configuration tabs.

- Edit and set the **Group Permissions** for the new user group as per your requirement.
- Create **Group Mappings** rules to map the sponsor to a group based on information returned from the authentication server. Select the server you wish to create a rule for and then select whether the group class name equals to or contains a specific term.
- The **Account Groups** allow a sponsor to assign different levels of access to a user account. You can select which sponsor user groups are allowed to assign certain profiles to users. By default, a sponsor user group has the ability to assign users to the default profile. The administrator can choose the additional groups the sponsor can assign, or can remove the default profile from the user group.
- The **Usage Profiles** allow a sponsor to assign different levels of access usage to a user account. You can select the sponsor user groups that are allowed to assign certain usage profiles to guests. By default, a user group has the ability to assign guests to the default usage profile. The administrator can select which additional usage profiles the sponsor can be assigned, or can remove the default usage profile from the user group.
- The **Device Account Groups** allow a sponsor to assign different levels of access to a device account. You can select which sponsor user profiles are allowed to assign certain account groups to device accounts.
- A user group has the ability to assign users to the **Device Usage Profile**. The administrator can select which additional usage profiles the sponsor can be assigned, or can remove the default device usage profile from the user group. Each user group must have the ability to assign Users in at least one device usage profile.
- In the **Group Preferences** the administrators can restrict/disable or enable controls on a sponsors default preferences page.

Guest Portals

Portals are used to allow administrators to create their own portal pages and host them on the FortiGuest. These are created by administrators and can be fully customized and used to provide the following.

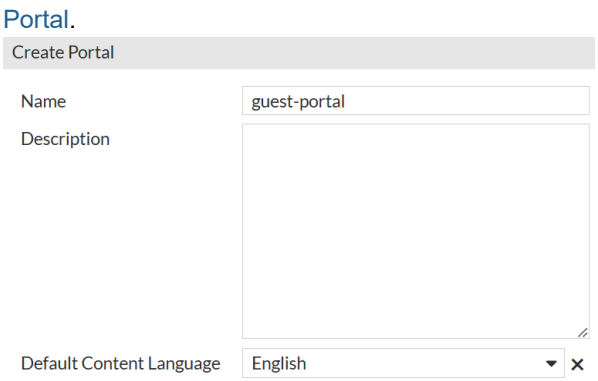
- Customized authentication pages - Allow portal pages to be located on the FortiGuest instead of on each captive portal device, providing a centralized location for configuration and display.
- Guest Self Service - Allows users to self-register by entering their details to create their own user accounts.
- Credit Card Billing support - Enables administrators to allow guests to purchase guest accounts by linking into payment gateways to purchase accounts.
- Hotel PMS Integration - Integrates multiple hotel PMSs to include the cost of internet access in the guest's hotel bill.
- Smart Connect - Secure Smart Connect provisioning for devices.
- Event Codes - Enables administrators to create event codes that allow users to create their own accounts during specific events

This chapter describes the following content.

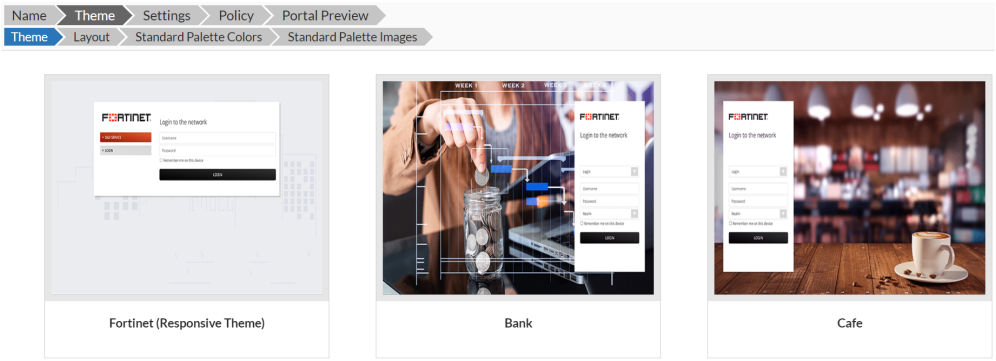
Creating a Guest Portal

Follow these steps to create a portal in FortiGuest. You can **Clone** a portal and reuse the configurations.

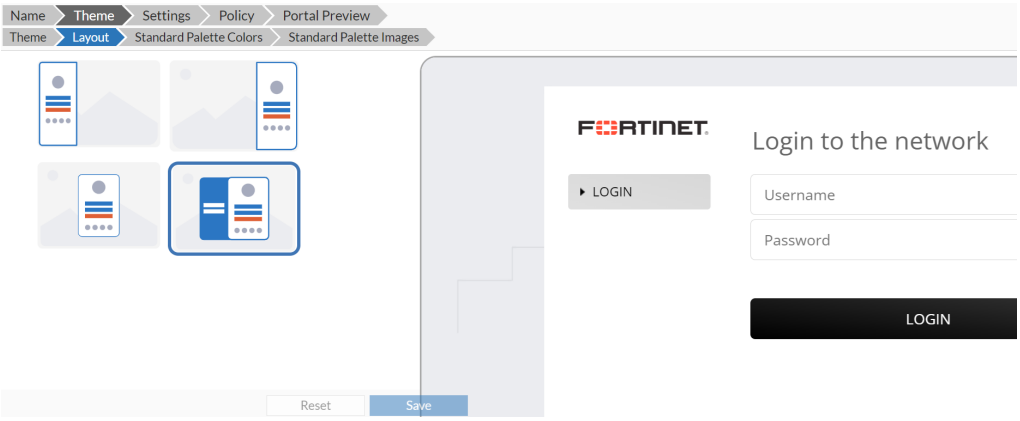
1. Navigate to **Guest Portal > Portals** to create a portal site.
   a. Enter a *Name* and *Description*. The name you enter is included in the portal URL and is visible to portal users.
   b. Select the **Default Content Language**. This is the default portal language unless it is manually changed. You can add multiple languages to a guest portal. See Adding Multiple Languages to Guest



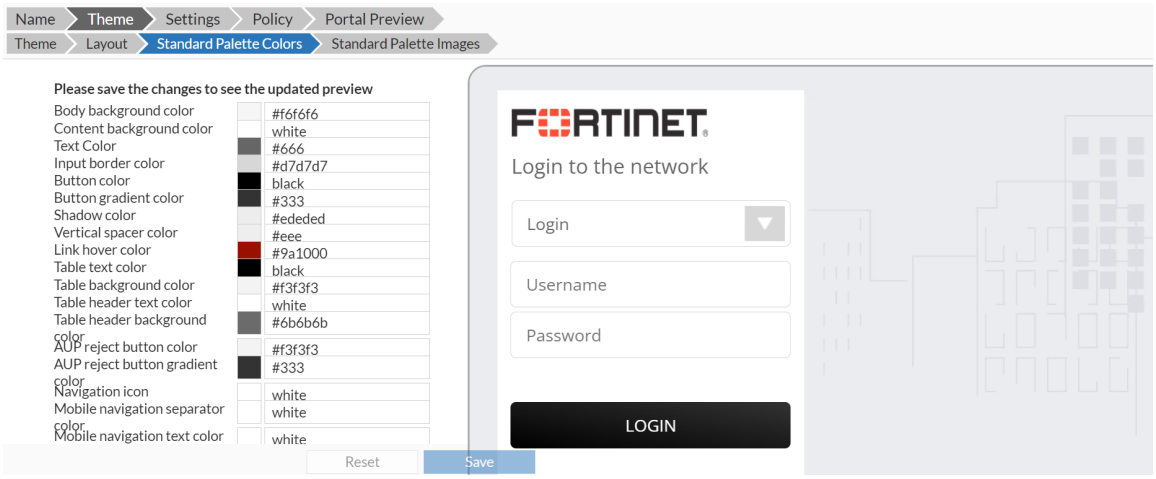
2. Select a pre-defined portal theme, multiple default themes are available for the guest portal based on your enterprise requirements. You can also upload new customized themes in *Guest Themes*.



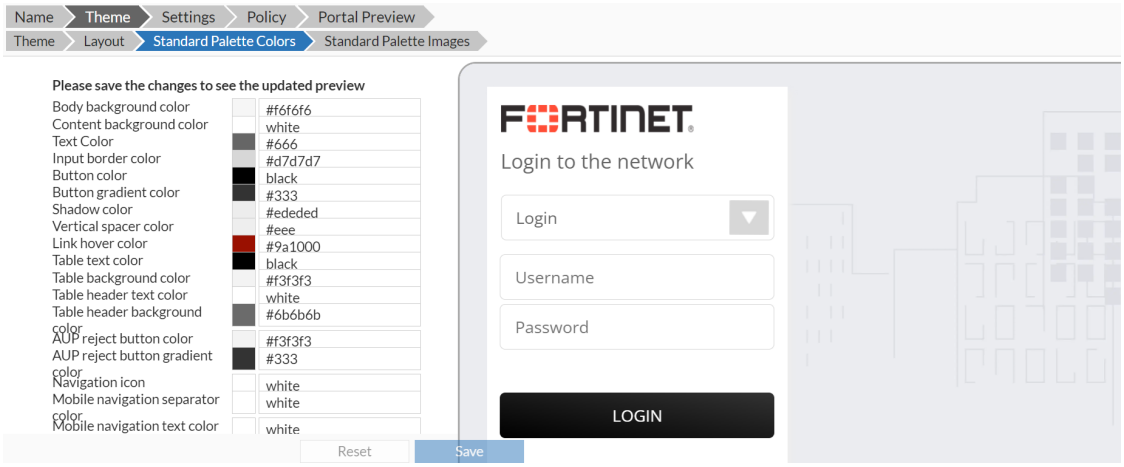
3. Define the layout type for visual representation of the portal page. Select the layout in the **Layout** tab, the available options allow you to align the content in the center, right, or left side of the portal page. The background image of the pages does not change as per the defined layout, it is just the position of the content that is changed as depicted in the following image.



4. A Select a color scheme for your portal theme from the **Standard Palette**.



5. Select a corporate logo image for the device accessing the guest portal in the **Standard Palette Images** tab. Click **Change Image** to upload display images of your choice.



   You can preview the portal page with the selected **Layout**, **Standard Palette Colors**, and **Standard Palette Images**, in the live preview component/panel. Save the changes on these pages to preview them.

6. Configure the Settings and Policy tabs to complete creating the guest portal.

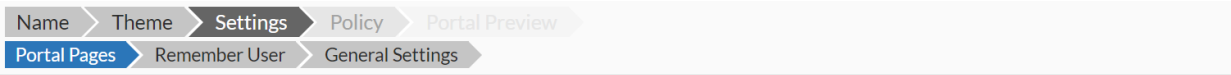
Settings

You are required to configure and apply multiple general and specific settings to the guest portal across various tabs displayed on this page.

- Portal Pages
- Remember User
- General Settings
- Self Service Settings
- Notification Settings

Portal Pages

You can add or remove features to the guest portal by modifying the selection of pages that should be available to users. In each case, enable pre-auth to make the feature available before authentication and enable post-auth to make the feature available after authentication. If you do not enable either of the options, then the feature is disabled.



Page	Displayed in Menu	
	Enabled pre-auth	Enabled post-auth
Login	●	○
Acceptable Usage Policy	●	●
Password Change	●	●
Password Recovery	◐	○
Self Service	◐	◐
Device Registration	○	◐
CC Billing	◐	●
PMS Billing	●	○

The following options can be enabled for the guest portal.

- **Login** - Display a screen that will allow a user to Login in.
- **Acceptable Usage Policy** - Display the usage policy to access and use the guest portal.
- **Password Change** - Display a page allowing the user to change their password.
- **Password Recovery** - Display a page allowing password recovery options.
- **Self Service** - Display a page that allows a user to create their own account using the self service menu.
- **Device Registration** - Display a screen that enables a user to register their own device.
- **Success** - Display a screen that shows successful authentication.
- **CC Billing** - Display a screen that enables Credit Card Billing.
- **PMS Billing** - Display a screen that enables PMS Billing.
- **Welcome Back** - Display a welcome back page if the user has authenticated previously.
- **Logout** - Display a logout button.
- **Logged Out** - Display a logged out page.
- **SmartConnect** - Check to enable Smart Connect on the portal.
- **Click Through** - Allow access without having to authenticate.
- **My Account** - Display *My Account* details for the user to manage their account once logged in.
- **Session Management** - Allow users to close existing sessions when the concurrent session limit is exceeded.

Remember User

You can enable storing guest user credentials in FortiGuest, that are used to login automatically when the user connects again. The credentials are stored based on the browser cookies or device MAC address.

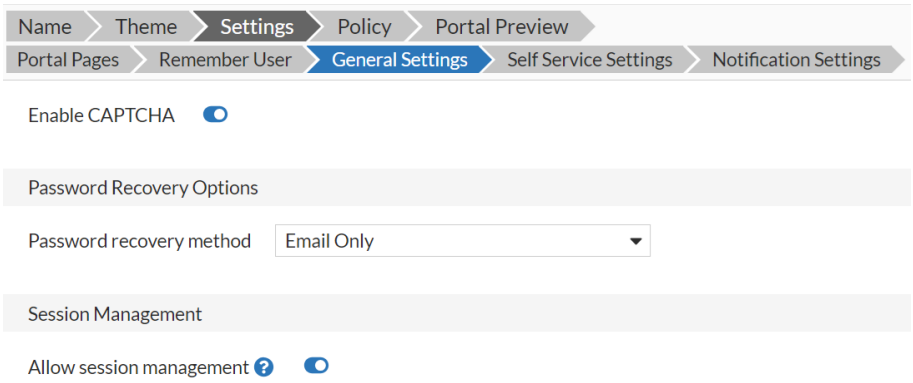
- **Remember Credentials** – Select the setting to apply to the remember user option. If you select *Let user choose*, then the remember user option is displayed in the login page of the guest portal. The guest can enable/disable it.
- **Remember for** – Select the time duration for which the credentials are stored, in the number or hours or days.
- **Remember a user by** – Select the method for storing the credentials. The following methods are available.
  - Cookies - The user credentials are encrypted and stored in a cookie that is saved in the device browser. When the user connects again, this cookie fetches the credentials, allowing the user to connect automatically without logging in.
  - MAC Address - The MAC address of the device is stored in the database and the credentials are stored in the cache for that MAC address. When the user connects again from the same device and the MAC address match is found in the database, then the user connects automatically without logging in.
  - Initially fetch the credentials using the cookie, if that fails, then retrieve the user credentials using the device MAC address.

Notes:

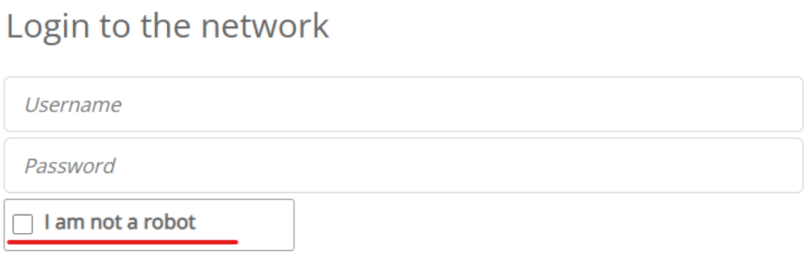
- FortiGuest stores user credentials only after successful authentication.
- This feature is not applicable, if FortiGate/enforcement device is configured with a re-direct URL other than FortiGuest, after authentication.
- The saved user credentials are deleted if the guest user logs out or changes/resets password.
- If the **Remember Credentials** is changed to **Never**, then all stored credentials saved for that portal are deleted.

General Settings

Based on the configured portal page settings, you are prompted to update the general settings for the guest portal.



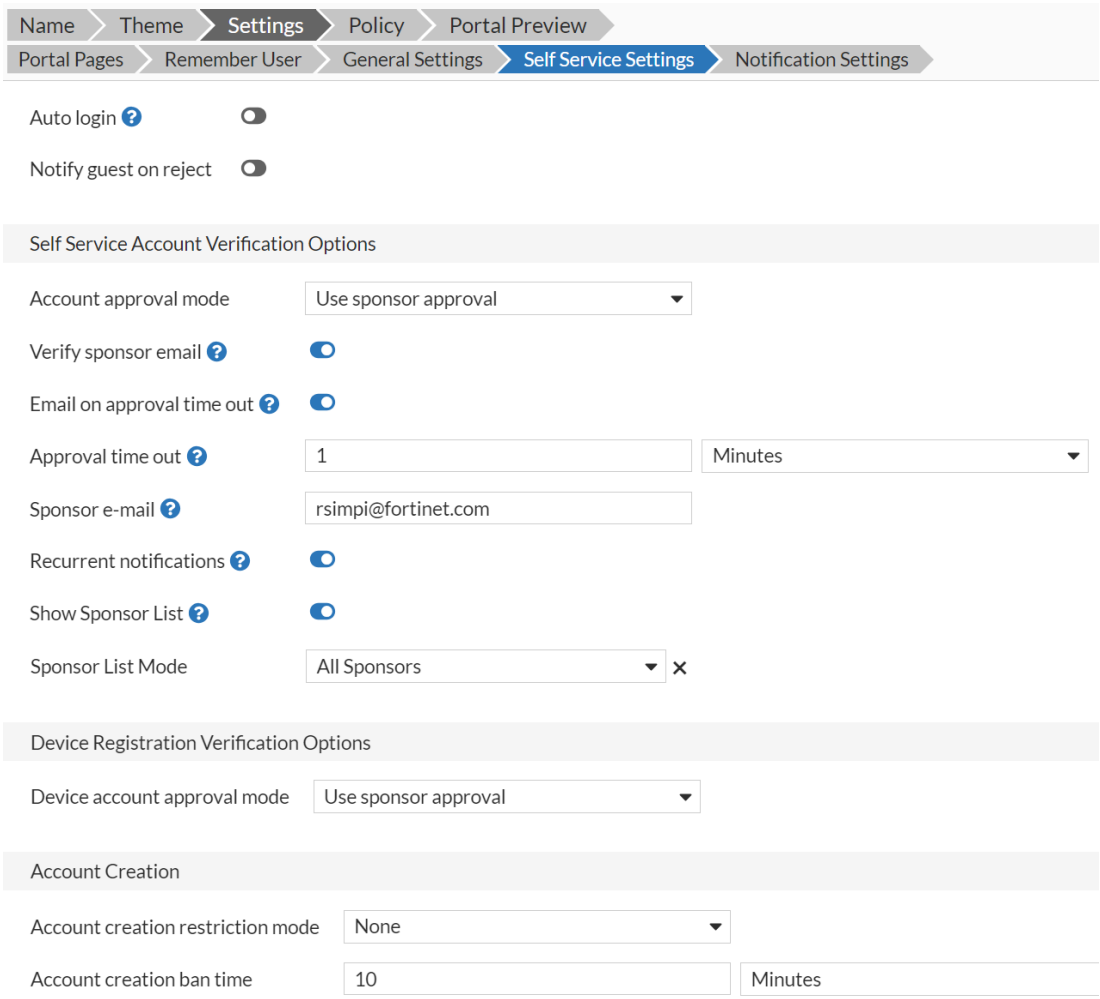
- **Enable CAPTCHA** - You can enable CAPTCHA for enhanced security. The CAPTCHA is available in the login page of the guest portal.



- **Password recovery method** - Select the user password recovery method. FortiGuest sends the new password as per the selected method.
- **Allow session management** - Allow users to close existing sessions when the concurrent session limit is exceeded.

Self Service Settings

If you have enabled the self service option for portal pages, you are required to configure these settings.



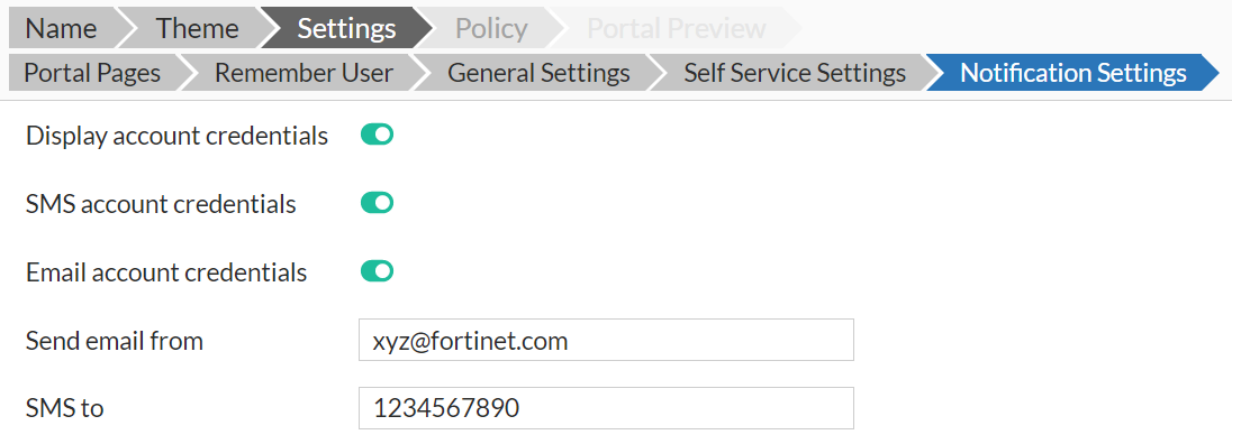
- **Auto login** - If enabled, the user is presented with a login button that allows them to authenticate without providing the new account credentials.
- **Notify guest on reject** - If enabled, the user is notified when the account request is rejected.

- **Self Service Account Verification Options** - You are required to select the **Account approval mode**. This field provides the option to **Use Event Codes** wherein the user is required to provide a valid event code generate an account or **Use Sponsor Approval** wherein a sponsor must approve the account before it is activated. Update the following parameters for sponsor approval.
  - **Verify sponsor email** - If this option is enabled, the email address entered by the guest is validated against the internal sponsor database and external authentication servers.
  - **Email on approval time out** - If this option is enabled, a message is sent to a designated email address after the defined time out period.
  - **Approval time out** - This is the time window sponsors have to approve or reject the account before a notification email is sent to the designated sponsor.
  - **Sponsor email** - The email address of the sponsor in charge of dealing with guest accounts waiting for approval.
  - **Recurrent notifications** - The notification emails are sent recurrently until the account is approved, rejected, or expires.
    Optionally, you can enable the **User sponsor approval and event codes** option to use both the features.
  - **Show Sponsor List** - The sponsor list (with valid email addresses only) is displayed. Once enabled, select a sponsor from the **Sponsor List Mode** that displays the following sponsors.
    - **All Sponsors**
    - **All Local Sponsors**
    - **All Remote Sponsors**
    - **Sponsors based on Server Types** and select the authentication server type. Sponsors in the selected servers are only displayed in the guest portal page.
    - **Sponsors based on User Groups** and select the user groups. Sponsors in the selected user groups are only displayed in the guest portal page.
      Note: Microsoft Active Directory and OpenLDAP are the only supported server types options.
- **Device Registration Verification Options** - You are required to select the **Device account approval mode**. This field provides the option to **Use sponsor approval**, so that a sponsor must approve the account before it is activated.
- **Account Creation** - You can configure the account re-creation restrictions. Set the **Account creation ban time**, that is, the time interval that prevents the creation of self service accounts with the same personal details (email/phone) post the original account creation. You can enforce the ban based on the phone or email address in the **Account creation restriction mode**. An additional option, **None**, is also added to NOT enforce this uniqueness in the guest accounts. The following features are applicable, if the user enforces a unique phone or email address.
  - The guest user cannot create a new account with an email address/phone, if an active account with the same email/phone already exists.
  - The email address/phone is a mandatory field in the guest portal, even if it is not set as the username in the username policy.
  - If a guest account exists with the same email address/phone and is inactive, then you can create another account with the same.
  - Since the username is unique, and 2 different accounts cannot exist with the same username, the account's username is pre-fixed with a numeric value

If the user does NOT enforce a unique email address/phone, then guest user can create multiple accounts with the same credentials. The accounts will have different usernames, pre-fix the username with a numeric value.

Notification Settings

Define the notification options to send email and SMS notifications to the guest.



Policy

You can define various policies for users to access and use the guest portal.

- Payment Provider
- PMS Provider
- Access Plans
- Realm Policy
- Allowed Account Groups
- Username Policy
- Password Policy
- Policy
- Redirection Policy

Payment Provider

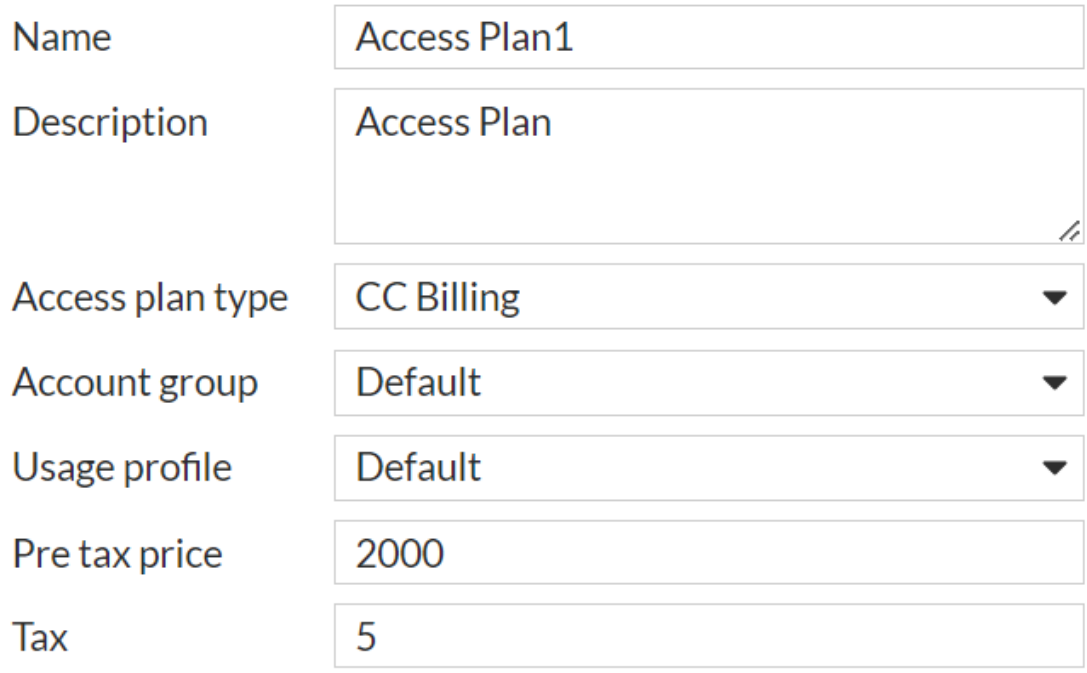
Select the payment provider configured to enable credit card billing. See Credit Card Billing.

PMS Provider

Select the Hotel PMS provider configured in Hotel Property Management System (PMS) and select the currency to make the payment.

Access Plans

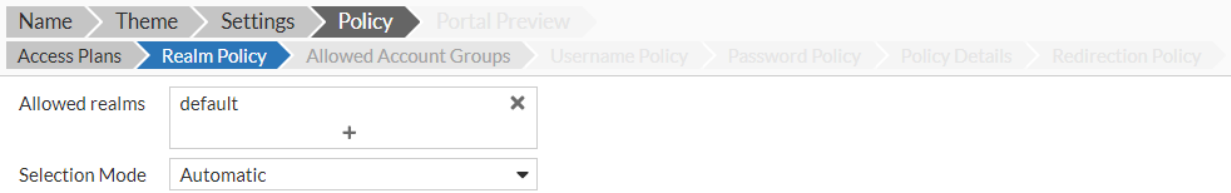
The access plan policy implements the usage and account policies for any self-service user account. The user account is created in FortiGuest as per the usage profile and account group mapped to the access plan. The default self -service and device registration plans are mapped to the default usage profile and account group. You can manage the access plans that the users accessing the guest portal are allowed to select.



- **Name** and **Description** - Enter a unique name and description for your access plan.
- **Access plan type** - Select whether the access plan is for *Self Service*, *CC Billing*, or *PMS Billing*.
- **Account group** - Select a pre-defined account group. See Account Groups
- **Usage profile** - Select a pre-defined usage profile. See Usage Profiles.
- **Pre-tax price** - If your profile is assigned to a billing plan, then enter the price of your plan, prior to the applied tax.
- **Tax** - Enter the percentage of tax you wish to charge.

Realm Policy

This policy selects the realms to use for authentication in the login page. The realms are defined in the Authentication Policies and are used to authenticate users against different external servers.



- **Allowed Realms** - Select and add the realms for authentication.
- **Selection Mode** - If the selection mode is **Automatic**, then each realm added in the **Allowed Realms** field is selected in the order in which it is listed. The realm selection starts from the first one and if authentication fails the next realm in the order is tried and so on. If the selection mode is **Manual** then the user is allowed to select the displayed realms in any order.

The first realm in the order is treated as a default realm, the default realm is selected by default when the user navigates to the login page in the manual **Selection Mode**.

Allowed Account Groups

Select the pre-configured account groups. See Account Groups

Username Policy

Configure the username policy. See Username Policy

Password Policy

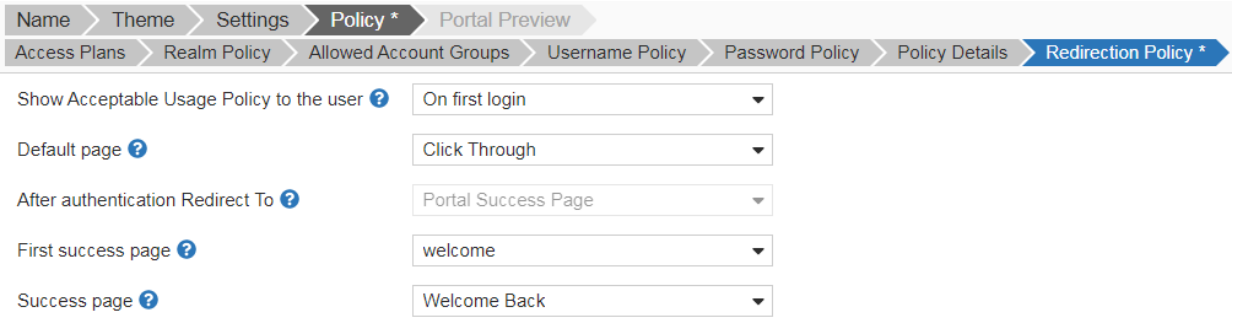
Configure the password policy. See Password Policy.

Policy Details

Configure the policy details. See Policy Details.

Redirection Policy

Configure this policy to redirect the users are they login into the guest portal.



- **Show Acceptable Usage Policy to the user** - Select the option to specify when the user has to accept the Acceptable Usage Policy after authentication.
- **Default page** - The portal page that the guests are redirected to after they login into the network for the first time.
- **After authentication Redirect To** - The configured portal page where the user is redirected to after successful portal authentication.
- **First success page** - The configured portal page that the first time users are taken to after successful authentication.
- **Success page** - The configured portal page that the returning users are taken to after successful authentication.

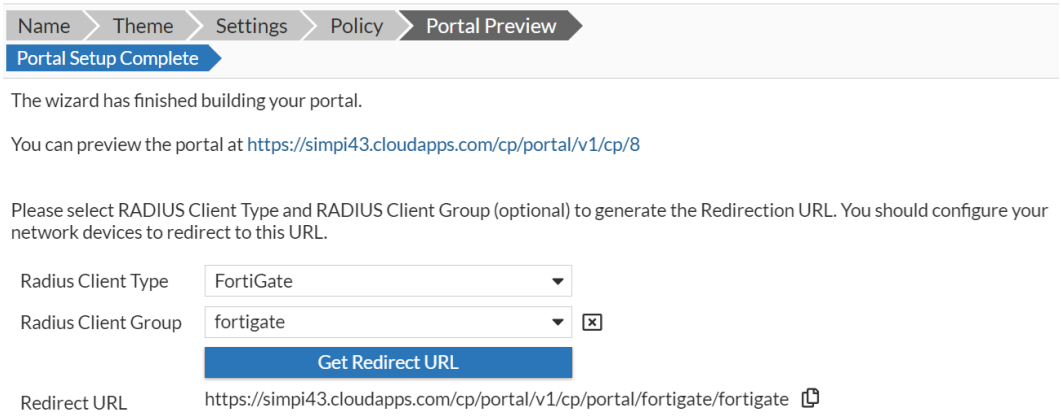
Creating the Portal Redirection URL

You can use the device IP address or the RADIUS client type to generate the redirection URL, this enables RADIUS clients of the same type to have a common redirection URL. Optionally, you can also include the RADIUS client group in the URL, this allows the admin to have a different URL within the same type of RADIUS clients. See RADIUS Client Group.

The following redirection URL formats are supported.

- *https://{Fortiguest}/cp/portal/v1/cp/portal/{Device_IP}*
- *https://{FortiGuest}/cp/portal/v1/cp/portal/{RADIUS_client_type}*
- *https://{FortiGuest}/cp/portal/v1/cp/portal/{RADIUS_client_type}/{RADIUS_client_group}*

When configuring the guest portal, in the **Portal Preview** tab, you can select the **RADIUS Client Type** and **RADIUS Client Group** (optional) to generate the Redirection URL. Click **Get Redirect URL** to generate the redirection URL.



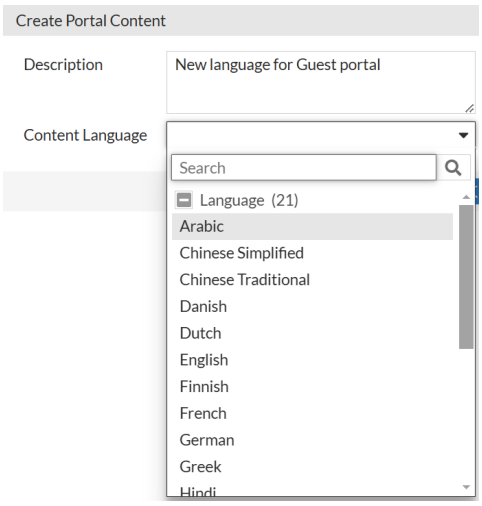
Notes:

- All access requests from the same RADIUS client type lead to the same portal, unless there are any other contrary conditions configured under the rules or have RADIUS client grouping.
- For a generic device, the redirection URL with the device IP address is only supported.

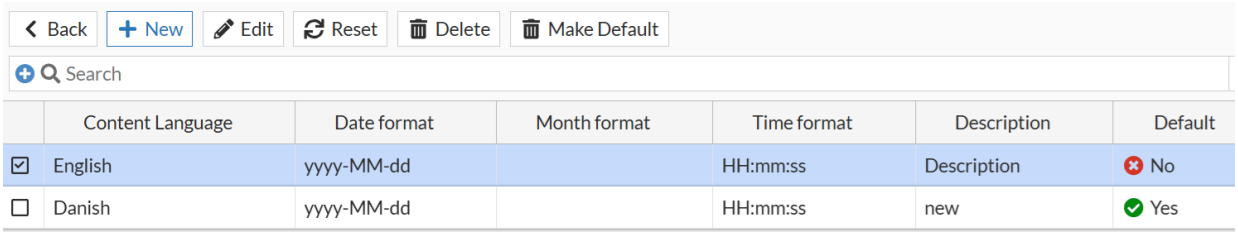
Adding Multiple Languages to Guest Portal

Perform the following steps to add more portal content languages:

1. Select the desired portal in the **Guest Portal > Portals** page and click **Edit Portal Content**.
2. Click **New**.
3. In **Create Portal Content** page, enter a description and select the desired language for the portal. All supported languages for the portal will be listed on this page.



To change the default language created earlier, select a different language on this page and click, **Make Default**.



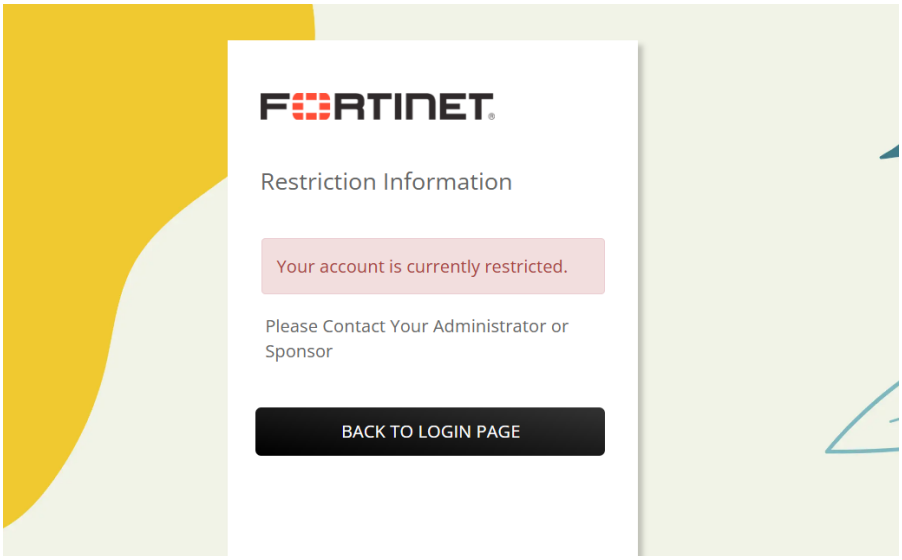
	Content Language	Date format	Month format	Time format	Description	Default
☑	English	yyyy-MM-dd		HH:mm:ss	Description	No
☐	Danish	yyyy-MM-dd		HH:mm:ss	new	Yes

The captive portal appears on the user device in the default language with a drop-down to change to another language.

- When the user accesses the guest portal for the first time, content is available in the default language.
- If the user selects another language, then this language is used on all subsequent guest portal logins

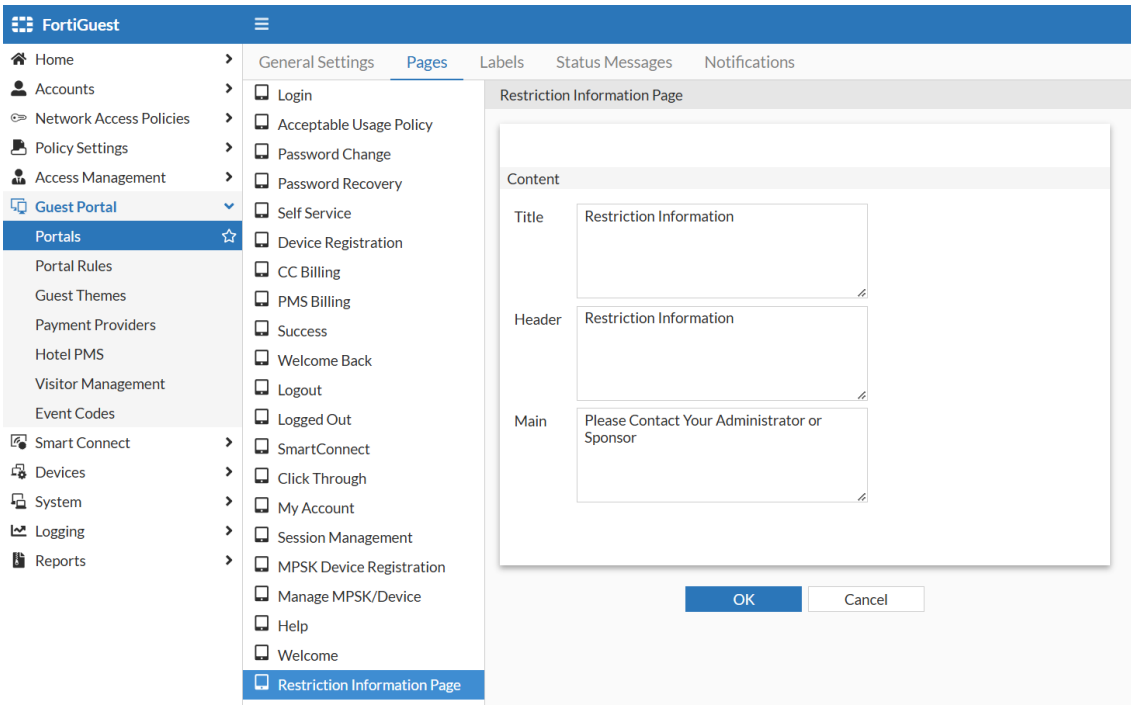
Configuring Restriction Information Page

FortiGuest supports a secondary landing page for captive portals. This page provides users with more specific information when they exceed usage limits or experience access restrictions. The error messages and the page content on this secondary landing page are customizable.

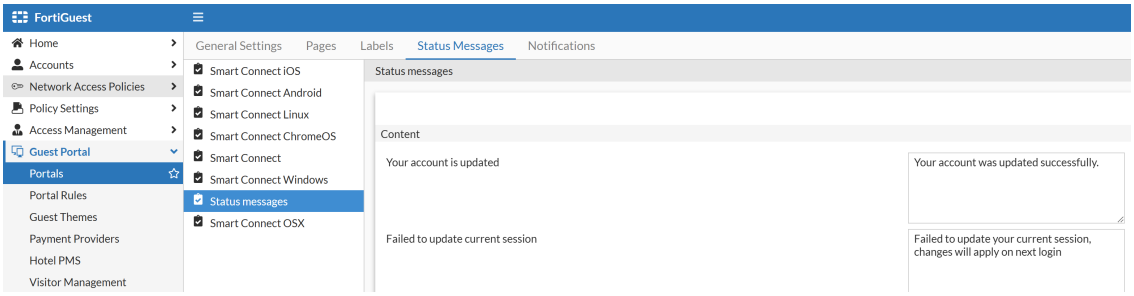


Perform the following steps to customize secondary portal.

1. Navigate to **Guest Portal > Portals**.
2. Select the desired portal and click **Edit Portal Content**.
3. Select the language of the portal and click **Edit**.
4. To customize the title and header content:
   a. Select the **Pages** tab and click **Restriction information Page**.
   b. Modify the **Title**, **Header**, and **Main** sections as needed.



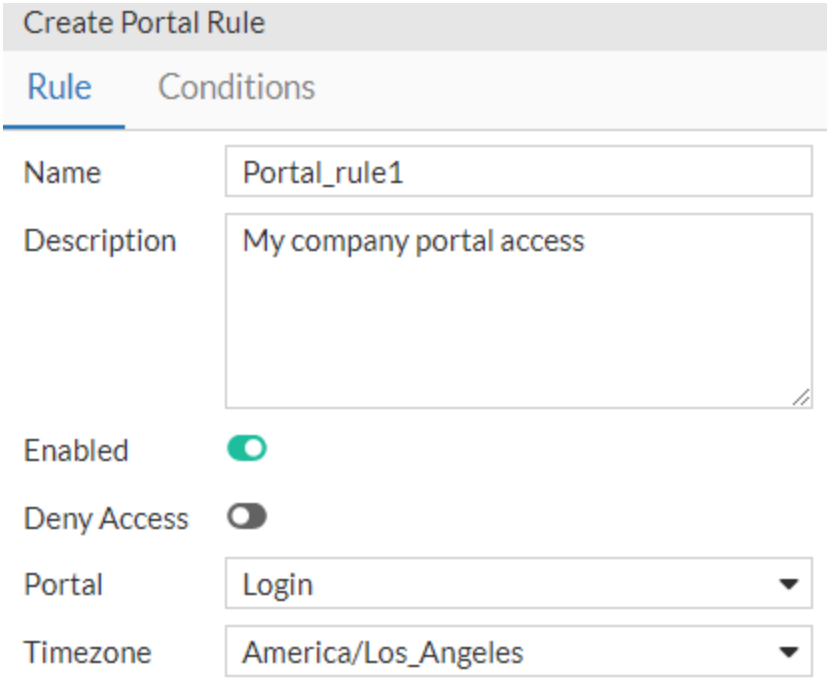
5. To customize error messages:
   a. Select the **Status Messages** tab and click **Status messages**.
   b. Modify the content for desired error message.



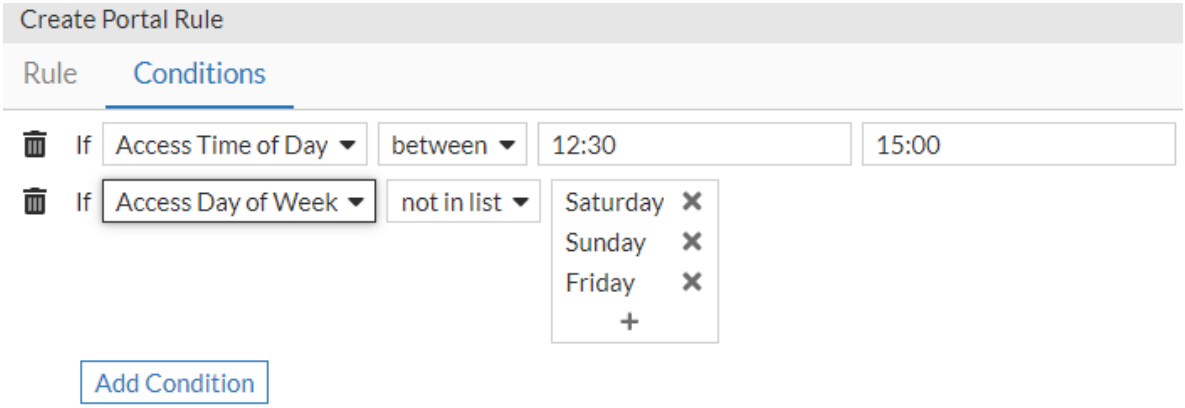
Portal Rules

The FortiGuest can be used to create a set of rules to allow user access to different portals that have been created. Each rule that is created is subject to certain conditions that you can create. If a rule is matched, the user is allowed or denied access to the portal and no other rules are checked. If no rule matches then the default rule is applied. You can **Clone** the portal rules to reuse them.

1. Navigate to **Guest Portal > Portal Rules** and create a rule.



2. Enter the **Name** of the new rule and provide a **Description**.
3. Select **Enabled** and then select one of the portals you have created, or the default portal from the **Portal** drop down menu to direct the user to the relevant portal.
4. Enable **Deny Access** if you do not wish to redirect the user to the guest portal.
5. Select the applicable **Timezone**.
6. Select the **Conditions** tab and create the conditions applicable to your portal rules.
7. Click **Add Condition** and create new conditions. From the provided drop down lists, create a set of rules that apply to your portal. In this example, the user is redirected to the portal **Login** (specified in the previous step) on a given day of the week (except Saturday, Sunday, and Friday) between 12:30 and 15:00.



Notes:

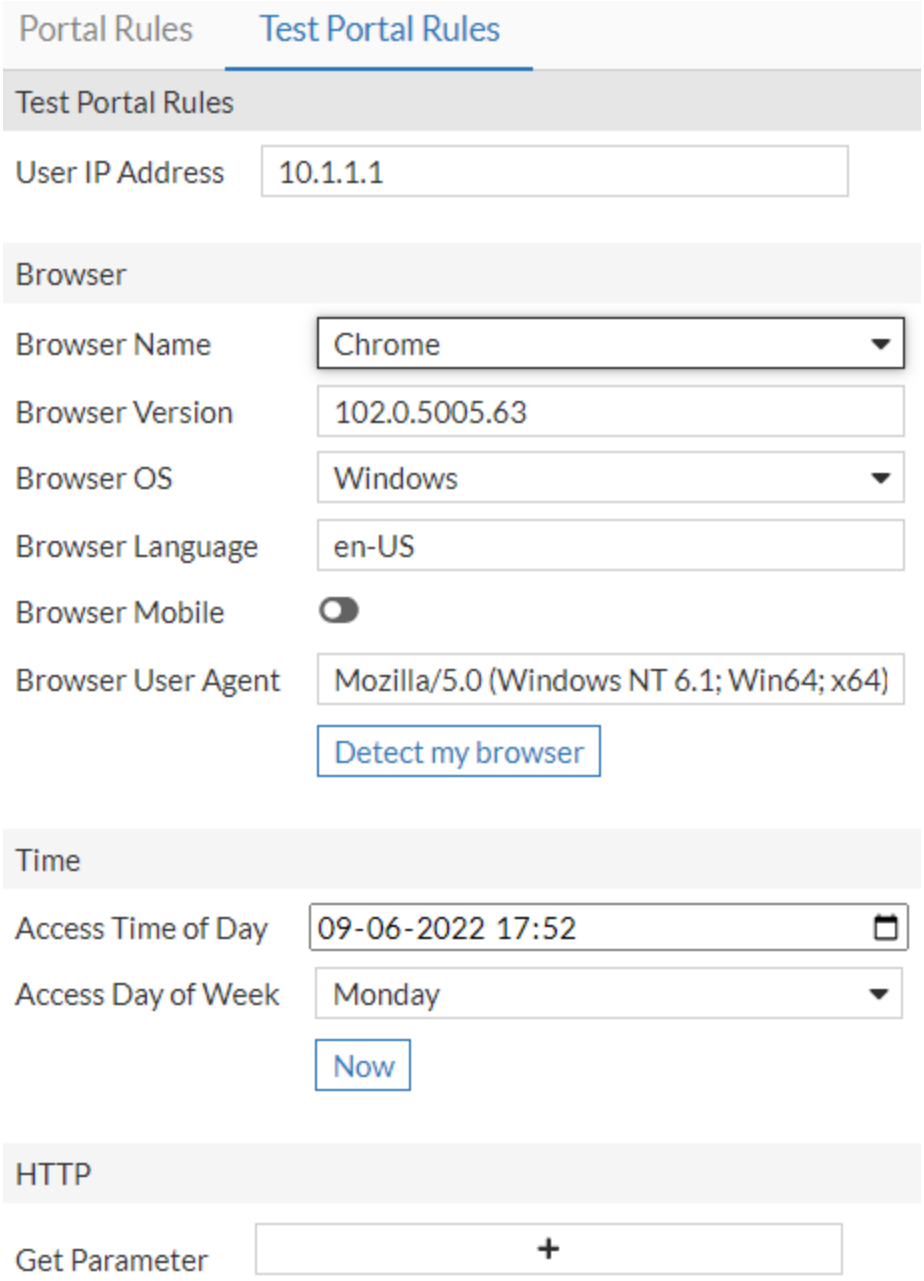
- Configure the following URL in the SSID for captive portal re-direction.
  `{FortiGuest_IP or FQDN}/cp/portal/v1/cp/portal/{FGT_IP}`
- Add the following FQDNs in the allowed list in FortiGate, for captive portal login with Google Chrome (Windows).

  - *Chrome: IP subnet 13.107.4.52 255.255.255.255*
  - *Fonts.gstatic.com FQDN*
  - *ssl.gstatic.com*
- RADIUS clients with a *generic* type cannot be added to any group.
- A RADIUS client cannot belong to multiple groups.

Test Portal Rules

You can test any portal rules you have created with the environment you define.

1. Navigate to **Guest Portal > Portal Rules > Test Portal Rules** and provide the following details.



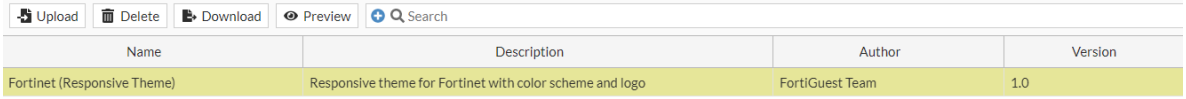
- **User IP Address** - Enter the User's IP Address.
- **Browser** - Select and define the browser details you wish to test against, such as browser type, version, OS, supported browser version and user agent. Enable **Browser Mobile** if you are using a mobile device. Optionally, click **Detect my browser** to allow FortiGuest to detect the browser on your machine.
- **Time** - Select the day of a week and a specific time to test the portal. Click **Now** to test the portal at a given time.
- **HTTP** - Update the HTTP fields for the web browser.

2. Click **Test**.

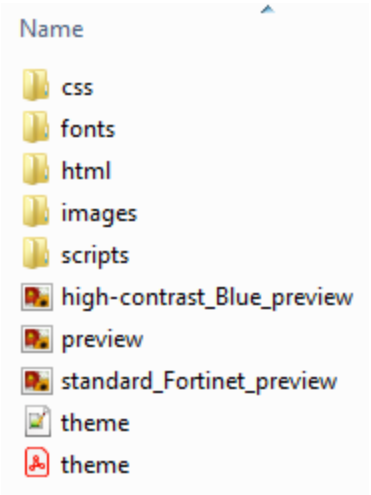
Guest Themes

You can create guest portal themes as per your business requirement. FortiGuest provides a default theme that you can download, customize and upload it. Ensure that you comply to the **Rules**, to successfully upload guest themes.

1. Navigate to **Guest Portal > Guest Themes**.



2. Select the default theme (or any existing theme) and click **Download**.
3. Unzip the downloaded file to view the folder structure of the theme.



4. Update the following files and folders and upload them on this page.
   - theme.css
   - theme.json
   - images
   - html

theme.css

This file is in the **css** directory of the theme structure and contain all the styles that are applied to the several HTML pages that make up the portal site.

theme.json

The *theme.json* file lists all resources used by the theme as well as defining the default values for several elements. You can update the following elements.

- id
- public_name
- author
- mandatory_pages
- optional_pages
- Layout

- images
- standard_palettes

id

This is a mandatory element, it should only contain letters, digits and the underscore symbol, theme IDs are unique so if there is already a theme with this ID installed on FortiGuest, then you cannot install this theme.

public_name

This is an optional element, it should contain the name displayed on the administration interface when referring to the theme, this element does not have the restrictions that apply to the ID element. If the **public_name** element is not present, the theme's internal name is displayed.

author

This attribute is used by the theme author to place his name and/or contact details.

mandatory_pages

In this element, you can list the HTML templates for every kind of page the portal uses as well as declaring what content areas each page has and what should be it's default value.

```
"login": {
      "menu_item_weight": 1,
      "label": "Login",
      "components": [
           {
                "label": "Title",
                "tag": "%TITLE%",
                "content": "Login to the network"
          },
          {
                "label": "Header",
                "tag": "%HEADER%",
                "content": "Login to the network"
          },
          {
                "label": "Main",
                "tag": "%MAIN%"
          }
    ]
}
```

This example specifies the HTML template for the login page in the **html** folder. The *login.html* file uses the following components.

```
<h2 id="pageTitle">%HEADER%</h2>
<div class="feedbackContent">%FEEDBACK_AREA%</div>
<div class="mainContent">%MAIN%</div>
<div class="widgetContainer">%LOGIN_WIDGET%</div>
```

```
<div id="loginNavigation" class="col-md-4 hidden-sm hidden-xs"> %NAVIGATION_MENU%
</div>
```

The placeholder variables for the several components defined in *theme.json* are placed amongst the markup, when the portal pages are generated the placeholders are replaced with the content associated with them. The content of these placeholders is built dynamically by FortiGuest depending on what options are selected during the portal setup. When creating your own themes you should make sure that these placeholders are in your template files otherwise the portal might not work as expected.

optional_pages

This section allows you to specify any optional pages you want to make available to portals using your theme. The default theme defines several optional pages, to add more you can copy one of the existing definitions and edit it as appropriate.

```
"menu_item_weight": 1000,
"label": "Welcome",
"id": "welcome",
"description": "Welcome page, can be used as alternative landing page to portal",
"components": [
      {
           "label": "Title",
           "tag": "%TITLE%",
           "content": "Welcome"
      },
     {
           "label": "Header",
          "tag": "%HEADER%",
          "content": "Welcome"
     },
    {
           "label": "Main",
          "tag": "%MAIN%",
          "content": "Welcome"
     }
]
```

Layout

The element **layout** is present in *theme.json* with the supported values of *one_panel_center*, *one_panel_right*, *one_panel_left*, and *two_panel*.

```
"layout": "two_panel"
```

images

This element of the file is used to list all image files that are referenced by the HTML and CSS for the theme. You can modify the default images by replacing them with your own `file_name`.

```
{
      "label": "Company logo large",
      "description": "Used on the login page on large screen devices",
      "tag": "%IMG_LOGO%",      "file_name": "Logo.png",
```

```
      "dimensions": "300x40"
}
```

This snippet specifies the label, description and recommended dimensions for the image. This information is displayed on the portal setup page so the administrator knows what this image is used for and can upload the right image for this purpose. The `tag` element specifies what placeholder variable is used in HTML and CSS template files to refer to this particular image, `file` element specifies which file is the default value for this image. All files are placed in the **images** folder.

To use this image in the login HTML template, add this to *login.html*.

```
<div id="headerImage" class="text-center"><img src="%IMG_LOGO%" class="img-responsive"/></div>
```

standard_palettes

These elements contain a list of all customizable colours used in the theme. The default theme already has a set of colour palettes defined, to add a new one, you can edit as follows.

```
{
     "tag": "%CL_BODY_BACKGROUND%",
     "label": "Body background color",
     "value": "#f6f6f6"
}
```

This snippet specifies the label and value for the colour, this information is displayed on the portal setup page so the administrator knows where and what for the colour is used for. The `tag` specifies what placeholder variable is used in HTML and CSS template files to refer to this colour, the `value` element specifies the colour hex value.

images

This folder contains all images used in your guest theme. Add all the images that you want to use in this folder.

html

This folder contains all the HTML files that are a part of the guest portal. You can edit all these files as per your requirement and portal design.

Rules

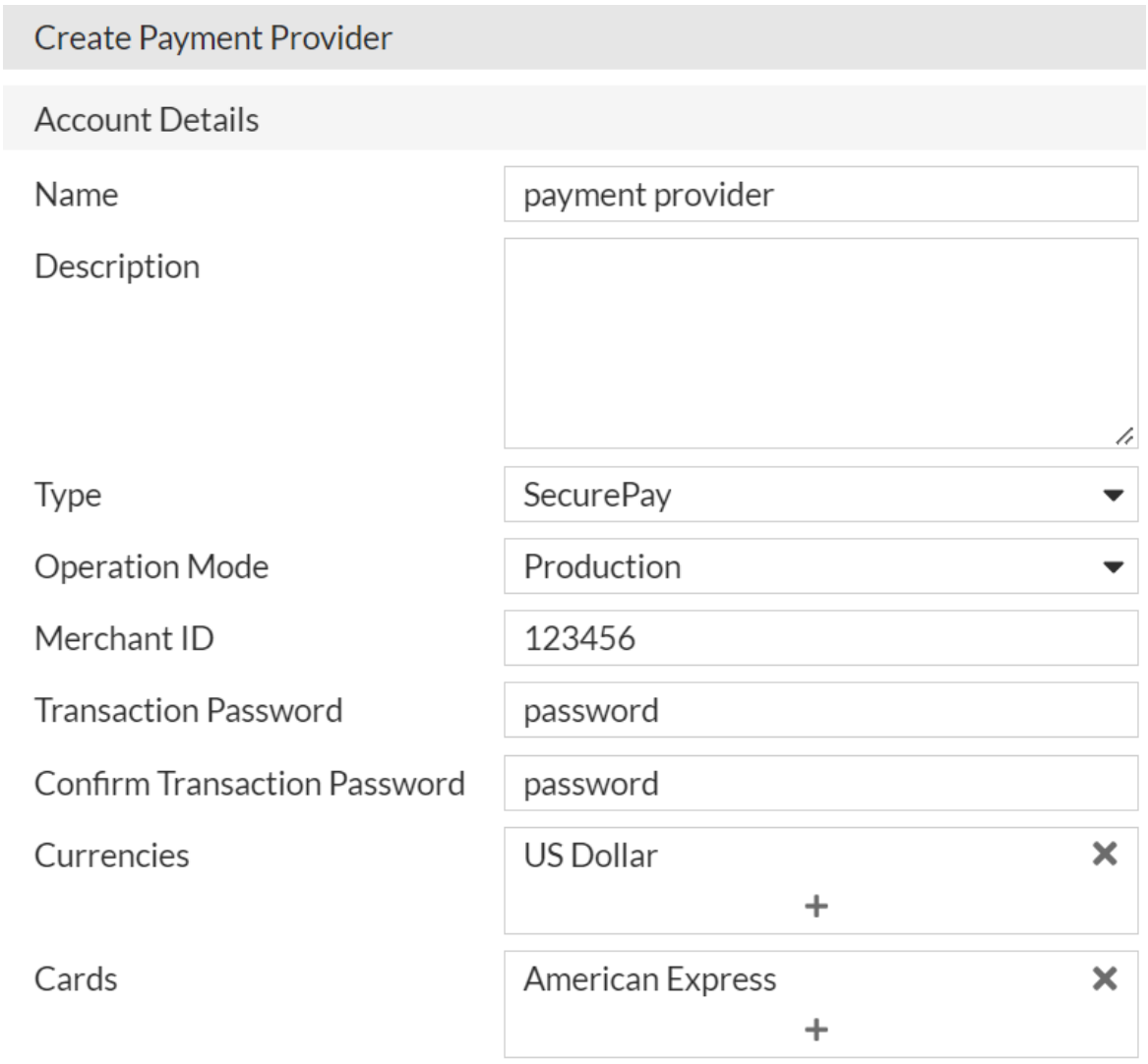
To successfully enable the upload of guest themes, ensure that the following rules are complied with.

Rule	Acceptable values
HTML elements	`html, body, nav, a, abbr, acronym, address, area, b, big, blockquote, br, button, caption, center, cite, code, col, colgroup, dd, del, dfn, dir, div, dl, dt, em, font, h1, h2, h3, h4, h5, h6, hr, i, img, ins, kbd, label, legend, li, map, menu, ol, p, pre, q, s, samp, small, span, strike, strong, sub, sup, table, tbody, td, tfoot, th, thead, tr, tt, u, ul, var`

Rule	Acceptable values
HTML attributes	abbr, accept, accept-charset, accesskey, action, align, alt, axis, border, cellpadding, cellspacing, char, charoff, charset, checked, cite, clear, cols, colspan, color, compact, coords, datetime, dir, enctype, for, headers, height, href, hreflang, hspace, id, ismap, label, lang, longdesc, maxlength, method, multiple, name, nohref, noshade, nowrap, prompt, rel, rev, rows, rowspan, rules, scope, shape, size, span, src, start, summary, tabindex, target, title, type, usemap, valign, value, vspace, width, class, role, data-toggle, data-target, style
HTTP schemes	http, https, lml

Credit Card Billing

This feature enables administrators to allow guests to purchase accounts by linking into payment gateways. You can select your payment provider details to allow credit card billing into your account. After the payment is successful, an account is created as per the guest portal username and password policy and the guest is notified about the username/password details. In the guest portal, select the configured payment provider in Payment Provider and the Access Plans on page 99.

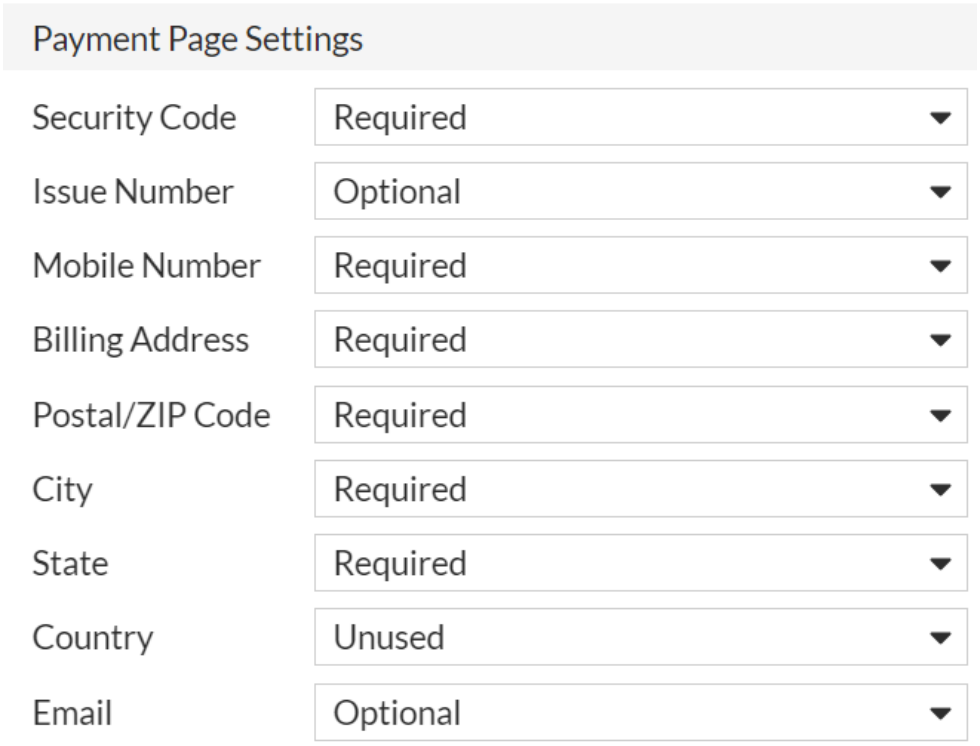


- **Name** - Enter a name for your account.
- **Description** - Enter a description for your account.
- **Payment Provider** - Select a payment provider, the supported providers are *Authorize.net*, *Peach Payments*, *Paya*, *PayPal*, *SecurePay API*, and *SecurePay*.

Type	Parameters
Authorize.net	• **Operation Mode** - Select the operation mode as *Production* or *Test*. You can select **Test** to test a transaction by sending gateway specific details to the payment provider. • **API Login** and **Transaction Key**- Enter the API login and the transaction key details for *Authorize.net*. • **Currencies** - Add the available currencies for your payment gateway. • **Cards** - Add from the available cards for the billing transaction.
PayPal	• **Operation Mode** - Select the operation mode as *Production* or

Type	Parameters
	Test. You can select **Test** to test a transaction by sending gateway specific details to the payment provider. • **Client ID** and **Client Secret**- Enter the client ID and secret for configuring PayPal. • **Currencies** - Add the available currencies for your payment gateway. • **Cards** - Add from the available cards for the billing transaction.
Peach Payments	• **Operation Mode** - Select the operation mode as *Production* or *Test*. You can select **Test** to test a transaction by sending gateway specific details to the payment provider. • **Bearer ID** and **Entity ID** - Enter the bearer and entity ID for configuring Peach Payments. • **Currencies** - Add the available currencies for your payment gateway. • **Cards** - Add from the available cards for the billing transaction.
SecurePay	• **Operation Mode** - Select the operation mode as *Production* or *Test*. You can select **Test** to test a transaction by sending gateway specific details to the payment provider. • **Merchant ID** and **Transaction Password** - Enter the merchant ID and transaction password for the SecurePay payment gateway. • **Currencies** - Add the available currencies for your payment gateway. • **Cards** - Add from the available cards for the billing transaction.
SecurePay API	• **Operation Mode** - Select the operation mode as *Production* or *Test*. You can select **Test** to test a transaction by sending gateway specific details to the payment provider. • **Merchant ID** - Enter the merchant ID for the payment gateway. • **Client ID** and **Client Secret**- Enter the client ID and secret for configuring SecurePay API. • **Currencies** - Add the available currencies for your payment gateway. • **Cards** - Add from the available cards for the billing transaction.
Paya	• **Operation Mode** - Select the operation mode as *Production* or *Test*. You can select **Test** to test a transaction by sending gateway specific details to the payment provider. • **User ID**, **User Key**, and **Location ID** - Enter the user ID, key, and location ID for configuring the Paya payment gateway. • **Currencies** - Add the available currencies for your payment gateway. • **Cards** - Add from the available cards for the billing transaction.

In the **Payment Page Settings** section, you can show or hide the input fields on the payment page of the portal, determine whether you wish use each field using the drop down menu.



- **Required** - Mandatory input required.
- **Optional** - Optional input required (not mandatory).
- **Unused** - Fields will not appear.

Notes:

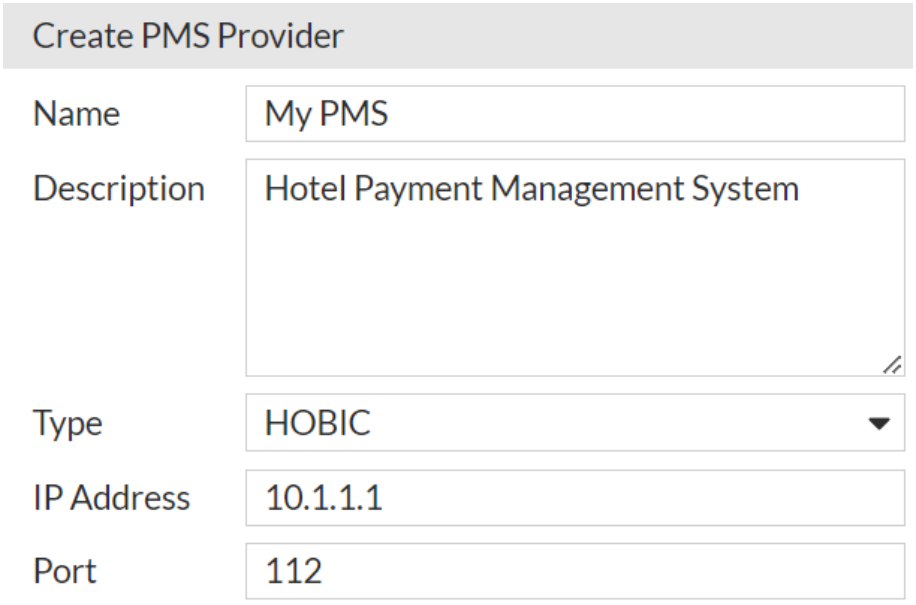
Install the certificates listed here and other configure other details, to allow secure access from FortiGuest.

- Install the following SSL certificates for *Peach Payments*.
  - *Sectigo RSA Domain Validation Secure Server CA*
  - *R3 and ISRG Root X1*
- Add the *Peach Payments* FQDNs (*oppwa.com* and *peachpayments.com*) in the allowed list of the SSID and the Firewall policy of FortiGate. Also, add the FQDNs in the **Addresses** section of **Policy and Objects** in FortiGate.
- Install the following trusted CA Certificates for *Paya*.
  - Amazon >> Subject CN
  - Amazon Root CA 1 >> Issuer CN
  - Amazon Root CA 1 >> Subject CN
  - Starfield Services Root Certificate Authority - G2 >> Issuer CN
  - Starfield Services Root Certificate Authority - G2 >> Subject
  - Starfield Services Root Certificate Authority - G2 >> Issuer
- Add the *Pay Pal* FQDNs *(*.sandbox.paypal.com* (for sandbox environments), **.paypalobjects.com*, and **.paypal.com*) in the allowed list of the SSID and the Firewall policy of FortiGate. Refer to the *Pay Pal* website for the list of URLs for live and sandbox environments.

Hotel Property Management System (PMS)

FortiGuest integrates multiple hotel PMSs to include the cost of internet access in the guest's hotel bill. This is achieved by adding the PMS login widget to a portal that communicates with the PMS.

Each portal defines it's own access plans, which determine the access time allowed and the associated cost to post to the PMS configured for that portal. The first time a user goes to the portal and supplies their credentials they are directed to a page with the available access plans. After the user selects an access plan and proceeds with the authentication process, their room is charged. The user can login without being charged until their account expires, after the account expires, the user is again directed to the page displaying the available access plans to purchase more time on the network. In the guest portal, select the configured payment provider in PMS Provider on page 99 and the Access Plans on page 99.

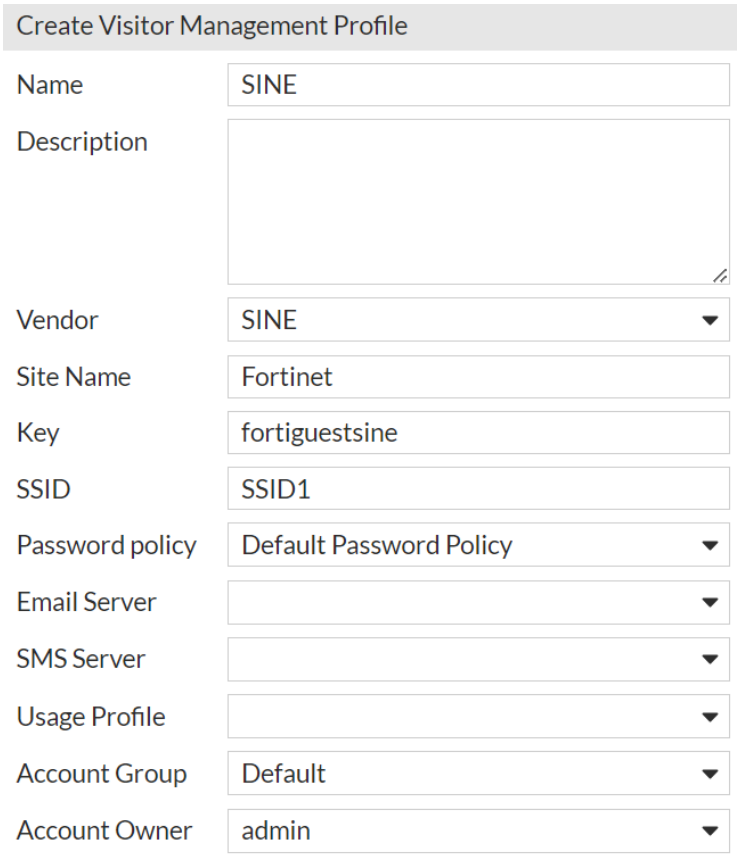


- HOBIC - Enter the **IP Address** and the **Port** number of the Hotel PMS.
- Oracle Cloud PMS - Enter the PMS **Server** IP address, unique **Hotel ID**, **Application Key**, **Client ID** and **Secret**, and your **Username** and **Password**.
- Oracle Opera - Enter the **IP Address** and the **Port** number of the Hotel PMS, also, configure the **Timeout** to establish a connection with the server.
- IDS Next - Enter the **IP Address** and the **Port** number of the Hotel PMS, also, configure the **Timeout** to establish a connection with the server.

Visitor Management

Sine is a cloud-based visitor management system that helps businesses streamline their visitor check-in process. It allows visitors to check in via the iPad or the Sine mobile app, and hosts to be notified of their arrival. Sine also offers a variety of features to improve security and compliance, such as pre-screening, geofencing, and badge printing.

After creating a site and configuring a webhook for the site, navigate to **Portal > Visitor Management** in the FortiGuest GUI to add a visitor management profile. The **Site Name** is the name of the site created in Sine and the **Key** is the the API key configured while creating the webhook integration.



Notes:

- Fortinet recommends that you have a auto-generated password policy configured in the visitor management profile.
- Ensure that **Start End** is specified as the **Account type** for the selected usage profile. See Usage Profiles.

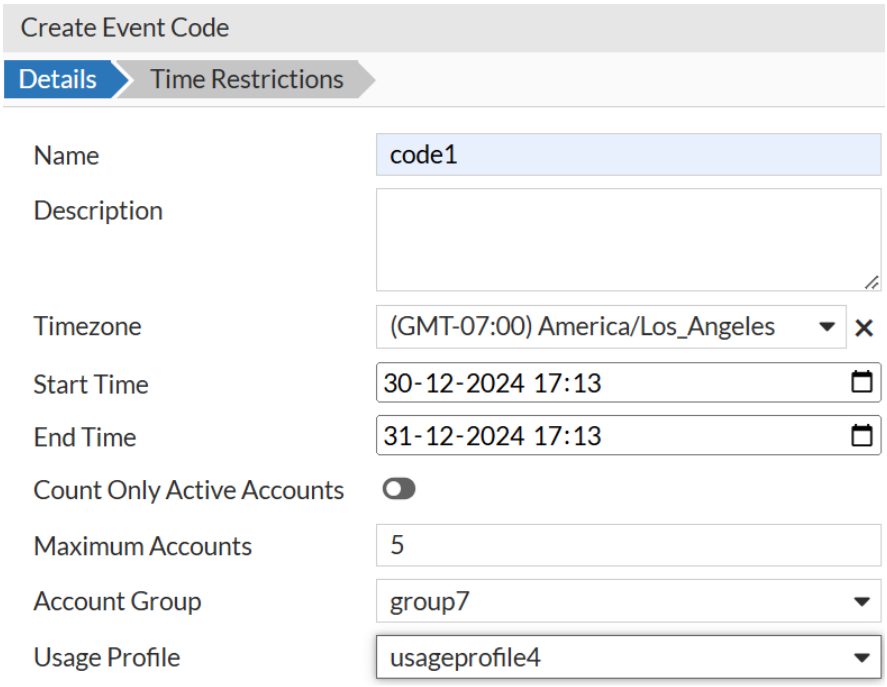
FortiGuest creates a guest user account using the details shared by Sine through webhook. You can view the guest user account populated in Creating and Managing User and Device Accounts.

- The **Status** field displays **Active** when the visitor is checked-in and **Expired** when the specified time-out period elapses.
- When the visitor checks-out, Sine sends a webhook request to FortiGuest, and FortiGuest deletes the guest user account.

Event Codes

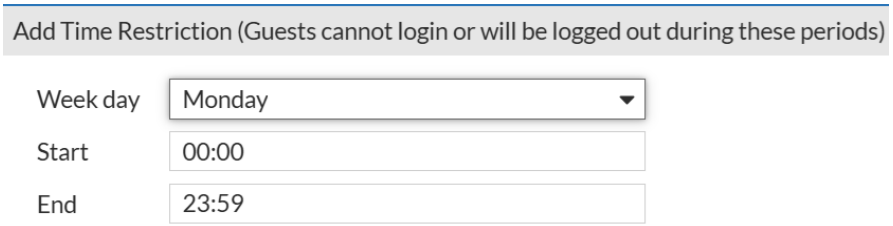
The event codes allow users to create their own accounts during specific events. The administrator generates an event code and shares it with the user to enable access to the hotspot created for a particular event and

allow registration. The codes generated are valid only for the event duration and then timeout. To generate a new event code, navigate to **Guest Portal > Event Codes**.



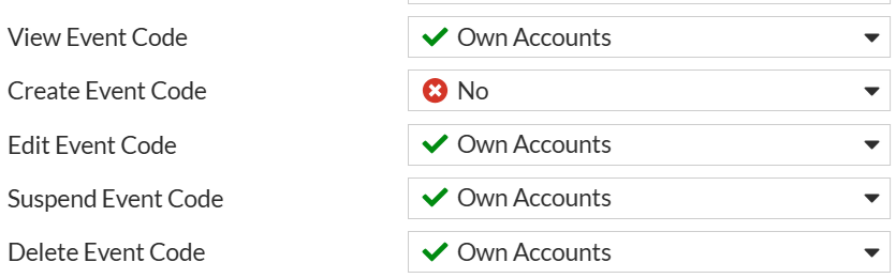
- Enter a unique code **Name** and an optional **Description**.
- Select the **Timezone** of the event.
- Select the **Start Time** and **End Time**, during which the users are able to create their own accounts. The event code will be active only for this duration.
- Enable **Count Only Active Accounts** to consider only user accounts in the **Active** state, ignoring accounts in any other state (e.g., expired, inactive, suspended).
- Enter **Maximum Accounts/Maximum Active Accounts** to restrict the maximum number of user accounts that can be created.
- Select the associated **Usage Profile** and **Account Groups** for the event codes.

In the **Time Restriction** tab, you can restrict users from creating their accounts for a certain duration.

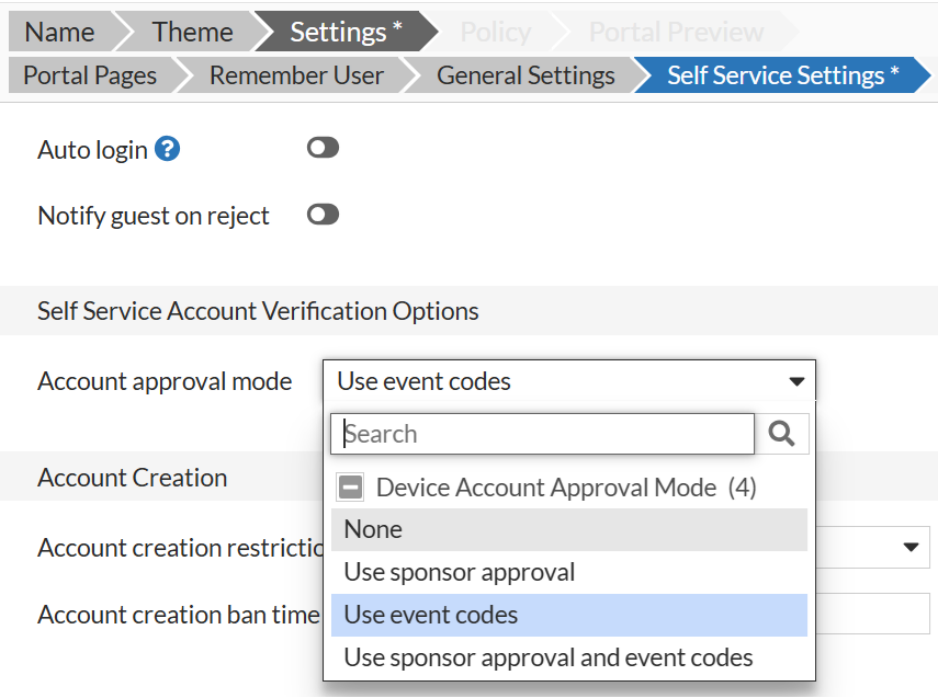


You can edit, delete, or suspend the listed event codes.

The administrator can set the permissions for sponsors to manage specific operations for the event codes in the **Access Management > Admin Groups** page.



After creating the event code, navigate to **Guest Portal** and enable the **Self Service** page (**Enabled pre-auth**). Set the **Account approval mode** for the gust portal in the **Self Service Settings** to **Use Event Codes** or **Use sponsor approval and event codes**.



Smart Connect

In large secure wireless enterprise networks configuring and managing an enormous number of secure clients to operate in a desired manner is a challenge. Smart Connect uses FortiGuest's built-in database and infrastructure to automatically configure both wireless and wired client devices, categorized as different device types and requiring different wireless settings. This avoids manual configuration of a large number of devices. Smart Connect supports iOS, Chrome, Android, macOS, Windows, Linux, and wired networks.

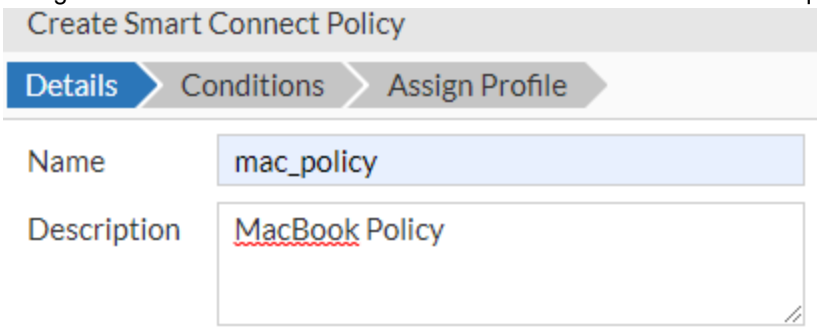
Smart Connect has the ability to configure wireless profiles and ensure that users are provisioned and connected to the secure network across a range of laptops, phones, and tablets. Smart Connect allows you to define a set of rules known as a *Smart Connect Policy*. This policy defines which *Smart Connect Profile* is applied to each user. After a user is authenticated and authorized, FortiGuest applies the Smart Connect policy rules on that user, to find the appropriate Smart Connect profile to connect to the network.

Note: New version of Smart Connect application is now available in the app stores (version 1.8.2 for Android and 2.0 for Windows). This new version of the app must be used with FortiGuest as it has an important security enhancement. Older versions of Smart Connect app will no longer work with FortiGuest 2.0.0 onwards.

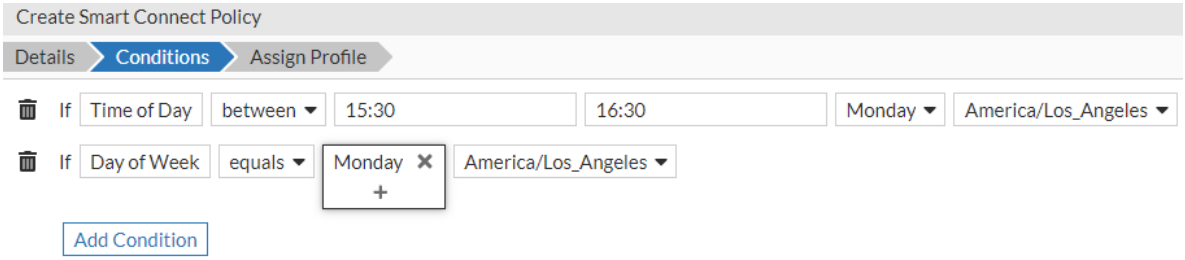
Smart Connect Policies

Smart Connect allows you to create and apply different policies to a device based on the device type classification. Smart Connect allows your wireless settings to be automatically configured to securely connect you to a wireless network. It allows you to download a profile from a network that uses Smart Connect and define a set of rules known as a *Smart Connect Policy*. You can **Clone** the policy to reuse configurations.

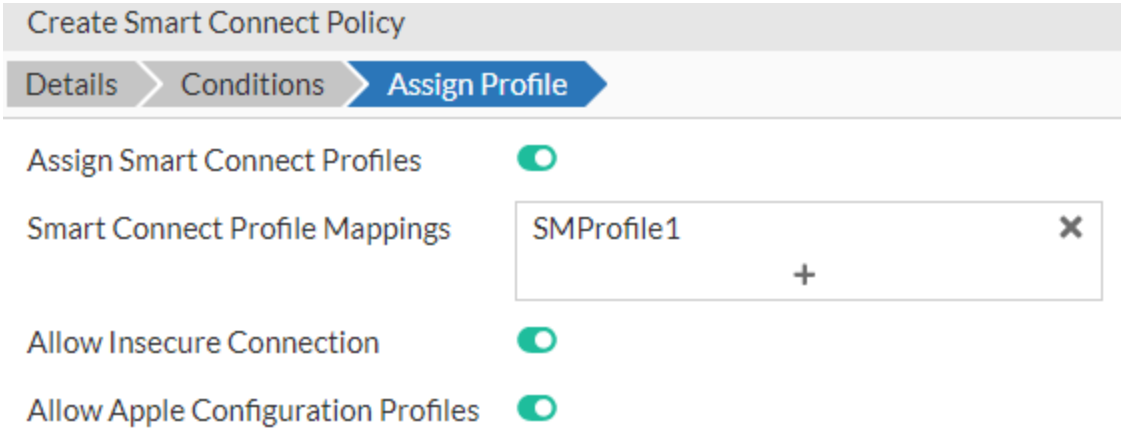
1. Navigate to **Smart Connect > Smart Connect Policies** and enter a unique policy name.



2. You can add **Conditions** to your policy by adding attributes. To add more conditions click **Add Condition** and select the appropriate attribute from the drop down menu.



3. Select the Smart Connect profiles that you want to assign to users that match the rule you have created. Enable **Allow Insecure Connection** to enable users to continue using open networks instead of running Smart Connect when they authenticate as per your requirement. Optionally, you can enable/disable **Use Apple Configuration Profiles** for Apple devices.



After a user is authenticated and authorized, FortiGuest applies the Smart Connect policy rules on that user, to find the appropriate Smart Connect profile to connect to the network.

Smart Connect Profiles

Create a Smart Connect profile defining your network type and authentication settings for client in your network. You can **Clone** the profile to re-use configurations.

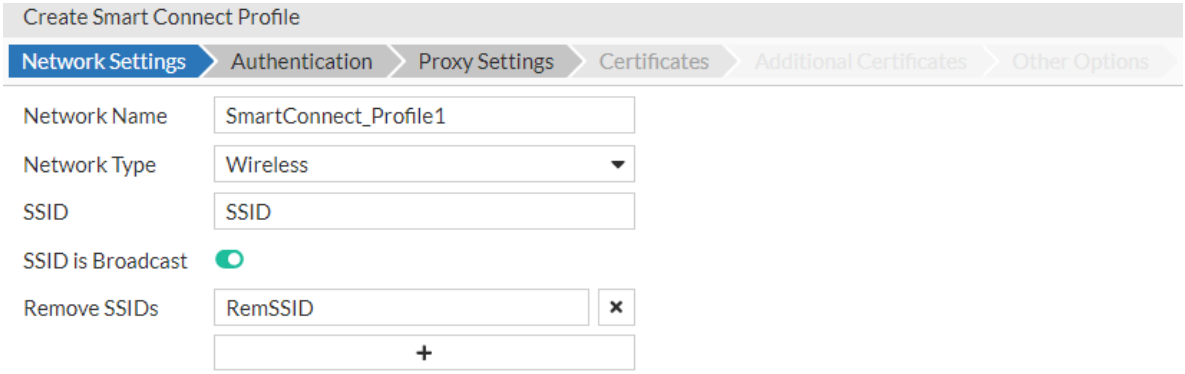
Note: Smart Connect on Linux supports only Ubuntu versions 20, 22, and 24.

This table describes the EAP types supported for Smart Connect on different platforms.

Platform	PSK	EAP MSCHAPV2	EAPGTC	EAP TLS Local certificate authority	EAP TLS with SCEP server
Windows	Supported	Supported	Not Supported	Supported	Supported
Android	Supported	Supported	Supported	Supported	Supported

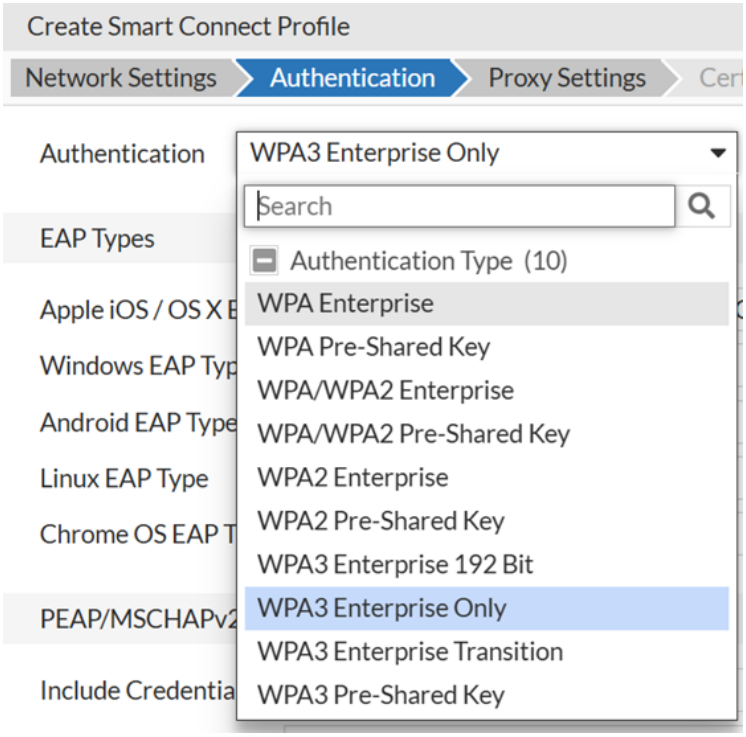
Platform	PSK	EAP MSCHAPV2	EAPGTC	EAP TLS Local certificate authority	EAP TLS with SCEP server
iOS	Supported	Not Supported	Supported	Not Supported	Supported
Wired network	Not Supported	Supported	Not Supported	Supported	Supported

1. Navigate to **Smart Connect > Smart Connect Profiles** and click **New**.
2. In the **Network Settings**, enter a unique **Network Name** (for your network) and select the **Network Type** (only **Wireless** is supported in this release).
3. Enter the **SSID** name and enable **SSID is Broadcast** as per requirement.
4. Optionally, you can specify the SSIDs you wish to remove from the client. This is required for any open network where client access is restricted.

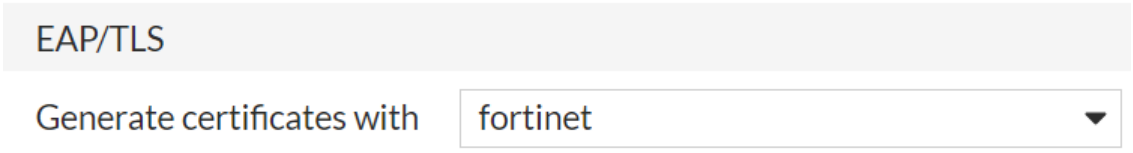


5. In the **Authentication** tab, you are provided the authentication methods based on the network type that you specify. FortiGuest supports WPA, WPA2 Enterprise, and WPA3 Enterprise authentication modes. For the **Pre-Shared Key** authentication methods, enter the **Pre-Shared Key**. For more information on WPA3

Enterprise authentication modes, see WPA3-Enterprise Support for SmartConnect.

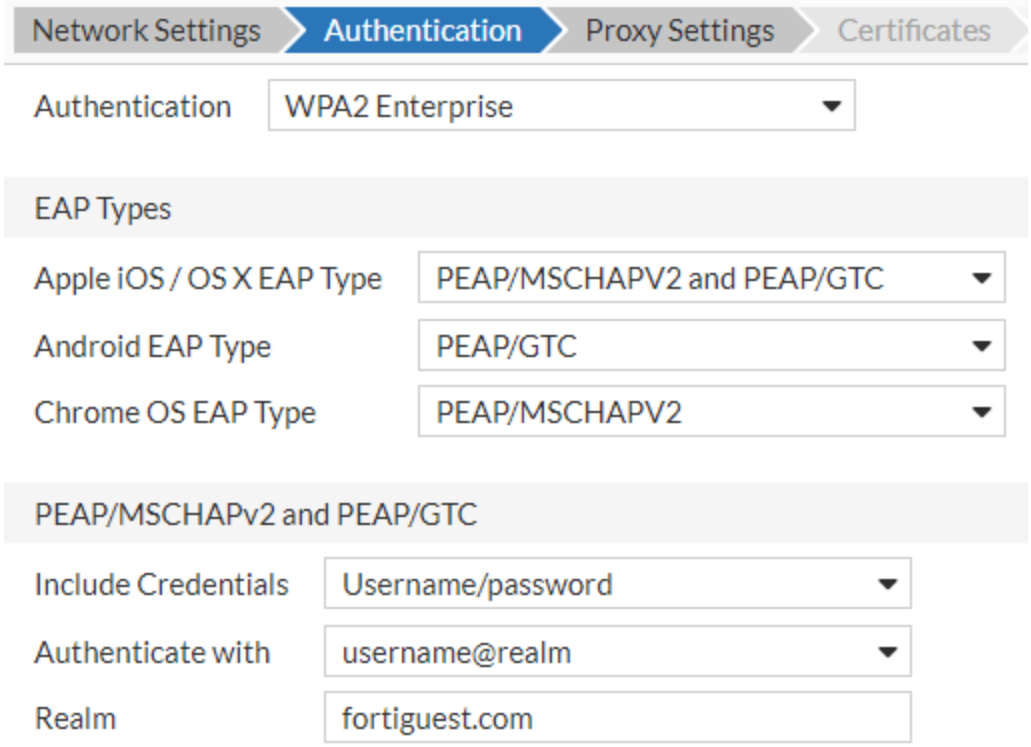


6. For the **Enterprise** authentication methods, enter the following.
   - **EAP Types** - Select an EAP type for authentication for different client devices, Apple, Android, Windows, Linux, and Chrome.
   - **EAP/TLS** (**Generate certificates with**) - If you select the EAP-TLS for authentication, then select the certificate provider. See SCEP Servers.

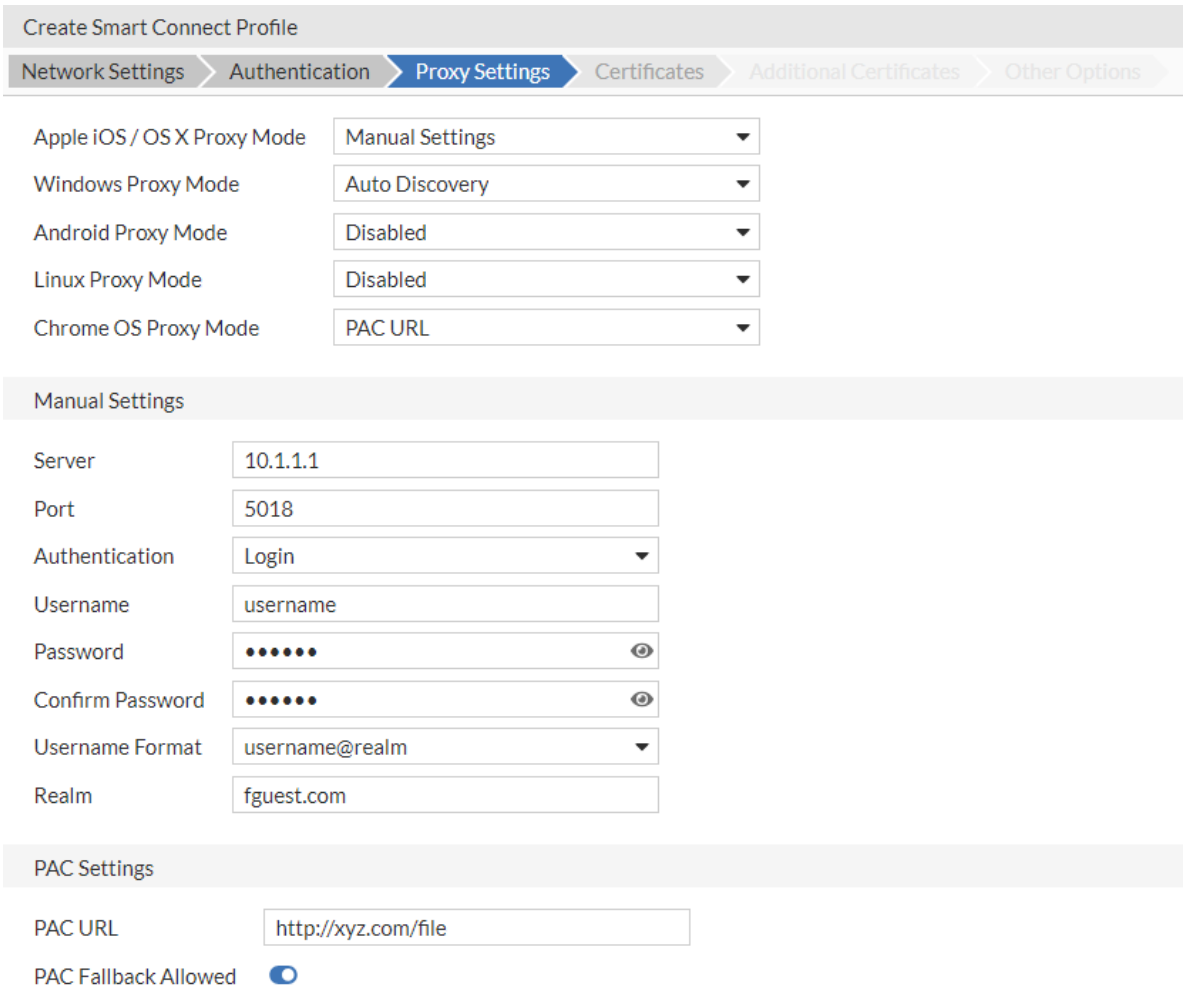


   - **PEAP/MSCHAPv2 and PEAP/GTC** - Determine in the **Include Credentials** field whether you want to include or not include the user name and password in the profile sent to the user. Select a specific user

name format for the client to **Authenticate with**. If you select realm, then define the **Realm**.

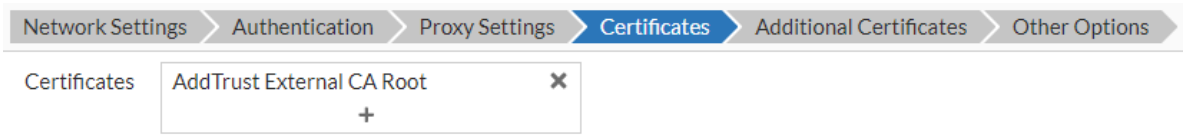


7. In the **Proxy Settings** tab, configure the proxy server settings for the client. You can configure any of the following options for **Apple iOS / OS X Proxy Mode**, **Windows Proxy Mode**, **Android Proxy Mode**, **Linux Proxy Mode**, and **Chrome OS Proxy Mode**.

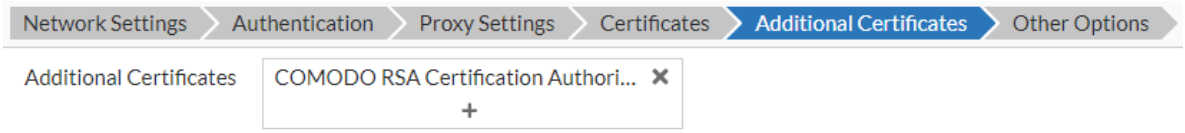


- **Disabled** - To disable the proxy mode for clients.
- **Auto Discovery** - To enable the automatic discovery of proxy settings.
- **Manual Settings** - Update the following proxy server settings.
  - **Server** - Enter your server's hostname or IP address.
  - **Port** - Enter the appropriate port number.
  - **Authentication** - Select whether no authentication is needed or whether a login is required. If a login is required then update the following.
  - **Username** - Enter the username for authentication.
  - **Password** - Enter and confirm the authentication password.
  - **Username Format** - Select a format to use for the authentication username.
- **PAC URL** - Update the following proxy auto-config (PAC) settings.
  - **PAC URL** - The URL of the PAC file that defines the proxy configuration.
  - **PAC Fallback Allowed** - When disabled the device is prevented from connecting directly to the destination if the PAC file is unreachable. This is enabled by default.

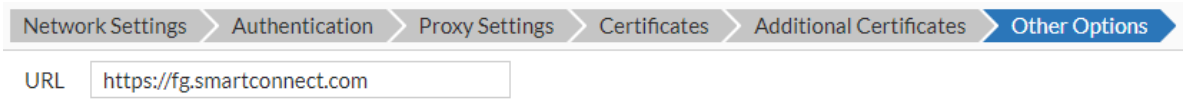
8. You can select any pre-installed **Certificates** that you require. Configure the certificates only if you are using the Enterprise authentication methods.



9. You can also install any additional CA certificates.



10. In the **Other Options** tab, enter the URL you wish to direct the browser to once connected, after Smart Connect has run.
Note: This does not apply to Apple devices configured using an Apple configuration profile.



SCEP Servers

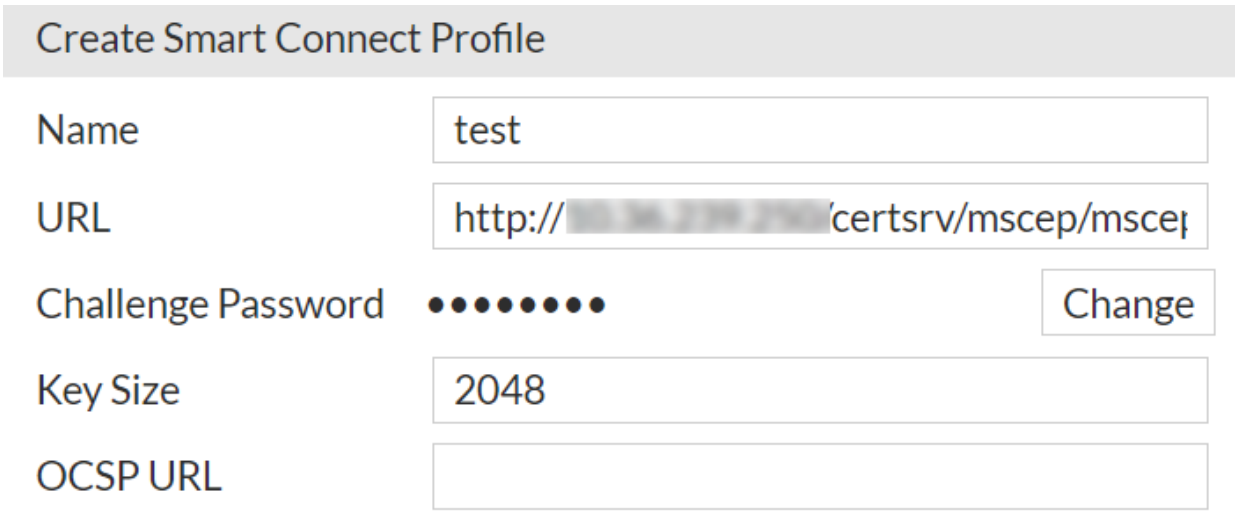
FortiGuest allows distribution of certificates to devices when they are authenticated onto the network. This is achieved in the following methods.

- You can generate user certificates on an external server like MS Active Directory and then add an entry in **Smart Connect > SCEP Servers**. When using SCEP for certificate generation, FortiGuest handles both revoked certificates with and without new replacements.
- You can also generate certificates internally on the FortiGuest in **System > Certificates > Local Certificate Authorities**.
- You can manually upload certificates while configuring the authentication policy. See RadSec Authentication.

When a network user requests a Smart Connect profile, then a user certificate is generated, this is achieved by selecting EAP-TLS as an EAP type in a Smart Connect profile. You can add an SCEP Server and generate certificates internally using the Local Certificate authorities. See Certificates.

Adding the SCEP Server

Navigate to **Smart Connect > SCEP Servers** and configure the following parameters to add an SCEP server.



1. Enter the **Name** of the SCEP Server.
2. Enter the **URL** of the SCEP Server (HTTP only)
3. Enter a **Challenge Password** that is required when connecting to NDES on a Windows server. If the password is not specified then the user's current password is used when generating the client certificate.
4. Enter the **Key Size**.
5. Enter the **OCSP URL** to send an OCSP request for validating user certificates when authenticating.

WPA3-Enterprise Support for SmartConnect

This release supports the robust WPA3 Enterprise authentication modes in Smart Connect profiles, enabling secure 6GHz wireless LAN deployments that require WPA3. This enforces enhanced encryption protocols with highest security standards for enterprise-grade wireless networks.

WPA3 Enterprise authentication modes are supported on devices running the following operating systems.

- Windows
- Android
- iOS
- macOS
- Linux
- ChromeOS

Navigate to **Smart Connect > Smart Connect Profiles** and you can select the WPA3 Enterprise authentication modes.For WPA3, you can select the following modes.

- WPA3 Enterprise Only
- WPA3 Enterprise Transition to allow for a smoother transition from WPA2 to WPA3, ensuring devices that do not support WPA3 can still connect securely.
- WPA3 Enterprise 192 Bit, a specialized mode of WPA3 Enterprise offering advanced security with 192-bit encryption strength. WPA3 Enterprise 192-bit mode is supported with *ECDSA* or *RSA* keys (with a minimum key size of 3072 bits). Administrators can select the desired key type and size when generating the local certificate. See Certificates.

Operating System	WPA3 Enterprise Only	WPA3 Enterprise Transition	WPA3 192 Bit
Android 11/12/13/14	Supported	Supported	Not Supported
macOS	Supported	Supported	Supported
iOS	Supported	Supported	Supported
Windows 10	Not Supported	Not Supported	Supported
Windows 11	Supported	Supported	Supported
Linux 20.04	Supported	Supported	Not Supported
Linux 22.04/24.04	Supported	Supported	Supported
ChromeOS	Supported	Supported	Not Supported

WPA3 Enterprise 192-bit security is not supported on Android and ChromeOS devices.

Managing Devices

You can configure a RADIUS client to authenticate users and configure user account notifications. When a user account is created, the details of the account need to be passed from the sponsor to the user, these notifications can be sent over emails or SMS text messages. SMS text message notification require email servers to be configured, but can be configured based upon policy.

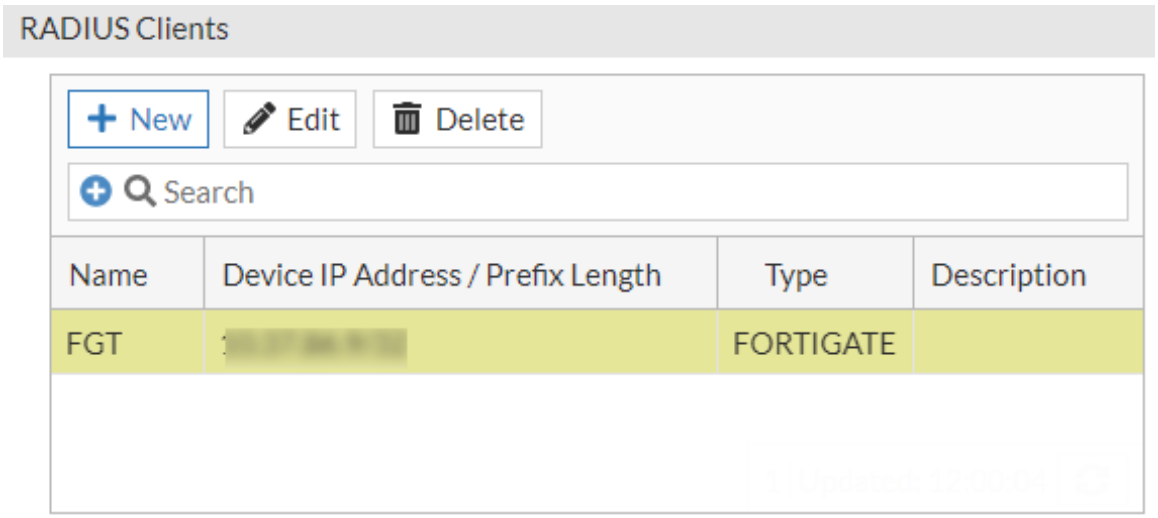
RADIUS Clients

FortiGuest uses the RADIUS protocol to authenticate and audit users who log in through RADIUS capable network enforcement devices. When a user authenticates against a RADIUS client, then that client performs an authentication check with FortiGuest, to validate whether the credentials supplied by the user/device are valid. If the authentication is successful, FortiGuest returns a message stating that the user is valid and the duration of time remaining before the user session expires. The RADIUS client must honour the session-timeout attribute to remove the user when the account time expires (unless the account is unlimited).

Notes:

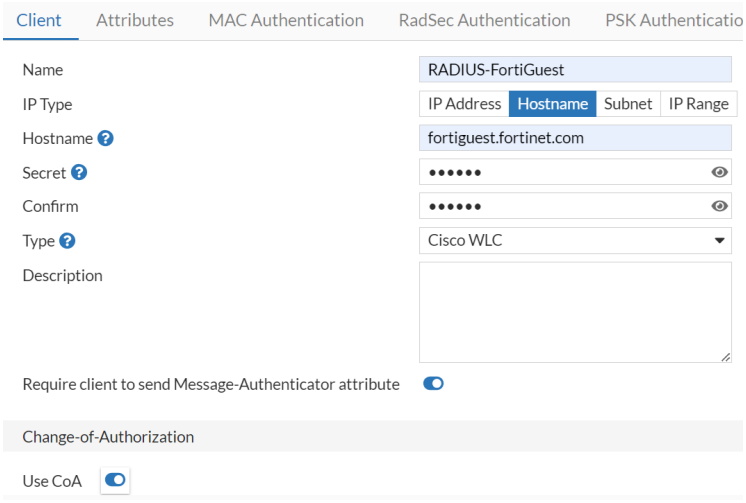
- Ensure that the FortiGate controller is specifically configured to allow AAA override. This enables it to honour the session-timeout attribute returned to it by FortiGuest.
- If there is a firewall between FortiGuest and the RADIUS client , then allow traffic to pass from the UDP port 1812 or 1645 (RADIUS authentication) and UDP port 1813 or 1646 (RADIUS accounting).

In addition to authentication, the RADIUS client device reports details to FortiGuest, such as the time the session started, time session ended, user IP address, and so on. This information is transported over the RADIUS accounting protocol.



The **RADIUS Debug** option turns the RADIUS server on in debugging mode, enabling detailed debug information to be viewed in **System Logs**. Perform the following steps to add a RADIUS client.

1. Navigate to **Devices > RADIUS Clients** and click **New** in the **RADIUS Clients** section.



2. Update the **Client** tab with the following configurations.
   - **Name** - Enter a unique name of the RADIUS client.
   - **IP Type** - Type the **Device IP Address / Prefix Length** of the RADIUS client, if you do not know the prefix length, then FortiGuest automatically selects this. This needs to match the IP address from which the RADIUS request originates. You can also configure the hostname/FQDN or the IP range when adding a RADIUS client in FortiGuest, select options options **Hostname** and **IP Range**. The IP range can be specified with a hyphen, for example, *1.10.1.1 – 1.10.1.15*.

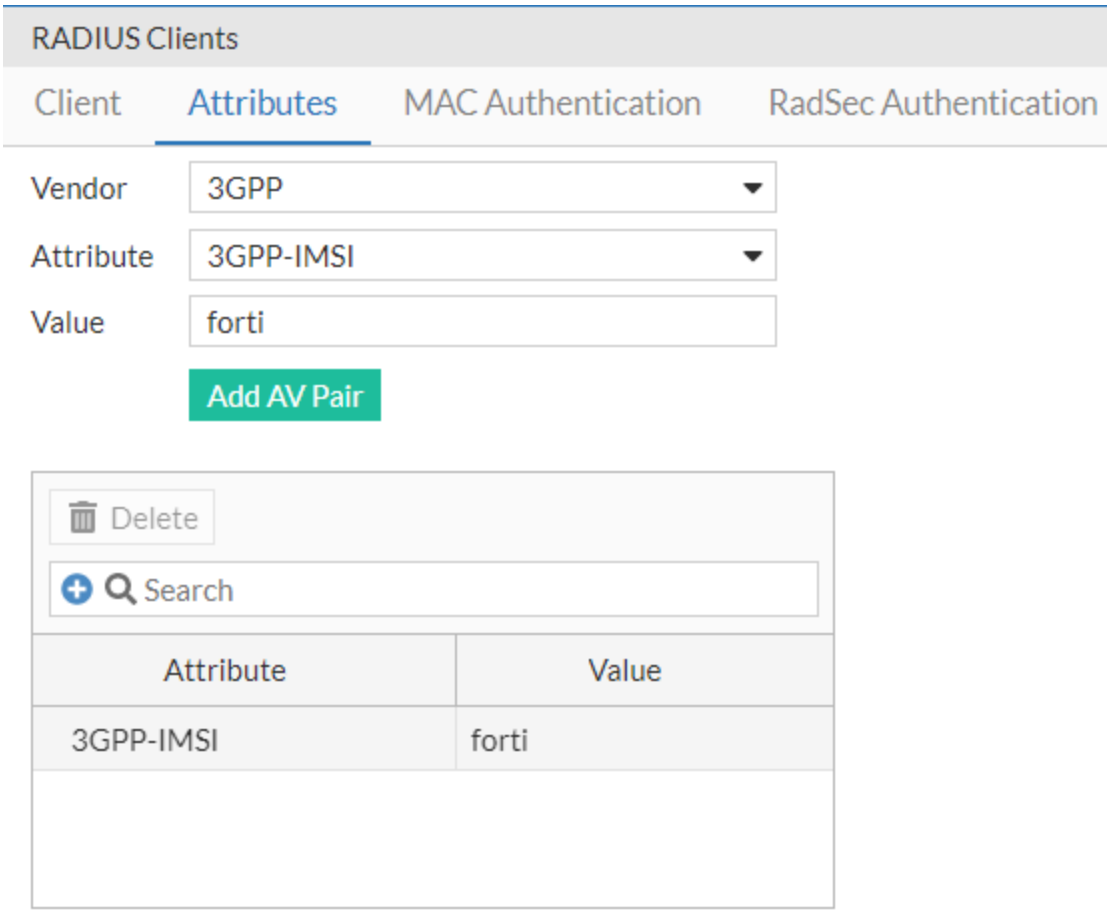
- **Secret** - A shared secret for the RADIUS client. Re-type the shared secret in the **Confirm** field.
- **Type** - Select the type or vendor of the RADIUS client. The supported vendor types are **Aruba Controller**, **Cisco WLC** (captive portal and 802.1x authentication), **FortiGate**, **FortiWLC**, **Generic RADIUS Device**, **Meraki**, **Ruckus Controller**, and **FortiLAN Cloud**. See Adding FortiGate as a RADIUS Client.
- **Description** - Enter a description of the client and any other information needed.
- **Message-Authenticator attribute** - You can enable/disable sending the message authenticator attribute to the server when configuring the RADIUS client. This option is disabled by default.
  Notes:
  - If this option is disabled, then FortiGuest processes RADIUS request packets with/without the message-authenticator attribute.
  - If this option is enabled, then FortiGuest drops RADIUS request packets without the message-authenticator attribute in them.
- **Change-of-Authorization** - Enable this field to use CoA and enter the port to use. Enable proxy CoA if required.

Update the following subsequent tabs to complete the configuration of a RADIUS client.

- Attributes
- MAC Authentication
- RadSec Authentication
- Guest Portal

Attributes

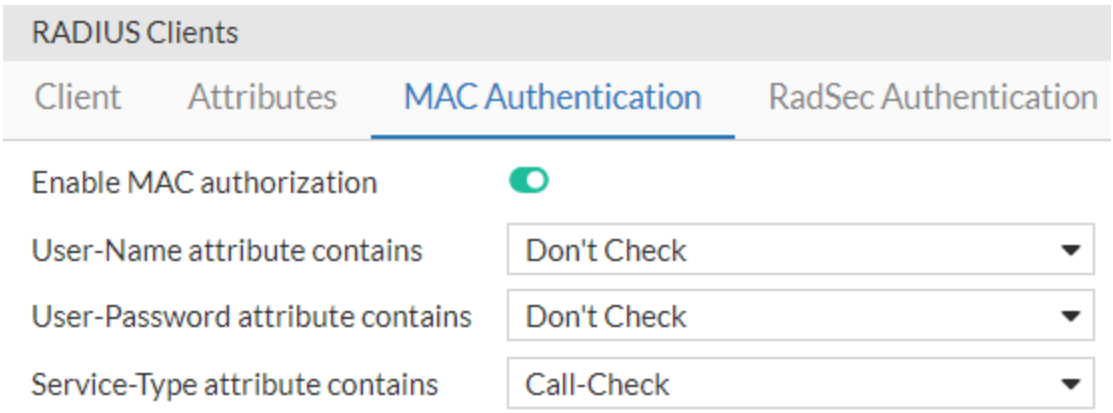
Update the **Attributes** tab to enable the RADIUS client to send any additional attributes upon successful authentication.



- **Vendors** - Select from the list of pre-defined vendors.
- **Attributes** - Select from the list of pre-defined attributes based on the selected vendor.
- **Value** - Enter the appropriate value for the selected attribute.
- **Add AV Pair** - Click to add the specified attribute-value pair.

MAC Authentication

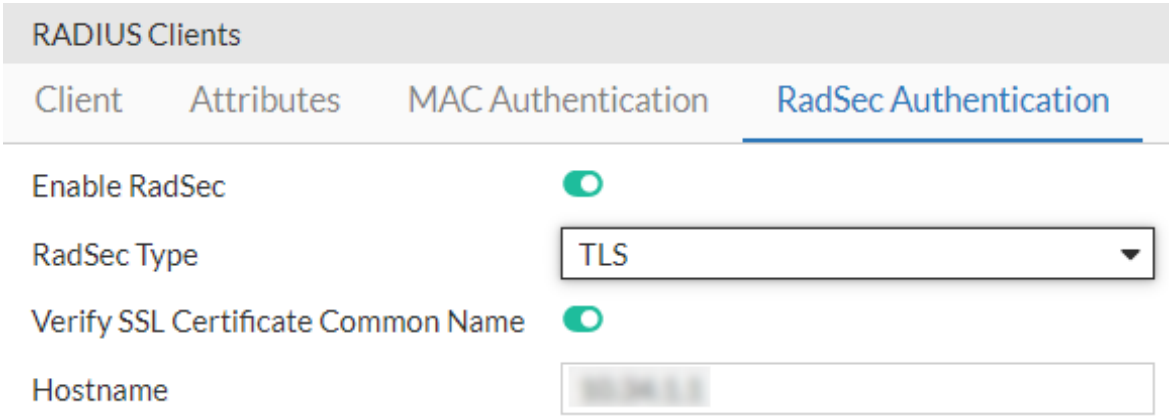
Update the **MAC Authentication** tab to setup and enable MAC address based authentication for user devices. Enable **MAC authorization** and configure the following parameters.



- **User-Name attribute contains** - Select whether the user name attribute contains the *Client MAC Address*, *Shared Secret*, whether it is *Not Present*, or *Don't Check*.
- **User-Password attribute contains** - Select whether the password attribute contains the *Client MAC Address*, *Shared Secret*, whether it is *Not Present*, or *Don't Check*.
- **Service-Type attribute contains** - Select whether the service type attribute contains the *Login-User*, *Framed-User*, *Call-Check*, whether it is *Not Present*, or *Don't Check*.

RadSec Authentication

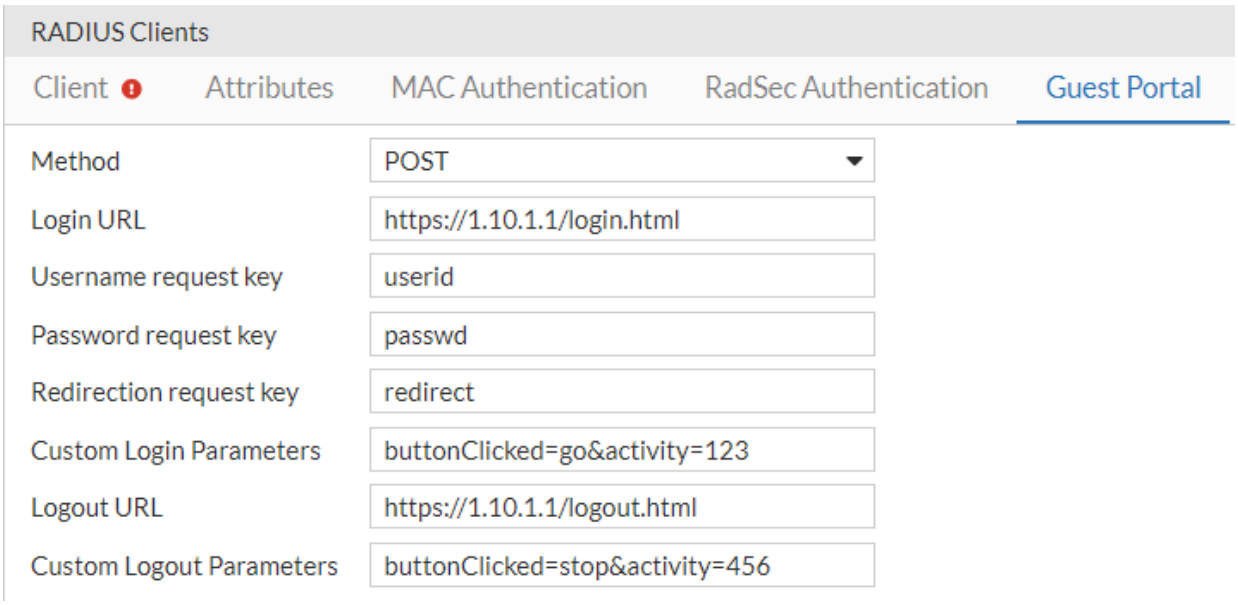
Update **RadSec Authentication** to secure communication between RADIUS/TCP peers on the transport layer. This is particularly useful in roaming environments where RADIUS packets are transferred through different administrative domains and untrusted, potentially hostile networks.



- Select the **RadSec Type**, *TLS* or *DTLS*.
- To enable verification, select **Verify SSL Certificate Common Name**.
- Enter the RADIUS client **Hostname**.

Guest Portal

Update the **Guest Portal** tab to allow a generic RADIUS client to interface with a portal by providing login/logout parameters and request keys.



- **Method** - Select the HTTP method with which forms are submitted to the generic RADIUS device.
- **Login URL** - Enter the URL used to login users to the device.
- **Username request key** - Enter the username key, this normally corresponds to the name of the HTML element that takes the username.
- **Password request key** - Enter the password key.
- **Redirection request key** - Enter the redirect key.
- **Custom Login Parameters** - Enter any custom login parameters the device may require.
- **Logout URL** - Enter the URL used to log out users on the device.
- **Custom Logout Parameters** - Enter any custom logout parameters the device may require.

Note: FortiGuestsupports TLS, PAP, CHAP, PEAP-MSCHAPv2 and PEAP-GTC in RADIUS Authentication.

Adding FortiGate as a RADIUS Client

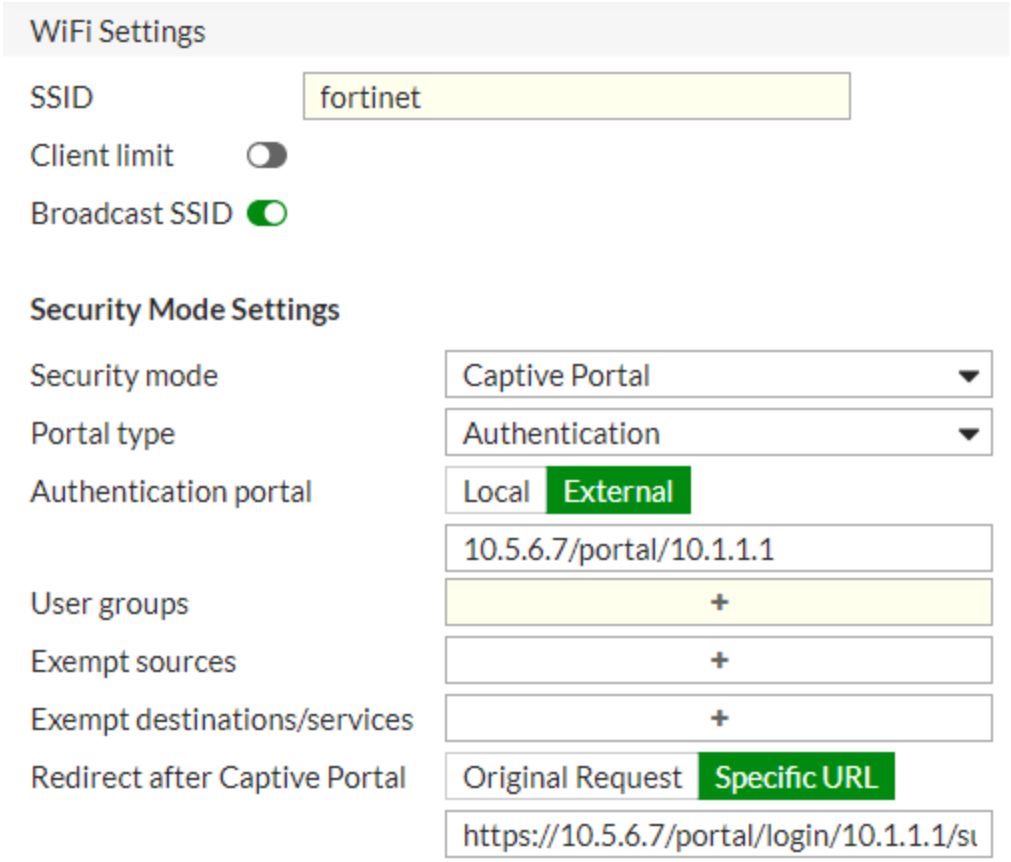
You can add Fortigate as a RADIUS client with the following limitations.

- Device authentication feature does not work as FortiGate does not send the NAS IP address/*Called-Station-Id* parameters.
- OAuth feature is supported if the required host names are in the allowed list on FortiGate. This enables client redirection to the OAuth provider site for authentication.
- As FortiGate does not send the AP name and AP ID, some guest reports and accounting logs have empty fields against them.
- Redirection URL after successful guest authentication must be set in FortiGate configuration.

In the **Attributes** tab (Attributes), add the *Acct-Interim-Interval* = <*nnn*> (between 600 - 86400 seconds) entry.

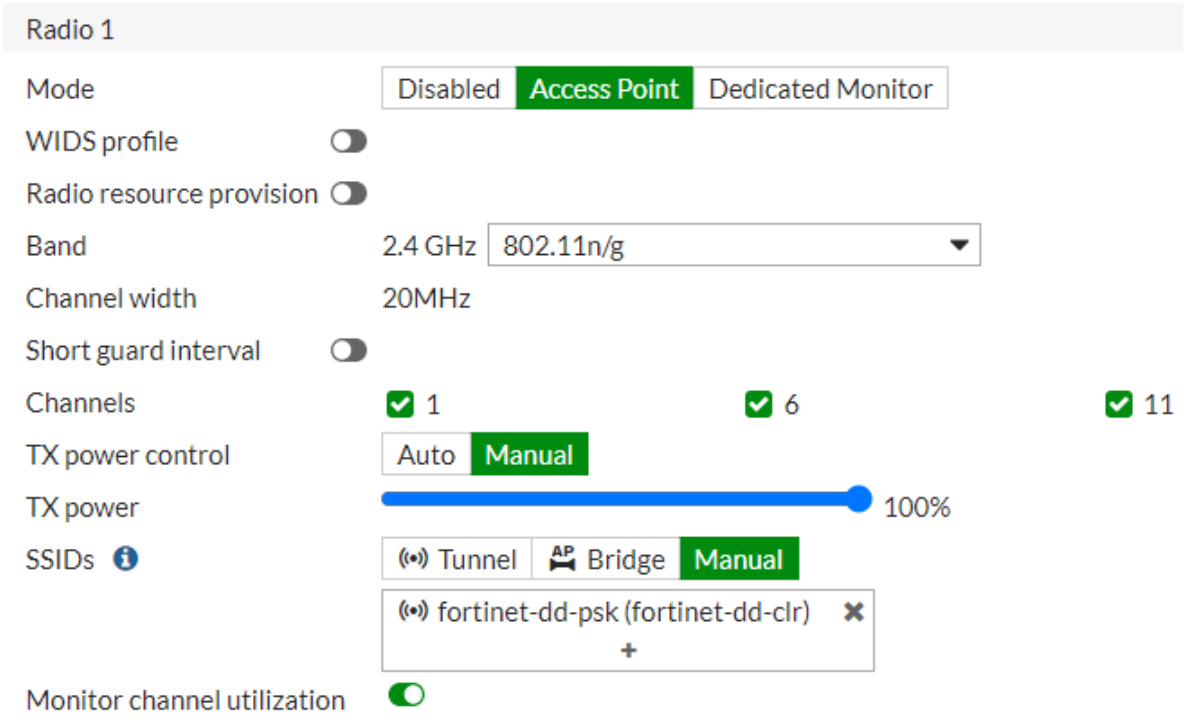
Perform the following steps in the FortiGate GUI to complete RADIUS client configurations.

1. Navigate to **WiFi and Switch Controller > SSIDs** and click **Create New**. Ensure the following configurations.

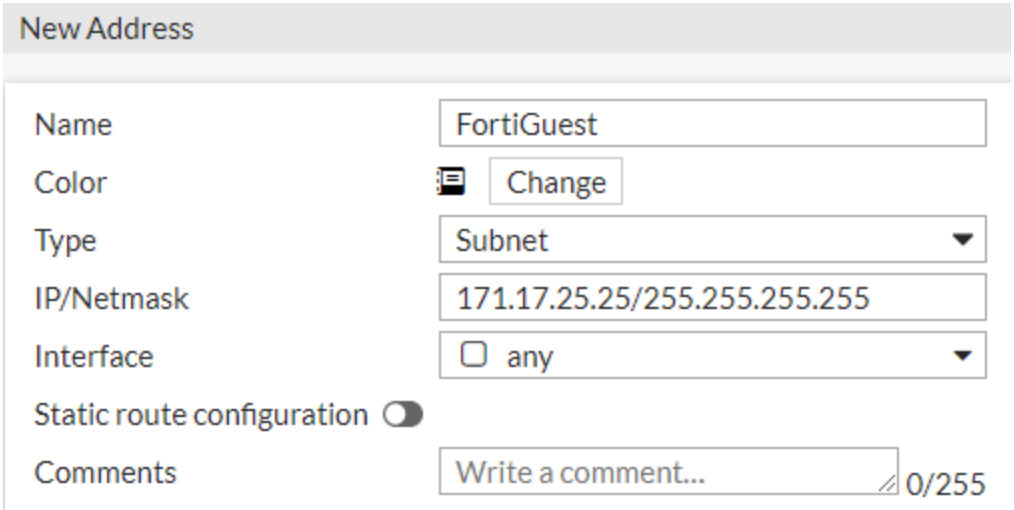


- **Security mode** is **Captive Portal**.
- **Portal type** is **Authentication**.
- Enter the **Authentication portal** address in this format, *<FortiGuestserverIP>/portal/FortiGate-serverIP>*.
- Provide a destination URL (`{FortiGuest_IP or FQDN}/cp/portal/v1/cp/success`) to **Redirect after Captive Portal** authentication.

2. Navigate to **WiFi and Switch Controller > FortiAP Profiles** and create or edit a profile. In the profile, set the SSID of each radio to the SSID created in the previous step.

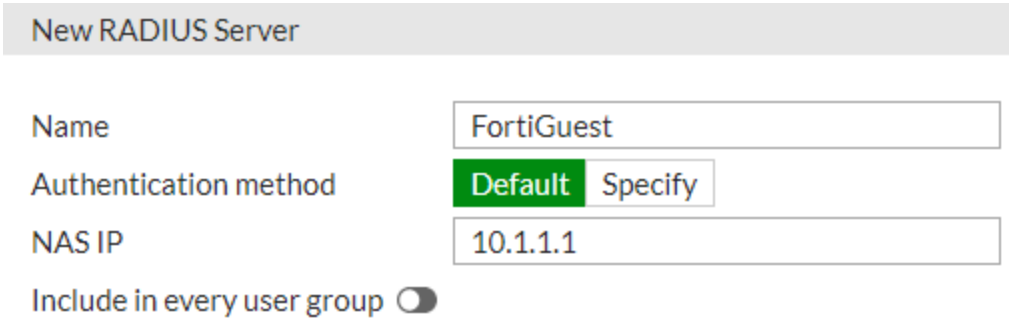


3. Navigate to **Policy and Objects > Addresses** and create a new entry with the FortiGuest server and its IP address.



4. Navigate to **User & Authentication > RADIUS Servers** and create a new entry for the FortiGuest server. The secret key entered here is used while adding the FortiGate server in FortiGuest. Ensure that you enter

the FortiGate server IP address as the **NAS IP**.

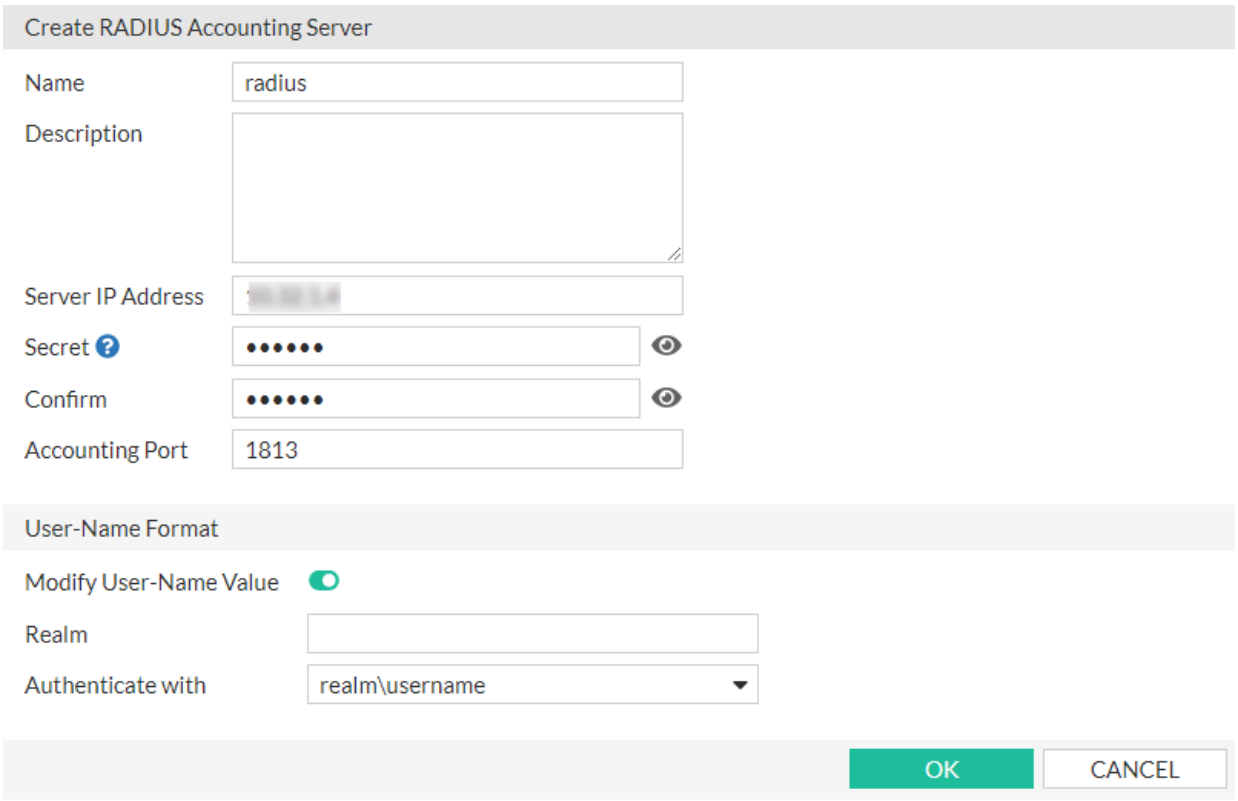


5. Run the following commands in the FortiGuest CLI to complete the integration of FortiGate.
   - Allow external web access - `# set captive portal exempt enable`
   - Configure accounting time interval - `# set acct-interim-interval [duration] (between 600 - 86400 seconds]`
   - Configure FortiGuest as the RADIUS accounting server.

     ```
     # config accounting-server
     # edit 1
     # set status enable
     # set server <IP Address of FortiGuest>
     # Set secret <Secret>
     ```

RADIUS Accounting Server

FortiGuest can replicate and forward any accounting packets to an admin defined server. Perform the following steps to add a RADIUS accounting server to forward the accounting packets to.

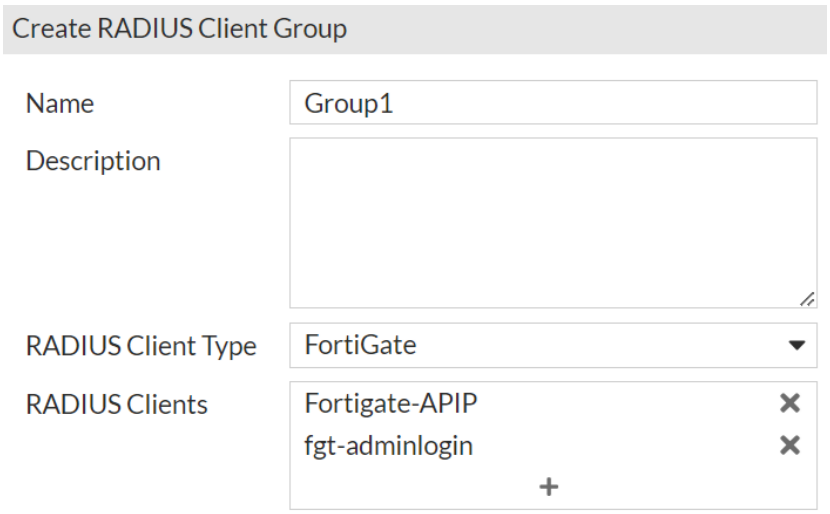


1. Navigate to **Devices > RADIUS Accounting Servers** and click **New**.
2. Enter the **Name** and **Description** of the RADIUS accounting server.
   - **Server IP Address** - The IP Address of the RADIUS accounting server
   - **Secret** - The shared secret of the RADIUS accounting server
   - **Confirm** - Confirm the shared secret.
   - **Accounting Port** - The accounting port used by the server.

You can modify the **User-Name** value of your server, enter the **Realm** details and select the format to **Authenticate with**.

RADIUS Client Group

Navigate to **Devices > RADIUS Client Groups** and group RADIUS clients of the same type. Select the **RADIUS Client Type** and add **RADIUS Clients** that belong to the selected type.


Create RADIUS Client Group
Name
Group1
Description
RADIUS Client Type
FortiGate
RADIUS Clients
Fortigate-APIP
fgt-adminlogin

MPSK Authentication

The Multiple Pre-Shared Key (MPSK) authentication feature facilitates the use of PSKs for guest portals to provide controlled and secure visitor access to the network resources. FortiGuest supports multiple PSKs simultaneously on a single SSID, each device uses a unique PSK to connect to the network. The guest users are prompted to enter the PSK via the captive portal page to connect to the network. This simplifies the on-boarding experience for users by granting them easy network access. This also allows the administrators to effectively track network usage.

Note: Administrators and sponsors can create MPSK profiles.

Just like the existing MAC authentication feature, PSK authentication can also be configured individually for a RADIUS client. FortiGuest assigns PSKs to devices through RADIUS clients, the FortiGate controller then leverages both MAC authentication and PSKs to authenticate devices for network access. The PSKs are not stored on the FortiGate and are returned as RADIUS attributes.

You can perform the following operations to use PSK authentication for guest portals.

- Create an MPSK password policy that defines the PSK complexity requirements for users logging in into the guest portal. This policy is tagged to the guest portal. See MPSK Password Policy.
- The administrator can create PSKs and tag them to user accounts and devices. On successful guest portal authentication, the guests can use the administrator created PSK or can create their own. See Creating PSKs.
- The guest user logging in into the guest portal with no devices tagged can register their device. See Guest Portal Device Registration.
- Both static and dynamic VLAN mapping is supported. Static VLAN mapping is available to the administrator per PSK, dynamic VLAN mapping is available when a PSK is authenticating via a RADIUS client. See VLAN Mapping.
- Enable MPSK and tag a password policy when configuring the guest portal in FortiGuest. See Guest Portal Configurations.
- To use FortiGuest MPSK feature specific configurations are required on FortiGate. See FortiGate Configurations.

Limitations

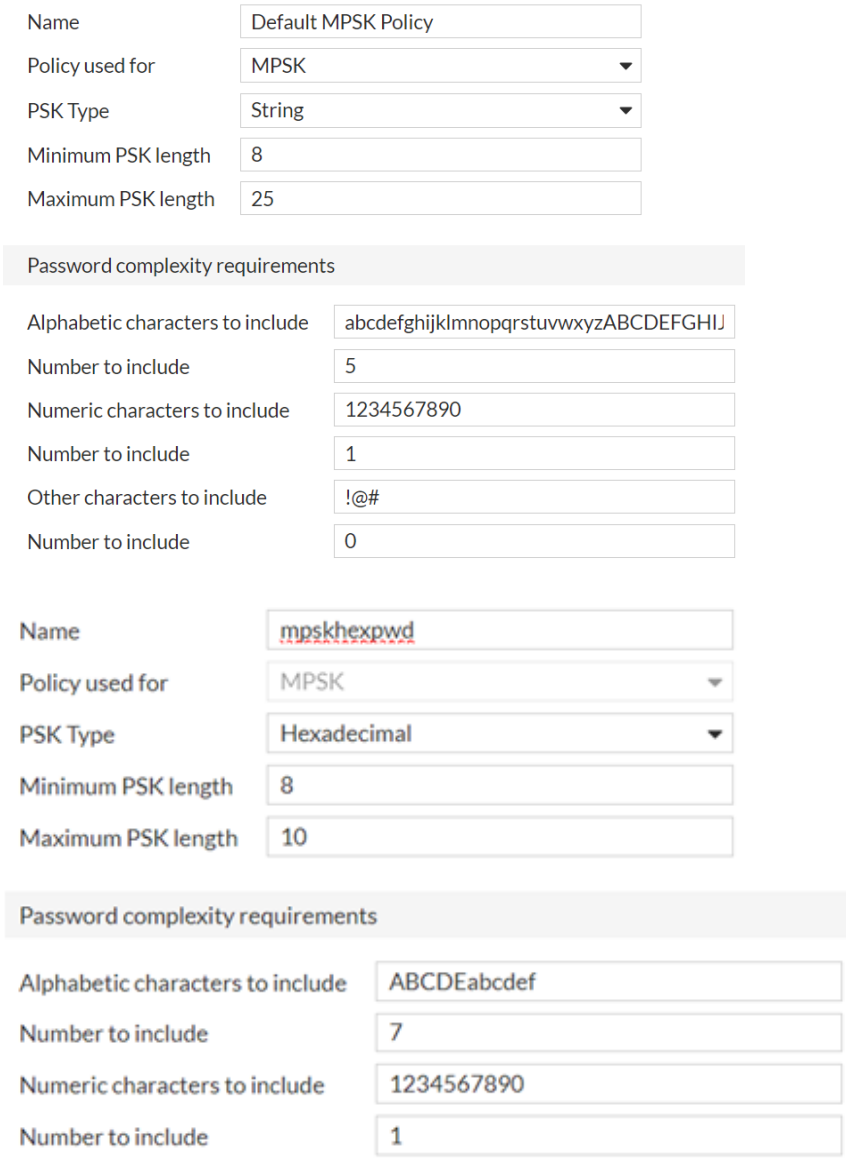
The following limitations apply to the usage of this feature.

- For iOS devices the CNA must be disabled.
- Dynamic VLAN assignment per user is not supported.

MPSK Password Policy

You can create an MPSK password policy similar to a user account password policy to define complexity requirements. The admin can create multiple password policies and a specific password policy is selected and tagged to a guest portal. This tagged policy is then applied to the PSKs that the guests logging in into the portal create. A default password policy exists for MPSK, you can also mark any password policy as default, which

then applies to all the PSKs created in the FortiGuest admin portal. The MPSK password policy is created in **Policy Settings > Password Policy** along with user account password policy.



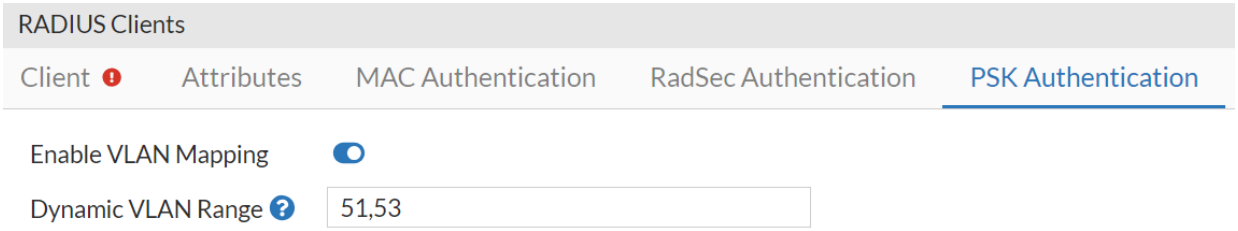
1. Ensure to select **MPSK** in the **Policy used for** field.
2. Select the **PSK Type** as **Hexadecimal** (a maximum of 64 hexadecimal digits) or **String** (8 to 63 printable ASCII characters).
3. The **Minimum PSK Length** which is 8 for both the PSK types.
4. The **Maximum PSK Length** which is 64 for Hexadecimal and 63 for string.
5. You can set the following password complexity parameters based on the PSK type.
   - **Alphabetic characters to include** - The permissible alphabetic characters that the password can include.
   - **Number to include** - The maximum number of alphabetic characters allowed in a password. The limit is 20 characters.

- **Numeric characters to include** - The permissible numeric characters (numbers) that the password can include.
- **Number to include** - The maximum number of numeric characters allowed in a password. The limit is 20 characters. Other characters to include - The permissible other (special) characters that the password can include.

Tag the MPSK password policy to the guest portal, see Tagging an MPSK Password Policy.

PSK Authentication

Update the **PSK Authentication** tab to setup and enable dynamic VLAN mapping for PSK based user authentication. Enable VLAN mapping and enter one or multiple VLAN IDs or ranges. The VLAN IDs are separated using commas and VLAN ranges are specified using hyphens.



For more information, see VLAN Mapping.

Guest Portal Configurations

The following configurations are required to enable and use the MPSK feature. Navigate to **Guest Portal > Portals** to complete the following.

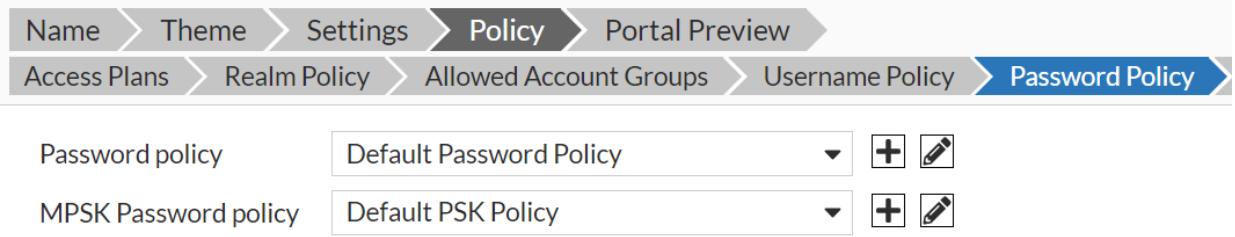
- Enabling MPSK Device Registration
- Tagging an MPSK Password Policy

Enabling MPSK Device Registration

The administrator can enable MPSK device registration as a post-authentication setting for captive portal. Navigate to **Settings > Portal Pages** and enable **MPSK Device Registration**. The guest users can create MPSK keys only after successful captive portal authentication.

Tagging an MPSK Password Policy

While creating a guest portal, you are required to tag an MPSK password policy in **Policy > Password Policy**. Select the policy that you wish to apply in the **MPSK Password policy** field. Optionally, you can also create a new password policy or edit an existing password policy on this page.



Guest Portal Device Registration

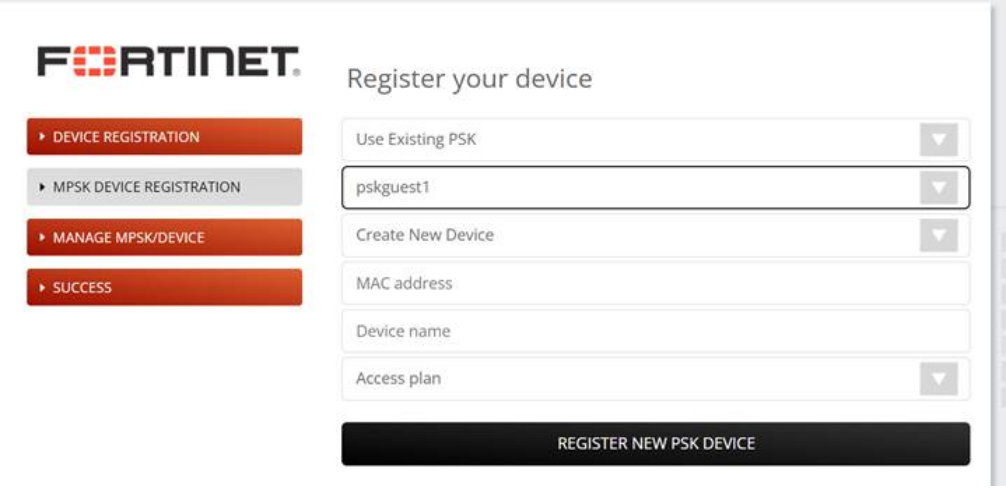
The following pages are displayed for MPSK management on the client device after successful captive portal authentication. The administrator can also create a PSK device account and tag it to the guest user, see Creating PSKs.

- MPSK Device Registration
- Manage MPSK/Device

MPSK Device Registration

When guest users log in for the first time and no devices are tagged to the guest user, the user device MAC address from the session is populated on this page. The guest is required to enter the **PSK Password**, **PSK Name**, and **Access plan**. The guest user can register more devices by choosing from an existing PSK which was created earlier.

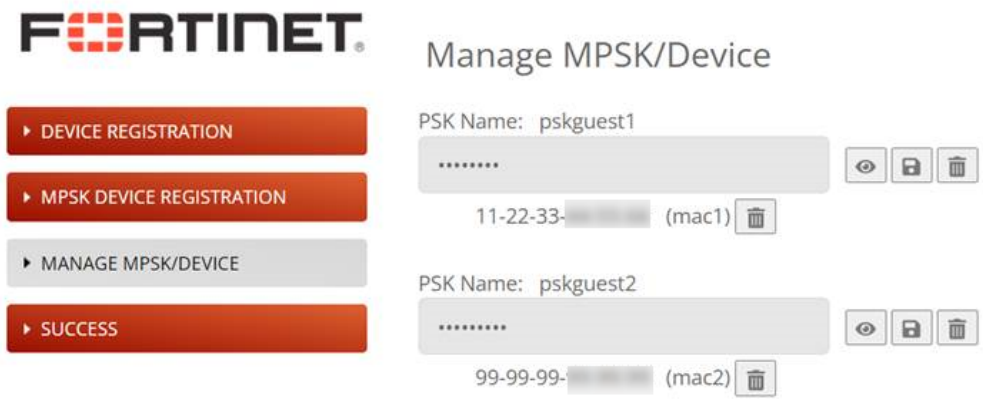
Note: Ensure that an unlimited usage profile is created and referenced in the access plan when configuring the guest portal. There is no default access plan and usage profile created for MPSK.



Manage MPSK/Device

The guest users can view and manage all PSKs and device information and can perform the following operations from this page.

- Edit, save, and delete a PSK.
- Delete MAC addresses associated to a PSK.



Email and SMS notifications are sent to the guest user based on the configured notification settings in the FortiGuest GUI. The SMS body for an unlimited device account SMS template is required to be configured. The **MPSK Password Policy** tagged to the guest portal is applied to all the PSKs created here. See MPSK Password Policy.

FortiGate Configurations

Use the FortiGate command line interface for related MPSK configurations to use with FortiGuest. For more information see FortiGate CLI Reference.

- Configuring an MPSK profile
- Configuring Virtual Access Point (VAP)

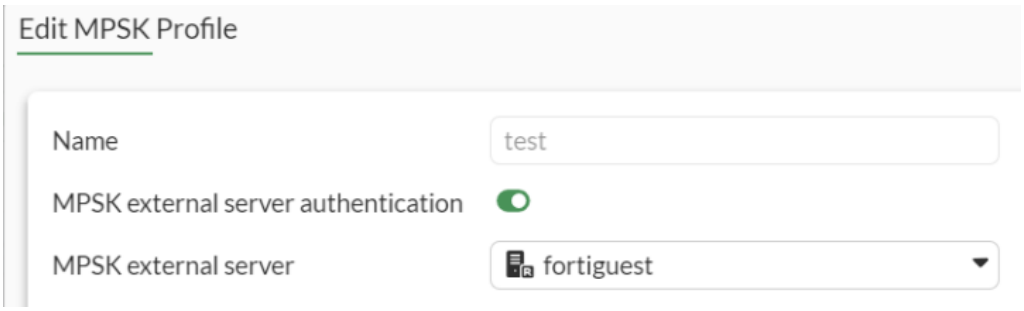
Configuring an MPSK profile

Run the following commands to enable an MPSK Profile on an external server.

```
config wireless-controller mpsk-profile
    edit "<MPSK Profile Name>"
       set mpsk-external-server-auth enable
       set mpsk-external-server <server-1>
```

Note: The shared secret must be the same as the secret in the **RADIUS Client** configured in FortiGuest.

You can configure FortiGuest as the external server in the FortiGate GUI. Navigate to **WiFi & Switch Controller > Connectivity Profiles**. Enable **MPSK external server authentication** and select FortiGuest as the **MPSK external server**.



Configuring Virtual Access Point (VAP)

Run the following command to configure a VAP. Ensure that an SSID used here is configured with the security mode **WPA2 Personal**.

```
config wireless-controller vap
    edit "SSID Name"
       set ssid "SSID Name"
       set security wpa2-only-personal
       set mpsk-profile "MPSK Profile Name"
    next
```

System Settings

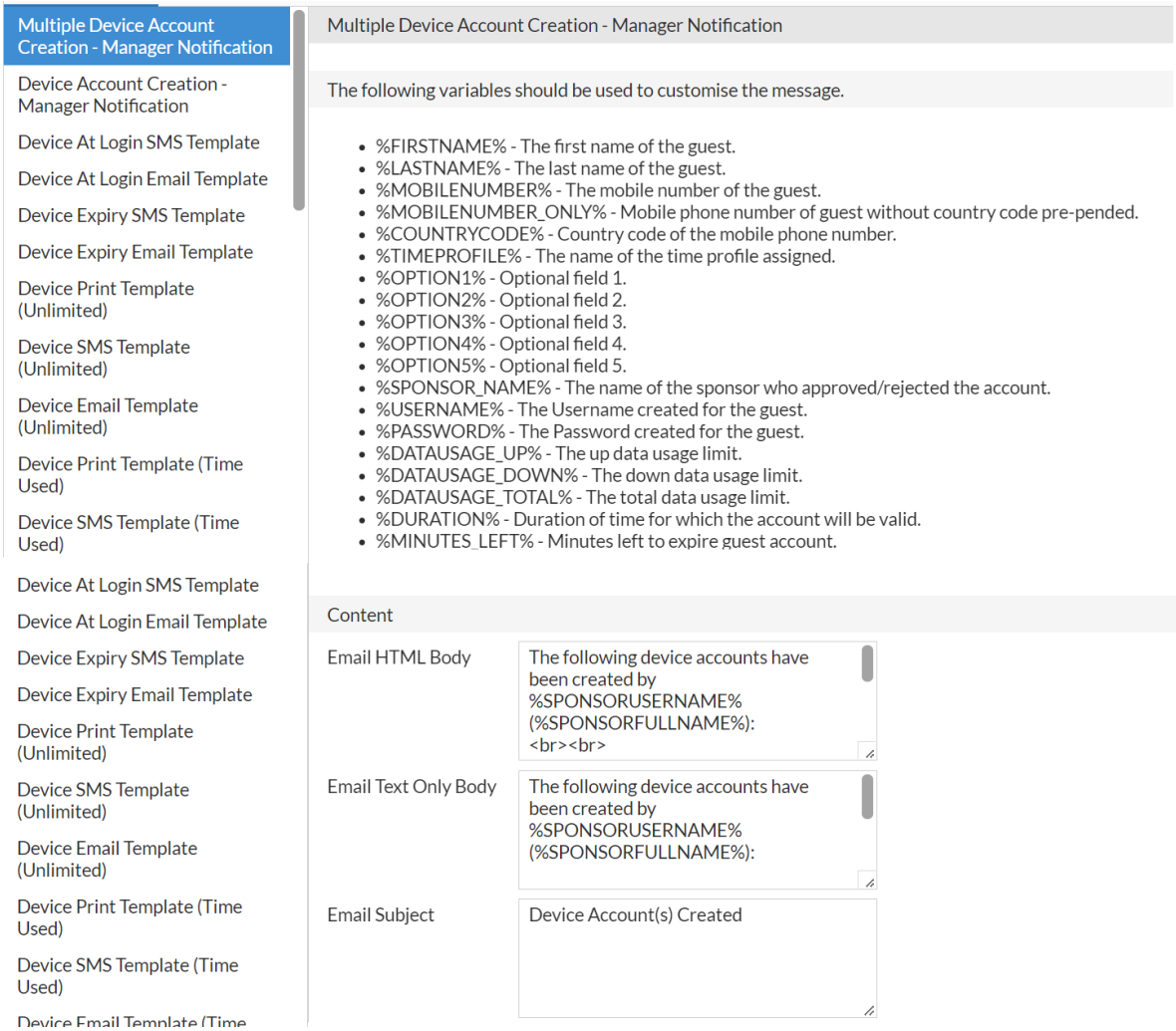
FortiGuest is administered using a web interface over either HTTP or HTTPS, or partially via the CLI. After initial installation, you can perform specific network configurations and administrative tasks.

Language Templates

You can edit the guest/device email, SMS, and print templates containing the user account and activity details, that a sponsor can communicate to the guest. The contents of the template messages can be fully customized. Navigate to **System > Language Templates**.

Notes:

- English, French, Spanish, and Portuguese are the supported languages.
- Ensure that SMS and email notifications are enabled, to send the relevant notifications. See SMS Notifications and Email Notifications.



1. Create a new template and click **Edit**.
   On the left pane various templates for email, SMS, and print notifications are displayed. These templates are classified based on usage profile types like unlimited, time used, from creation, and so on.
2. Select the notification template from the list in the left panel. The customizable variables are displayed.
3. Modify the default HTML code in the text message fields as required.

Note: when using HTTP API based SMS gateways, these characters are allowed in language templates or notification templates in the guest portal content, !$^*()-_=+[]{};:@#~,<>?. Use backslashes for the characters, /\", when using them in language templates or notification templates. For example, *V* \\ \".

Network Settings

You can configure the following network settings for your FortiGuest.

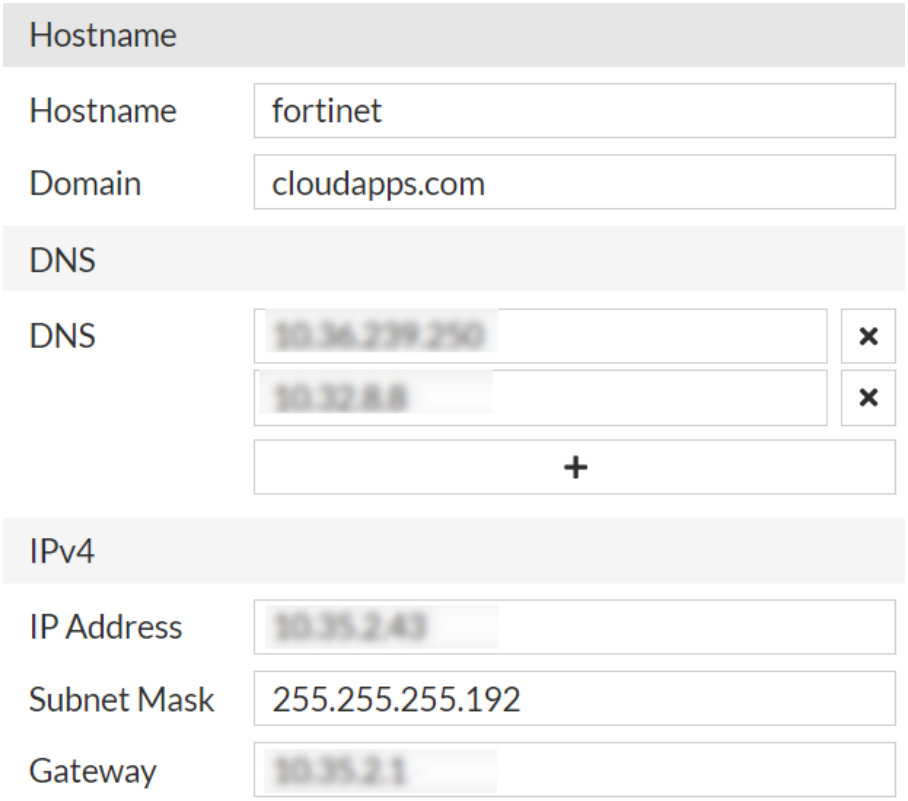
- Server Information
- Network Interface Information

- Static Routes on page 150

Server Information

You can configure or modify the pre-configured FortiGuest server settings.

1. Navigate to **System > Network Settings**.

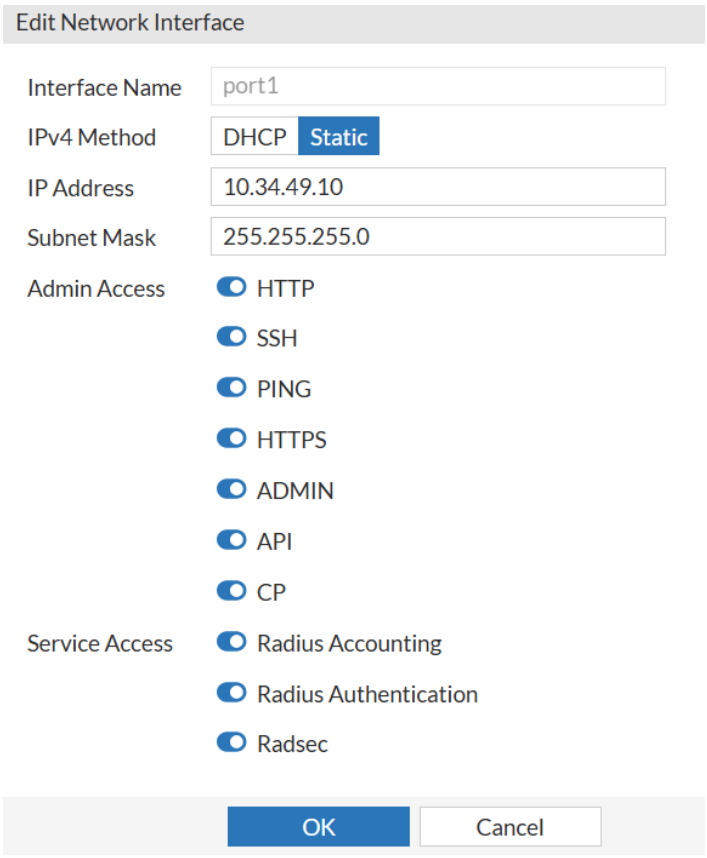


2. Configure the **Hostname** settings.
   - **Hostname** - Assign a hostname as defined in DNS (without DNS suffix).
   - **Domain** - Enter the domain name for your organization (e.g. *fortinet.com*).
3. Enter the IP address of the **DNS** server.
4. Configure the network IPv4 address settings.
   - **IP Address** - Enter the network IPv4 address.
   - **Subnet Mask** - Enter the corresponding subnet mask.
   - **Gateway** - Enter the default gateway for the network to which FortiGuest is connected.

Network Interface Information

You can configure FortiGuest with 4 active interfaces with traffic segregation. The administrators can configure administrative access and services like captive portal and RADIUS authentication/accounting on a per interface basis.

Note: If administrative access services and captive portal are configured for different interfaces, then FQDN forward and reverse lookup in the DNS server should point to the IP address of the interface which has captive portal configured. In such a scenario, the administrator can access the FortiGuest portal only with IP address and not with the FQDN.

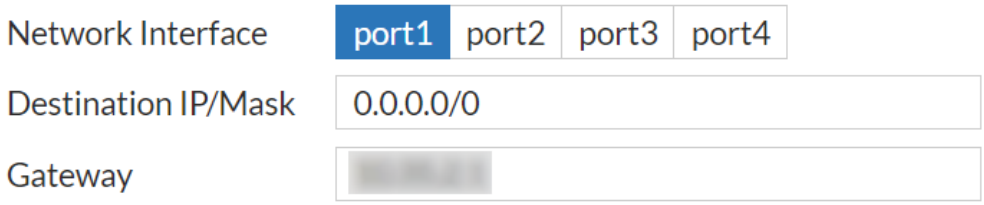


Select a port and click **Edit** to modify the following settings as required.

Settings	Description
IP Address and **Subnet Mask**	Select IPv4 method as **DHCP** or **Static**. If Static is selected, enter the IPv4 address and netmask associated with this interface. **Note**:Only one of the four port interfaces can support DHCP configuration at a time.
Admin Access	Select the allowed administrative service protocols from the following. • SSH • HTTP • Ping • HTTPS - Specify admin (GUI), REST API, and/or captive portal access.
Service Access	Enable the services that you want FortiGuest to act as a server for. • RADIUS Accounting • RADIUS Authentication • RadSec

Static Routes

In this page, you can create a default route to your network gateway on the interface that connects to the gateway. You can create, edit, or delete routes as required.



Settings	Description
Network Interface	Select the network interface that connects to the gateway.
Destination IP/Mask	The destination IP address and netmask for this route.
Gateway	Enter the IP address of the next hop router to which this route directs traffic.

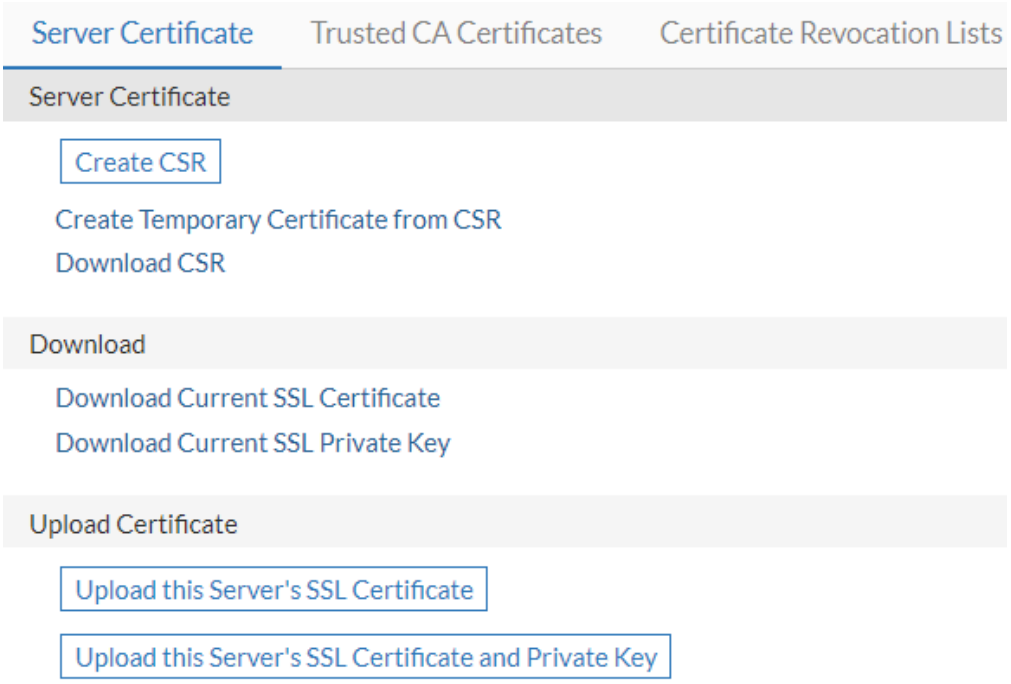
Certificates

You can configure and manage certificates from the FortiGuest GUI to secure communication with devices that make SSL connections.

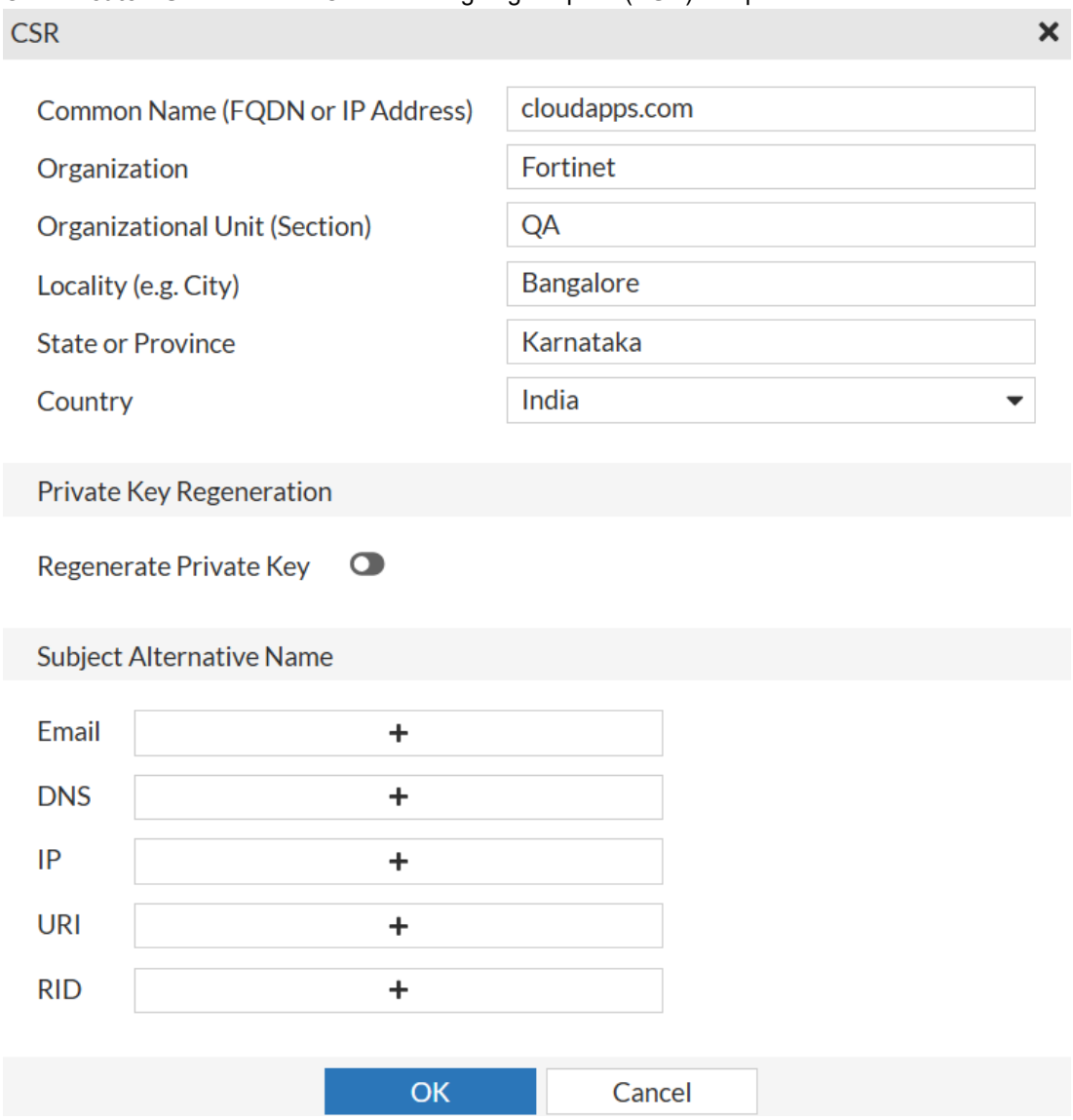
- Server Certificate
- Trusted CA Certificates
- Certificate Revocation Lists
- Local Certificate Authorities

Server Certificate

You can create server certificates and manage them easily via the GUI.


Server Certificate
Trusted CA Certificates
Certificate Revocation Lists
Server Certificate
Create CSR
Create Temporary Certificate from CSR
Download CSR
Download
Download Current SSL Certificate
Download Current SSL Private Key
Upload Certificate
Upload this Server's SSL Certificate
Upload this Server's SSL Certificate and Private Key

1. Navigate to **System > Certificates** and click the **Server Certificate** tab.
2. Click **Create CSR** to create a Certificate Signing Request (**CSR**) and provide details for the certificate.



- **Common Name (FQDN or IP Address)** - This is either the IP address of FortiGuest or the fully qualified domain name (FQDN) for FortiGuest. The FQDN must resolve correctly in DNS.
- **Organization** - The name of your organization or company.
- **Organizational Unit (Section)** - The name of the department or business unit that owns the device.
- **Locality** (e.g. City) - The city where the server is located.
- **State or Province** - The state where the server is located.
- **Country** - Select the relevant country.
- The **Regenerate Private Key** is optional. If you regenerate your private key, the current certificate is invalidated and a new self-signed temporary certificate is generated using the new private key and CSR. If you choose to regenerate the private key, services are restarted to enable you to use the new certificate and private key.
- **Subject Alternate Name** (SAN) is an extension of the X.509 certificate standard and allows you to secure multiple hostnames, IP addresses, or other identifiers with a single certificate. You canoptionally, enter the alternative names for the specified **Common Name** for the CSR, in one of the

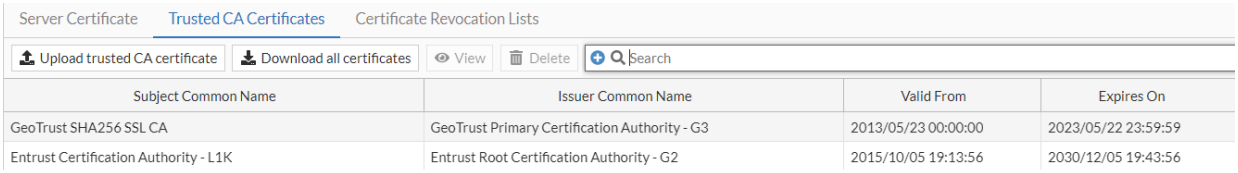
following formats.

- *Email address*
- *DNS*
- *IP address*
- *URI*
- *RID*

3. Click **Create Temporary Certificate from CSR** to generate a temporary certificate from the CSR that you created in the previous step.
4. Click **Download CSR** to download the CSR on to your machine.
5. You can backup the certificate and private key manually in a secure location. Click **Download Current SSL Certificate** and **Download Current SSL Private Key**.
6. After you have sent the CSR to a *Certificate Authority* and obtained the CA-signed certificate in return, you can upload it to FortiGuest in the **Upload Certificate** section. This installs a CA signed certificate or restores Base 64 PEM format certificate files previously backed up. You must upload certificate files in Base 64 PEM format or DER format. The certificate files are not backed up as part of any backup process. You must manually back them up in the **Download** certificate files section. Click **Upload this Server's SSL Certificate** and locate the SSL certificate file you want to upload. If the private key have been created separately, then you can select both from different locations and upload them under the **Upload this Server's SSL Certificate and Private Key** section on the same page.

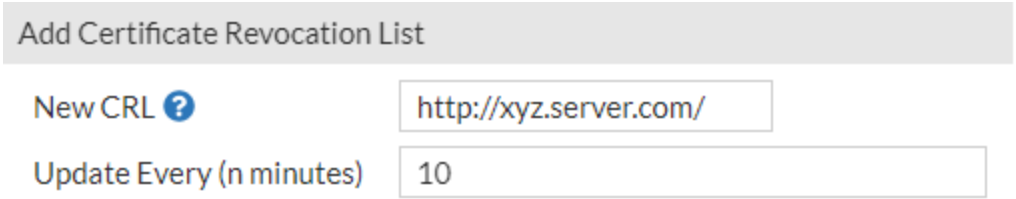
Trusted CA Certificates

FortiGuest allows you to upload trusted CA certificates so that it can trust devices that it makes SSL connections to. Locate the file using the **Upload trusted CA certificate** and upload it. You can also click on the **Download all certificates** link to download all certificates.



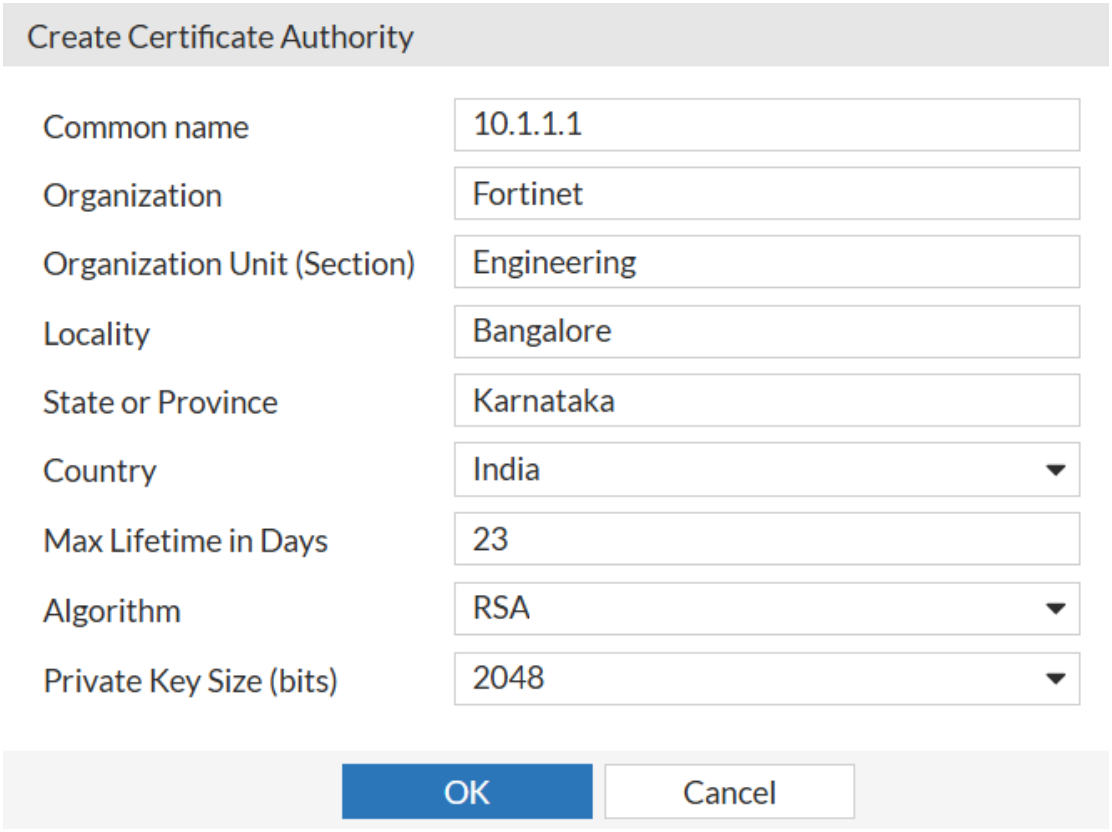
Certificate Revocation Lists

A certificate is irreversibly revoked if, for example, if a private key is thought to have been compromised. Certificates may also be revoked for failure of the identified entity to adhere to policy requirements specified by the CA operator or its customer. The most common reason for revocation is the user no longer being in sole possession of the private key. FortiGuest automatically uploads certificates to a revocation list and updates the certificate at a set specific time period. CRL's can be manually added to this list by entering the URL of the stored CRL into the **New CRL** option. Enter a time value that you wish this CRL to be updated in the **Update Every** field.



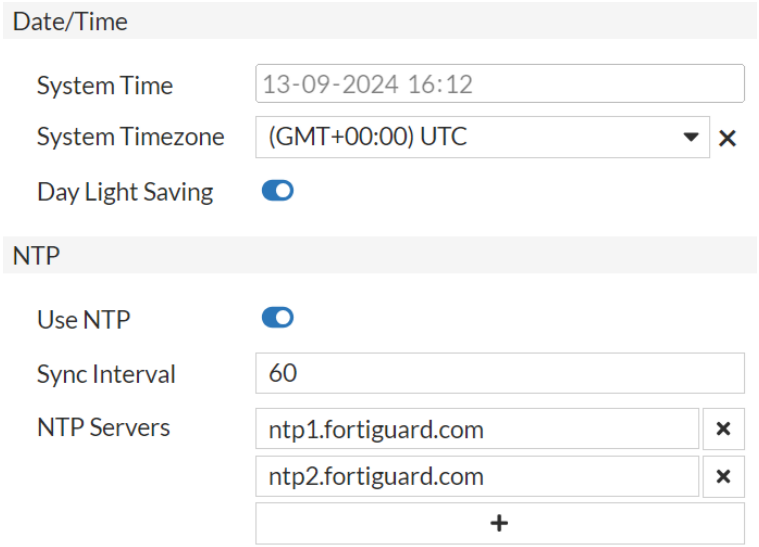
Local Certificate Authorities

1. Perform the following steps to generate certificates internally.
2. Navigate to **System > Certificates > Local Certificate Authorities**.
3. Click **+New**.
4. Configure the following parameters.
   - **Common Name** - This is either the IP address of FortiGuest or the fully qualified domain name (FQDN) for FortiGuest. The FQDN must resolve correctly in DNS.
   - **Organization** - The name of your organization or company.
   - **Organizational Unit (Section)** - The name of the department or business unit that owns the device.
   - **Locality** (e.g. City) - The city where the server is located.
   - **State or Province** - The state where the server is located.
   - **Country** - Select the relevant country.
   - **Maximum Lifetime in Days**- The maximum lifetime of any generated certificate in days.
   - **Algorithm** - The algorithm to be used, *RSA* or *ECDSA*.
   - **Private Key Size (bits)** - If RSA algorithm is selected, set the minimum size of the private key to generate. The minimum size is 2048 bits.



Date/Time Settings

Ensure that the correct date and time format are configured as FortiGuest authenticates users based on the time associated with their accounts (activation and expiry). You can view and configure the system date and time on FortiGuest.



1. Navigate to **System > Date/Time Settings** and select the date and the **System Timezone** where your FortiGuest is located.
   Note: Modifying the **System Timezone** automatically adjusts the date and time on FortiGuest and you are notified appropriately.
2. You can **Use NTP** to synchronize the date and time with the configured NTP server. Enter the IP address (es) of the **NTP servers** available. Enable **Sync Interval** to configure the synchronization interval with the configured NTP server. The default is 60 seconds, and the allowed range is 1 – 1440 seconds.

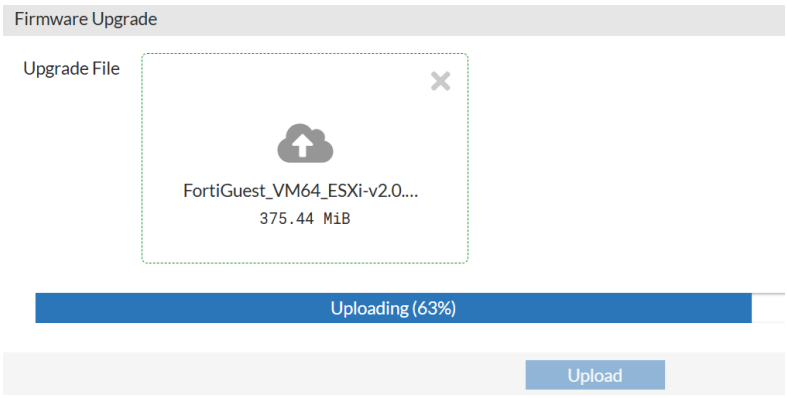
The date and time settings can be modified via the CLI.

Licensing

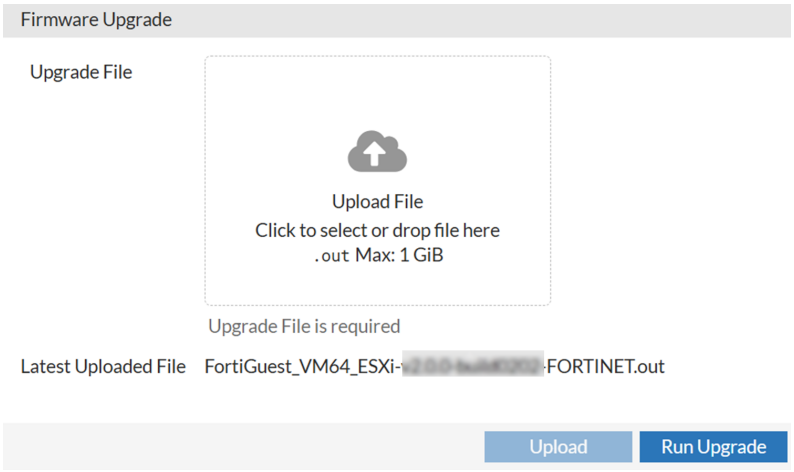
The licensing page allows you to view and upload the FortiGuest license file. For more information, see Licensing.

Firmware Upgrade

You can upgrade FortiGuest from the GUI, navigate to **System > Firmware Upgrade** to upload the FortiGuest image file.

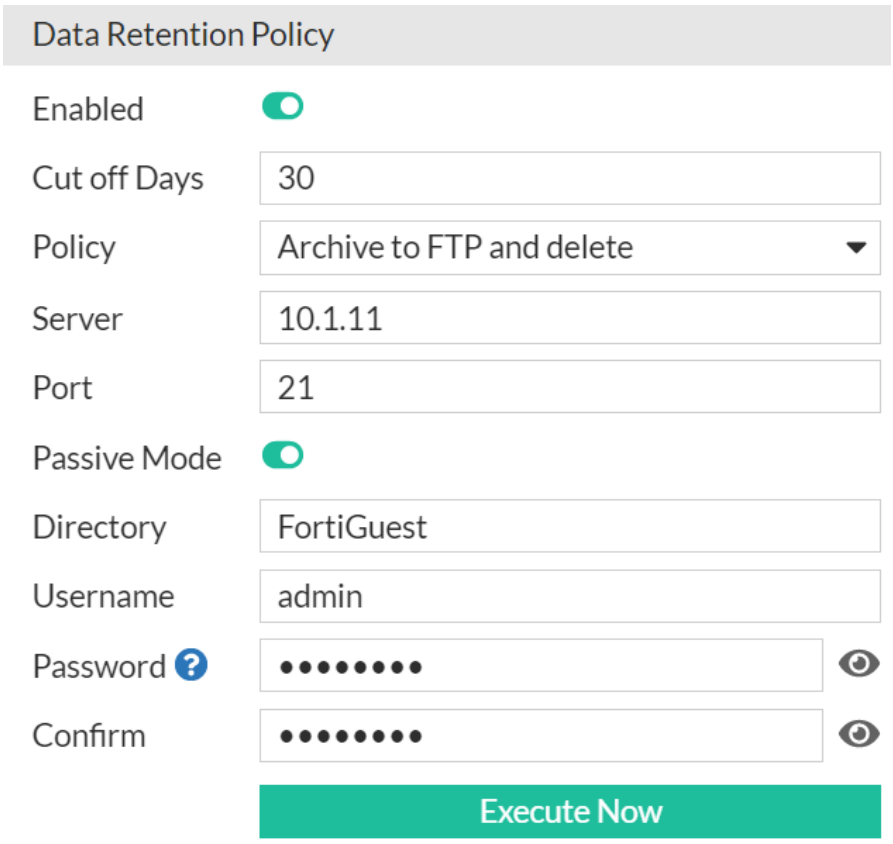


After successfully uploading the file, click **Run Upgrade**.



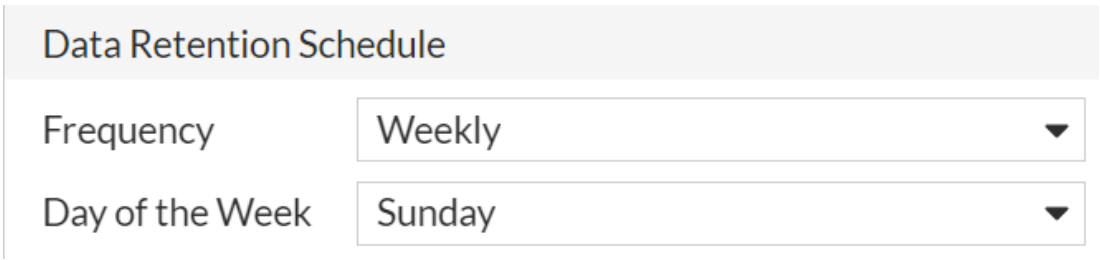
Data Retention Policy

You can delete or archive old data from FortiGuest based on the configured data retention policy. Navigate to **System > Data Retention Policy** and enable and configure the following retention settings to archive data.

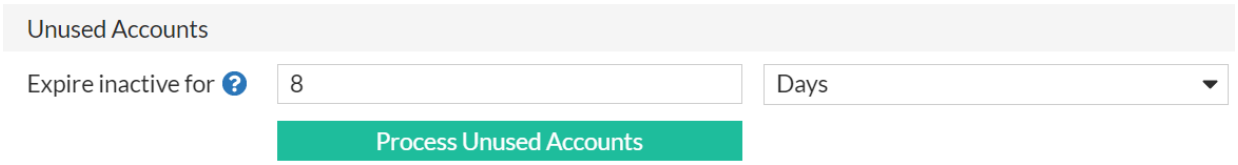


- **Cut off Days** – Enter the number of days to process the data as per the configured policy.
- **Policy** - Select a policy to create a backup/archive on an FTP (**Archive to FTP and delete**) or SFTP (**Archive to SFTP and delete**) server prior to deleting the data from FortiGuest. You can also choose to delete data without archival (**Delete only**). Update the following fields if you select data archival on the FTP/SFTP servers.
  - **Server** – Enter the IP address or hostname of your SFTP/FTP server.
  - **Port** - Enter the required port number.
  - **Passive Mode** – (FTP only) Enable the FTP passive mode for data backup.
  - **Directory** – Specify the directory name to archive the data.
  - **Username** and **Password** – Enter the FTP/SFTP server username and password. **Confirm** the password.
- Click **Execute Now** to implement the data retention policy.

You can enable expiration of any **Unused Accounts** if they are inactive for a certain amount of time. Select the duration for which the account is inactive, to allow expiration and click **Process Unused Accounts**.



Configure the frequency of data retention in the **Data Retention Schedule** section. You can configure a data retention **Frequency** of **Daily**, **Weekly**, or **Monthly** and select a relevant **Day**.



Backup Policy

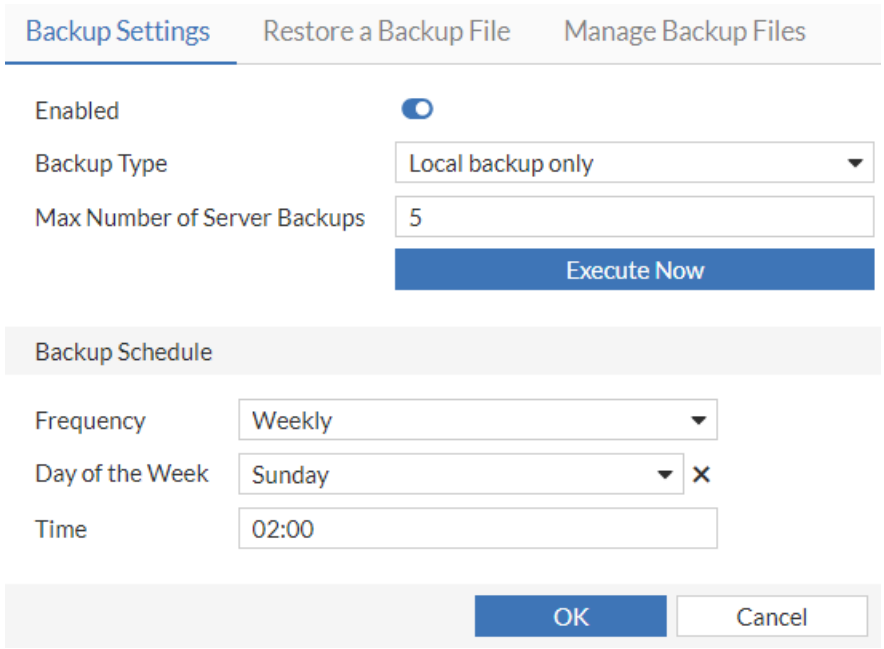
Backup the FortiGuest on a regular basis so that in the event of a hardware failure you do not lose critical data. The FortiGuest backup process backs up the system setup, account database, and all audit records, enabling you to recover everything you need in the event of a failure. You can either create a *point-in-time* snapshot or schedule system backups to be automatically saved to the FortiGuest or a remote server.

You can perform the following operations for FortiGuest backup and restore.

- Backup Settings
- Restore a Backup File
- Manage Backup Files

Backup Settings

1. Navigate to **System > Backup Policy** and select the **Backup Settings** tab.
2. Enable backup policy and select a **Backup Type**. You can backup the FortiGuest data on a local server (**Local backup only**), a local server and a remote FTP server (**FTP and local backup**), or a local server and a remote SFTP server (**SFTP and local backup**).



3. If the backup type is **Local backup only**, then enter the **Maximum number of server backups** to limit the number of backup files that are created. Leave this field blank to configure an unlimited number of backup files.
4. If the backup type is **FTP and local backup** or **SFTP and local backup**, then update the following fields.
   - **Server** - Specify the remote server IP address for the FTP/SFTP.
   - **Port** - Enter the TCP port used by the configured server.
   - **Passive Mode** - Enable to activate the passive mode for the FTP server *only*.
   - **Directory** - Specify the directory path to save the backup files.
   - **Username** and **Password** - Specify the username and password to access the FTP/SFTP servers.
   - **Max Number of Server Backups** - Specify the number of backup files that are created. Leave this field blank to configure an unlimited number of backup files.
5. Click **Execute Now** to initiate a backup immediately.
   Note: In case of insufficient disk space to complete the operation, requisite warning messages are generated in the Audit Logs. The default disk space requirement is 40% of the database.
6. Configure the frequency of the backup in the **Backup Schedule** section. You can configure to run the schedule **Daily**, **Weekly**, or **Monthly**. If you select **Weekly** you must also specify which day of the week. If you select **Monthly**, you must specify which day of the month.
   Note: FortiGuest removes old backups that exceed this amount by discarding the oldest backup when new files are created.

Restore a Backup File

You can restore a backup on FortiGuest, select the backup archive you want to restore. The backup is uploaded to the FortiGuest and the data is restored. After the data is restored, the server reboots so that the database is correctly loaded.

1. Navigate to **System > Backup Policy** and select the **Restore a Backup File** tab.
2. Select a **Backup** saved on the server to restore data on FortiGuest.

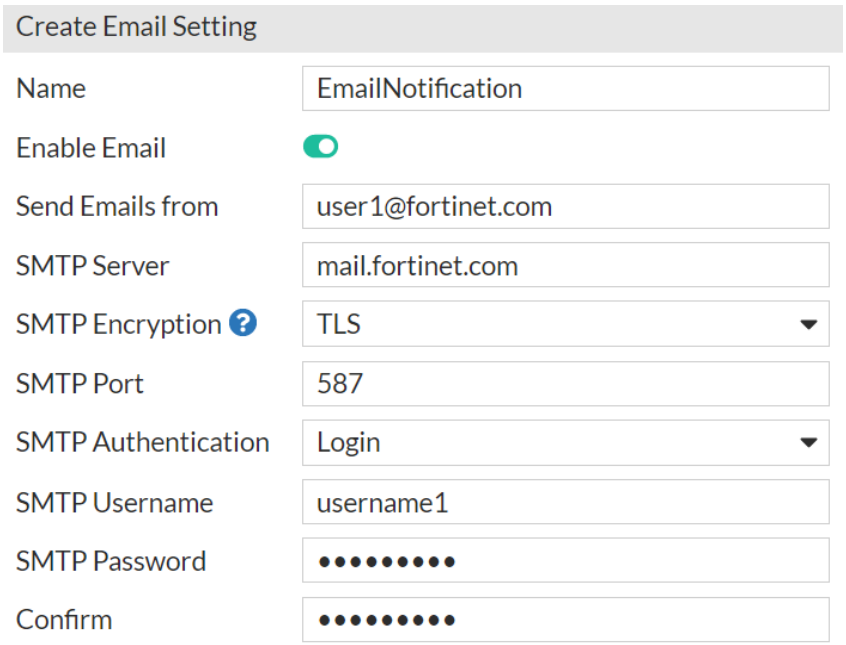
Manage Backup Files

You can manage all the backups you have performed using FortiGuest.

1. Navigate to **System > Backup Policy** and select the **Manage Backup Files** tab. All the backup files are displayed.
2. From here you can click on **Download** to save a file locally, or click on **Delete** to delete the file.

Email Notifications

You can configure email settings for FortiGuest to correctly deliver user account details via email. You can **Clone** the email notification settings to reuse configurations.

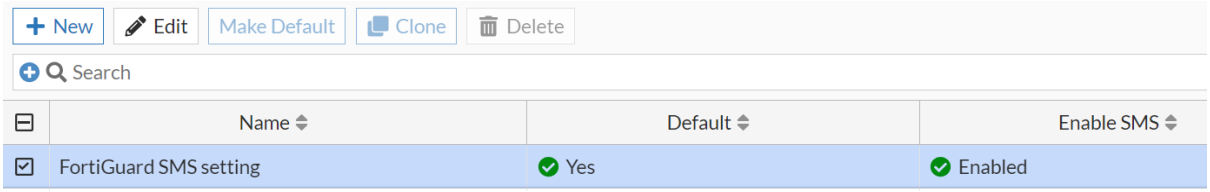


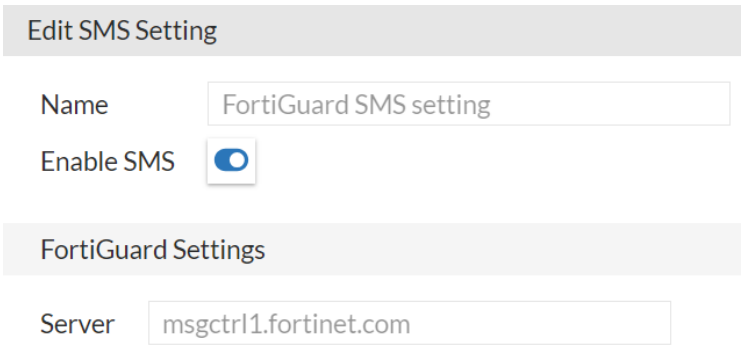
1. Navigate to **System > Email Settings** and enable email functionality globally.
2. Enter the email address from which you want to send user notification emails.
3. The IP address/FQDN of the outbound **SMTP Server** to which you need to deliver the email. If you enter localhost, or leave this field empty, the FortiGuest attempts to deliver the email directly to the user's SMTP server.
4. Select the SMTP encryption, **SSL** or **TLS**. When using encryption, ensure that the SSL certificates are uploaded in the **Server > SSL Settings > Trusted CA Certificates**.
5. Enter the SMTP **Port**, **Username**, and **Password** details.

SMS Notifications

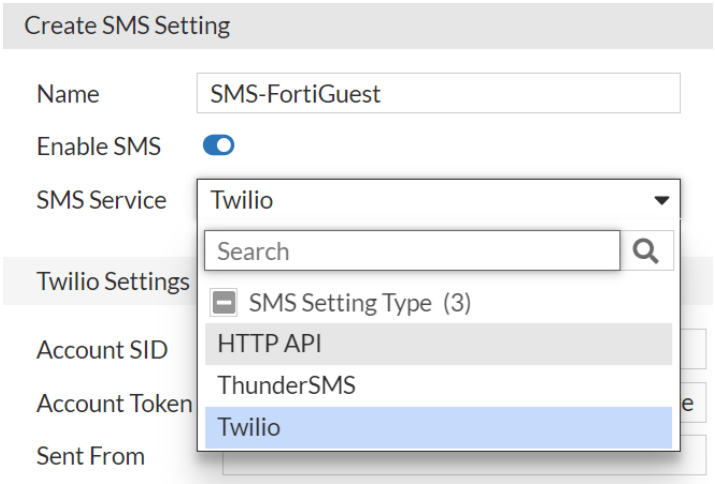
The Short Message Service (SMS) is delivered through an SMS gateway service that supports SMTP delivery. You need to have an internal SMS gateway service or subscribe to an external service to be able to deliver user details via SMS. You can **Clone** the SMS notification settings to re-use configurations.

To use FortiGuest's pre-existing FortiGuard SMS setting, mark this as the default, click **Make Default**. You can edit the settings as required.



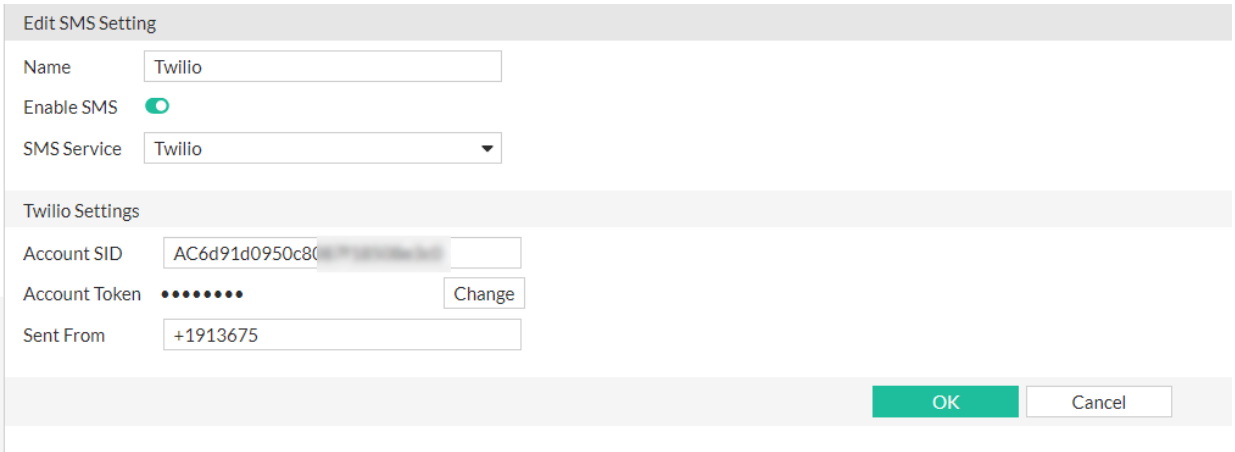


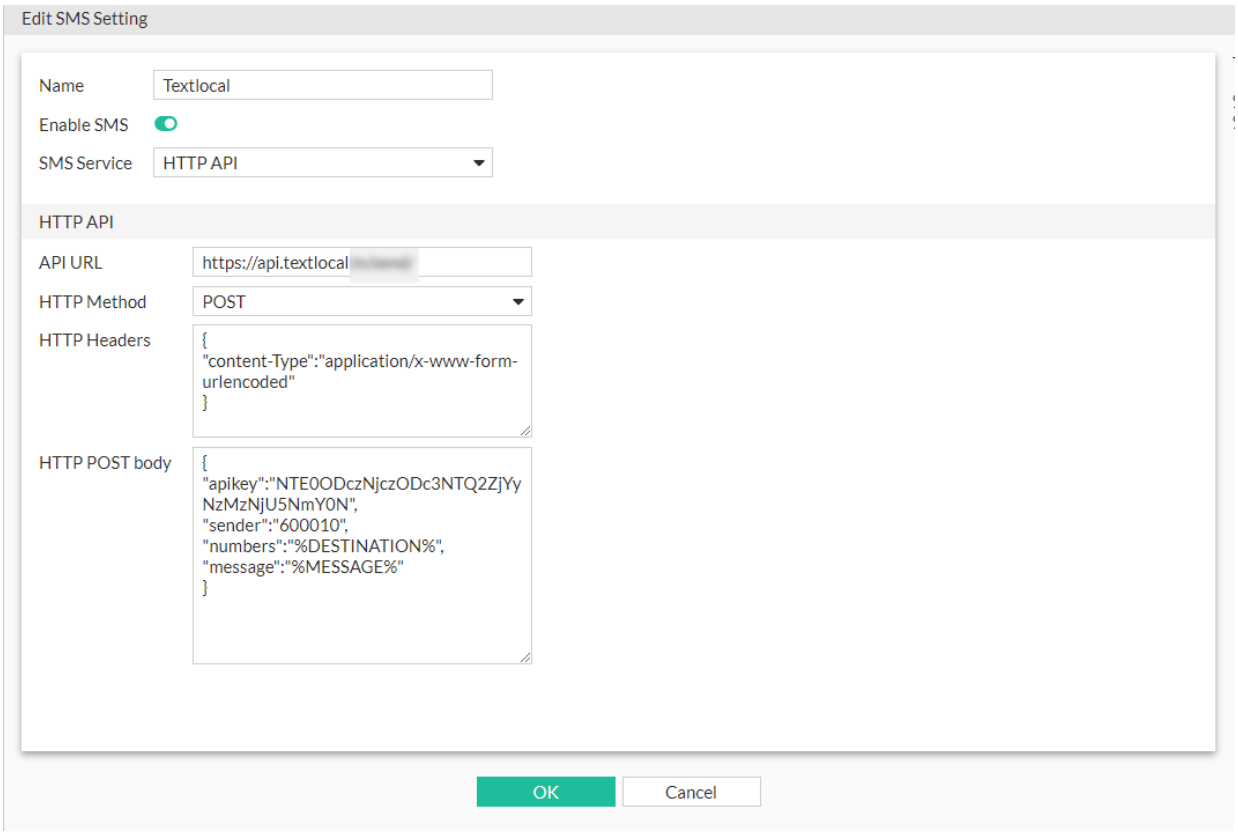
1. Navigate to **System > SMS Settings** and enable the SMS service globally on FortiGuest.



2. Select any of the following **SMS service**, update the SMS delivery settings as per the selected SMS service.
   - *HTTP API* - This option integrates SMS providers that offer a HTTP(S) API for sending SMS. Enter the API URL and HTTP message details.
   - *ThunderSMS* - The Thunder SMS account details are required. Enter the sender ID, API key, and a ThunderSMS enabled phone number are required.
   - *Twilio* - A Twilio API account along with a Twilio enabled phone number is required to configure with the FortiGuest, enter the relevant details.

The following are examples of Twilio and HTTP API SMS notification settings.

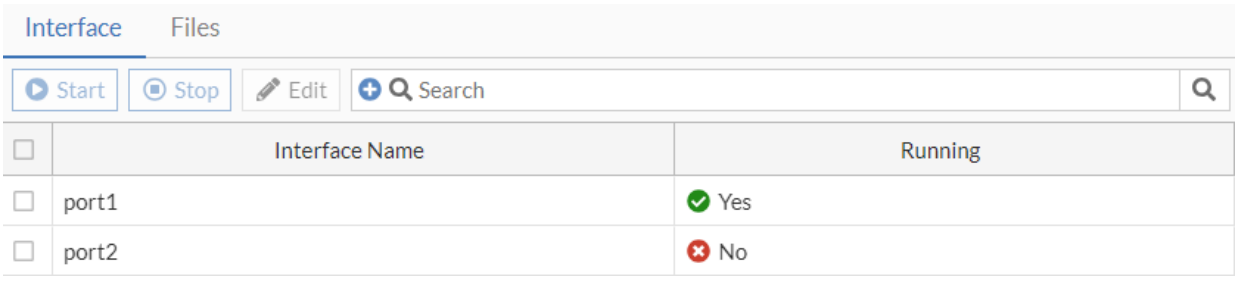




Note: when using HTTP API based SMS gateways, these characters are allowed in language templates or notification templates in the guest portal content, !$^*()-_=+[]{};:@#~,<>?. Use backslashes for the characters, /\", when using them in language templates or notification templates. For example, *V* \\ \".

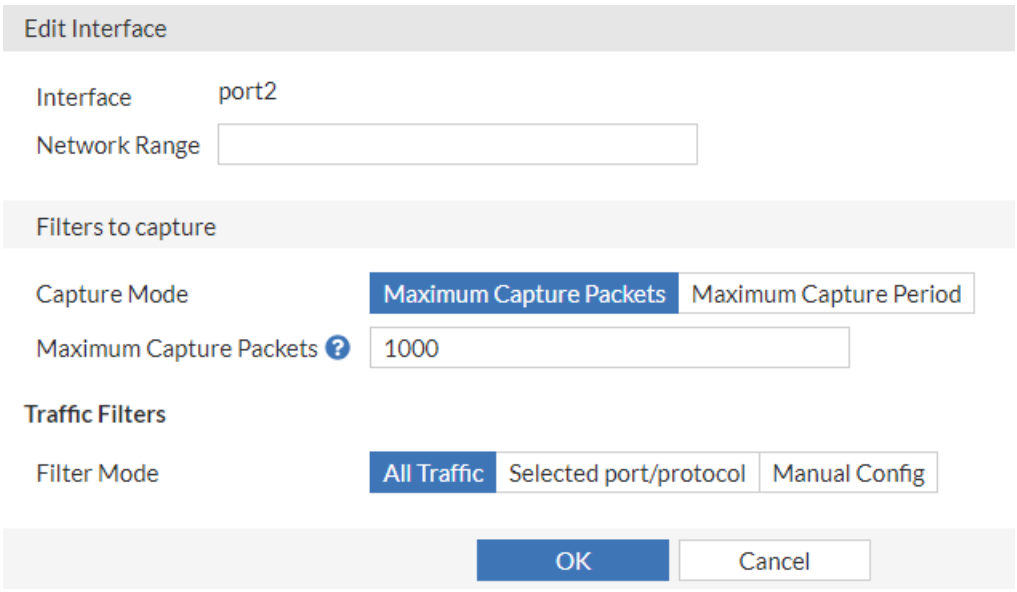
Packet Capture

FortiGuest allows the administrator to record packet data from an IP address/network range for all or specific network traffic/packets to specific ports. The packet capture feature generates log files that you can download and view using a packet viewing utility such as Wireshark.

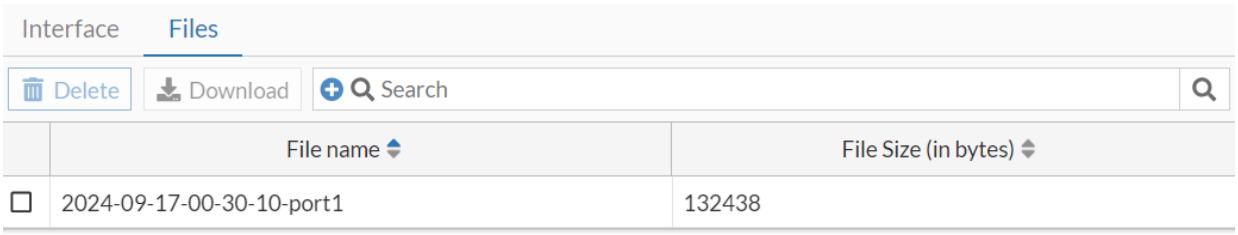


Note: Only the last 10 generated capture logs are displayed in the GUI.

Select an interface and click **Start** to start capturing packets. To update the packet capture settings, click **Edit**. Enter the **Network Range** you wish to capture traffic to and, specify either the maximu packet captures or the maximum capture period; enable **Maximum Capture Packets** and the allowed vlue range is 1 - 10000 OR enable **Maximum Capture Period** and the allowed value range is 1 - 300 minutes. Enable the relevant traffic to capture from the listed options. If you require to capture all the network traffic, select **All Traffic**.



You can download/delete the generated packet capture logs from the **Files** tab.



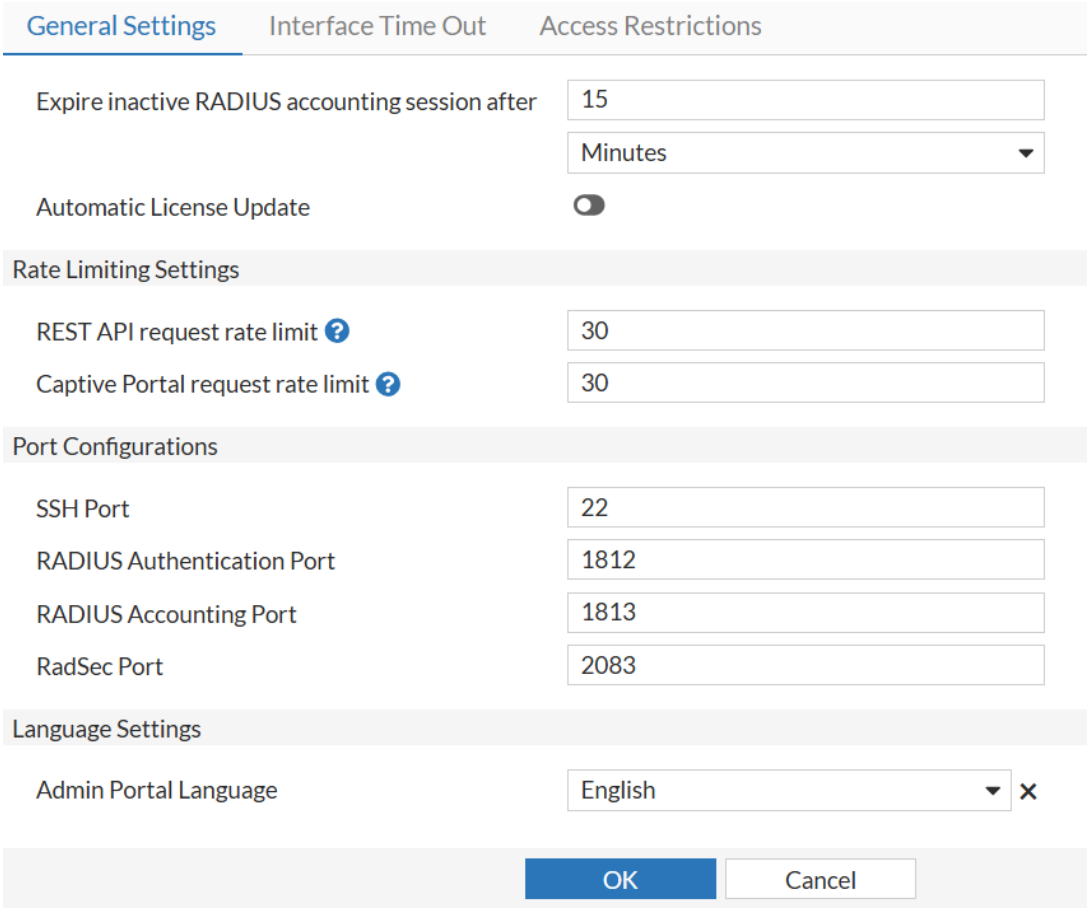
Settings

You can configure the settings related to RADIUS accounting and licensing, interface time out and access restriction.

- General Settings
- Interface Timeout
- Access Restrictions

General Settings

You can configure the following settings related to RADIUS accounting and licensing.



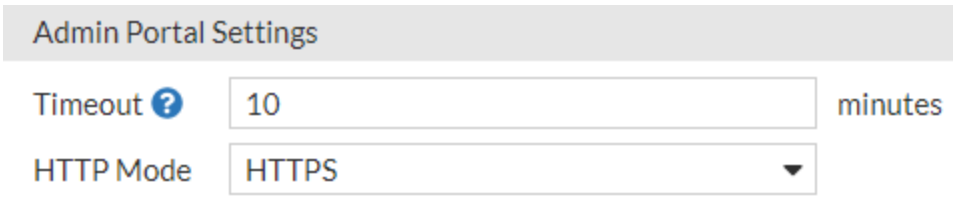
- **Expire inactive RADIUS accounting session after** - Set the time limit in minutes/hours/days, after which an inactive RADIUS accounting server session expires. See RADIUS Accounting Server.
- **Automatic License Update** - To automatically renew the license subscription for FortiGuest (valid for one year) before the expiry, contact *Fortinet Customer Support* and enable this option. The same license is updated and you are not required to procure a new license.
- **Rate Limiting Settings** - Set the rate limiting value for the FortiGuest admin and captive portal APIs. The allowed range for these fields is 5 - 50 requests per second and the default is 30 requests per second.
- **Port Configurations** - Configure ports for SSH, RadSec, and RADIUS Authentication and Accounting.
- **Language Settings** - Set the language for the admin portal.

Interface Timeout

A sponsor or administrator that logs in into the FortiGuest is logged out after a period of inactivity. You can set the inactivity period through the timeout settings.

Note: The session timeout defined here applies to both the sponsor and administration interfaces.

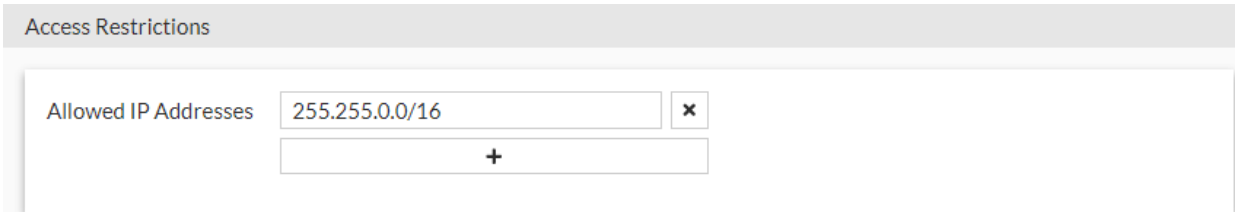
1. Navigate to **System > Interface Timeout Out** and enter the session **Timeout** value in minutes (default is 10 minutes). When you are inactive for the configured period of time, your sessions expire and the next action requires you to log in again.



2. Select the **HTTP Mode** used to access the FortiGuest portal.

Access Restrictions

You can configure FortiGuest to restrict access to only certain IP address ranges for the administrator and sponsor at any one time. Navigate to **System > Access Restrictions**. In the **Allowed IP Addresses** field, type a range of IP addresses that are allowed access to the FortiGuest interface, and apply a CIDR subnet range using the drop-down menu.



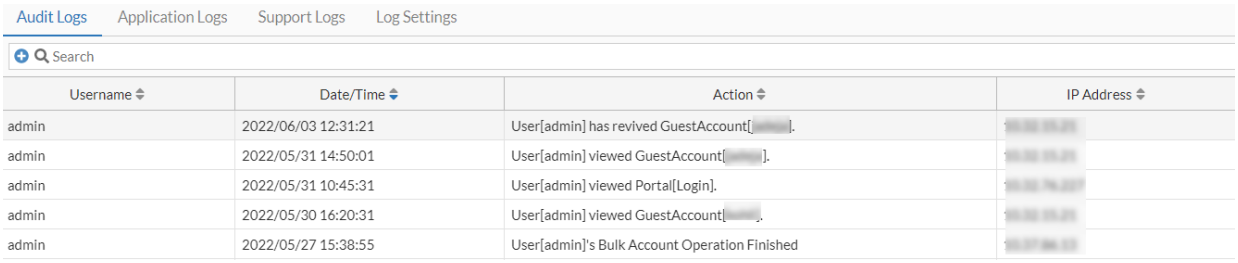
System Logs

All actions within the FortiGuest are logged into the database. This enables you to view any action that occurred as part of the normal operating process of the application, log administrator and sponsor actions, and create system logs. Navigate to **Logging > System Logs**.

- Audit Logs
- Application Logs
- Support Logs
- Log Settings

Audit Logs

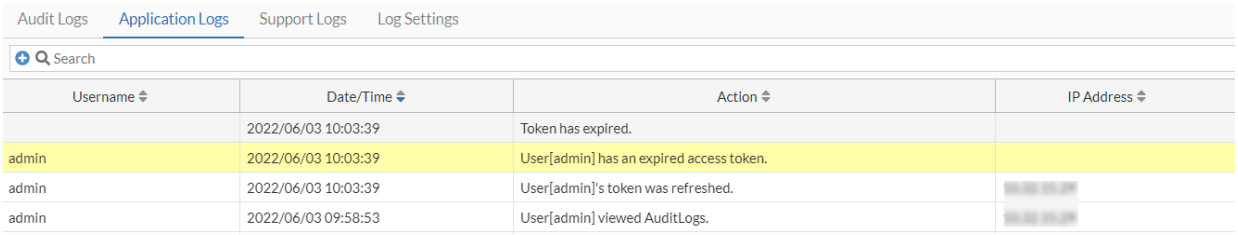
Audit logs create a record of administrator and sponsor actions.



Username	Date/Time	Action	IP Address
admin	2022/06/03 12:31:21	User[admin] has revived GuestAccount[ ].	
admin	2022/05/31 14:50:01	User[admin] viewed GuestAccount[ ].	
admin	2022/05/31 10:45:31	User[admin] viewed Portal[Login].	
admin	2022/05/30 16:20:31	User[admin] viewed GuestAccount[ ].	
admin	2022/05/27 15:38:55	User[admin]'s Bulk Account Operation Finished	

Application Logs

Application logs display the log containing application debug information.

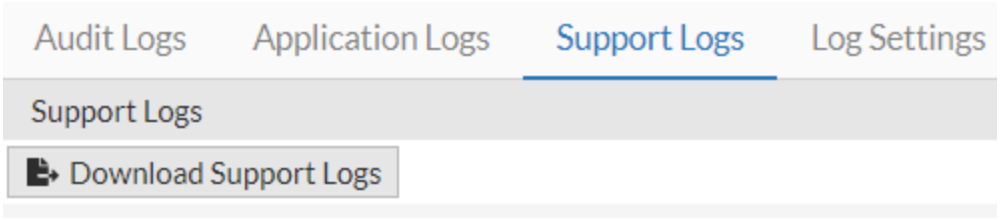


Username	Date/Time	Action	IP Address
	2022/06/03 10:03:39	Token has expired.	
admin	2022/06/03 10:03:39	User[admin] has an expired access token.	
admin	2022/06/03 10:03:39	User[admin]'s token was refreshed.	
admin	2022/06/03 09:58:53	User[admin] viewed AuditLogs.	

Support Logs

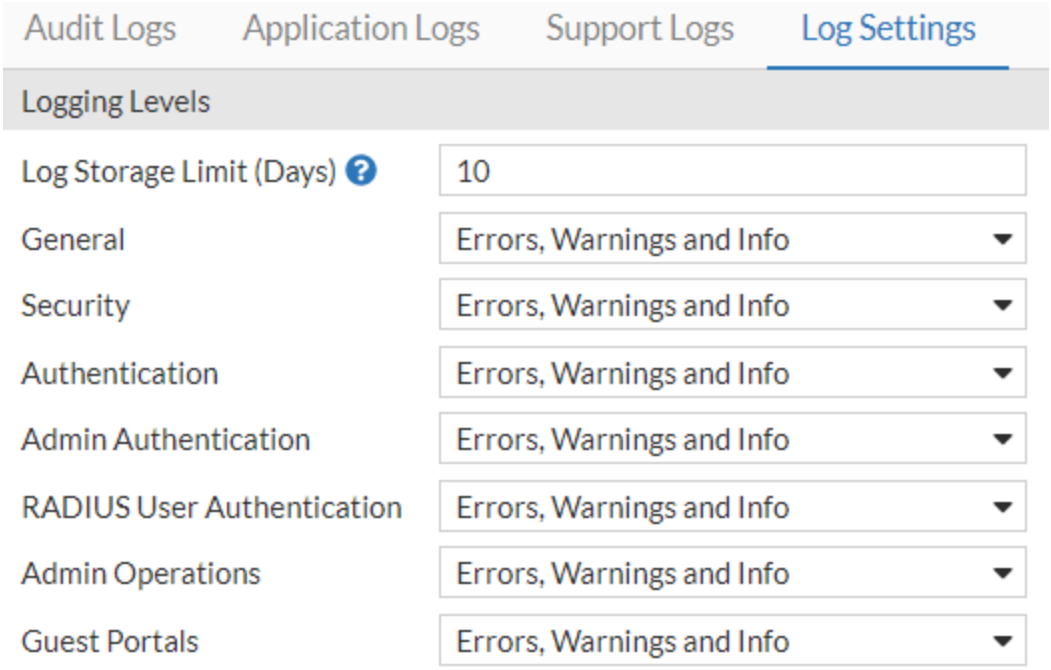
Support logs provide an area that stores the following information.

- HTTP error logs
- RADIUS logs
- Mail logs
- Debug logs
- Audit logs
- Application logs
- An XML file



Log Settings

The log settings page allows an administrator to set the level of logging and administer syslog settings. The **Logging Levels** allow an administrator to choose the level of logging for multiple criteria.



The logging levels are, **Errors and Warnings Only**, **Error Only**, **Errors, Warnings and Info**, or **Errors, Warnings, Info and Debugs**. You can specify the maximum number of days for storing logs in **Log Storage Limit**.

- General
- Security
- Authentication
- Admin Authentication
- RADIUS User Authentication
- Admin Operations
- Guest Portals

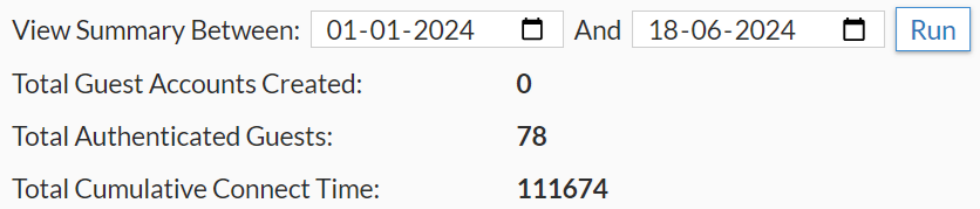
Reports

You can obtain reports on RADIUS authentication and accounting details, and payment. Navigate to **Reports** to view the following reports. Click on **Download CSV** to download reports in *.csv* format.

- Summary Report
- Access Report
- Sponsor Activity Report
- Concurrent Users
- User Activity Report
- RADIUS Authentication
- RADIUS Accounting
- Payment

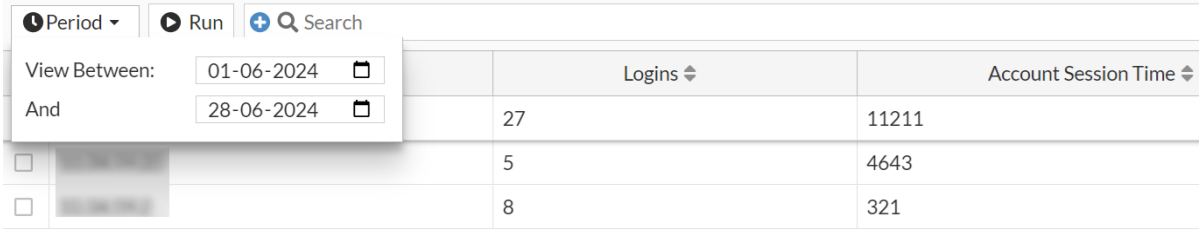
Summary Report

This report displays a summary of the number of guest accounts created, guests that were authenticated, and the total cumulative connected period of the guest accounts. Select a search criteria using the date pickers provided and click **Run**.



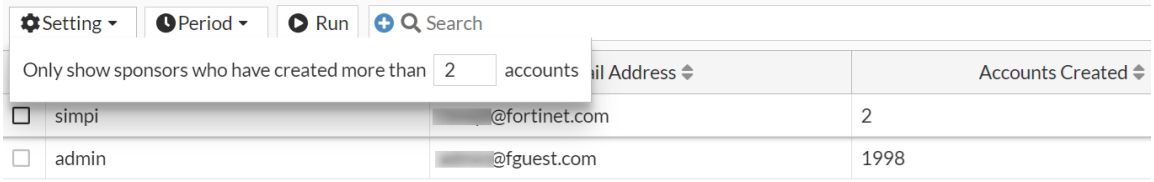
Access Report

The report summarizes the number of logins by the enforcement device (IP Address), and the cumulative duration of connected sessions based on NAS IP/Radius Clients. Select a search criteria using the date pickers provided and click the **Run** button.



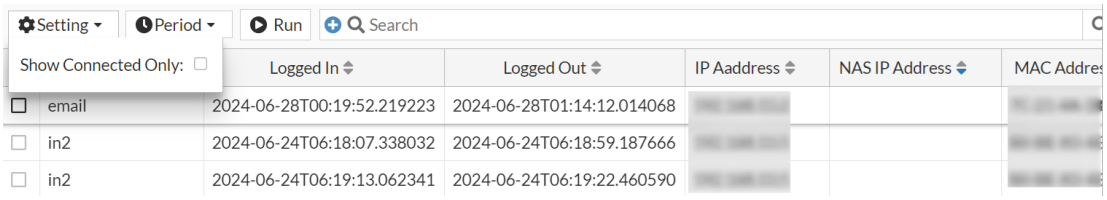
Sponsor Activity Report

This report summarizes the number of accounts created by sponsors based on number of log-ins created. Select a search criteria using the date pickers provided, you can also select a minimum number of accounts created by the sponsor, click **Run**.



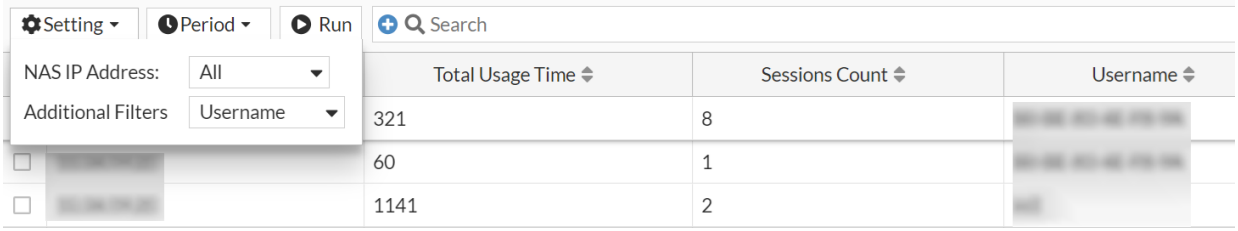
Concurrent Users

This report displays details of users concurrently connected to a network over a specific period, optionally, you can select to view connected users only. Select a search criteria using the date pickers provided and click **Run**.



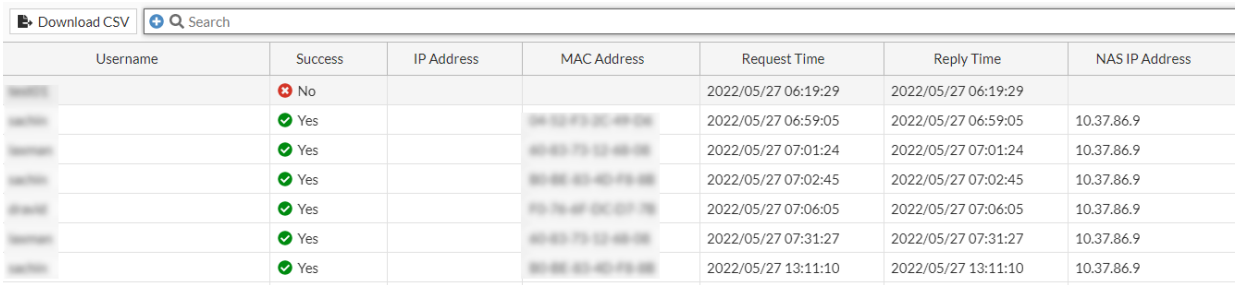
User Activity Report

This report displays guest user activity, such as, the total usage time and sessions count based on AP name, AP ID, and NAS IP address. Select a search criteria using the date pickers provided and click **Run**.



RADIUS Authentication

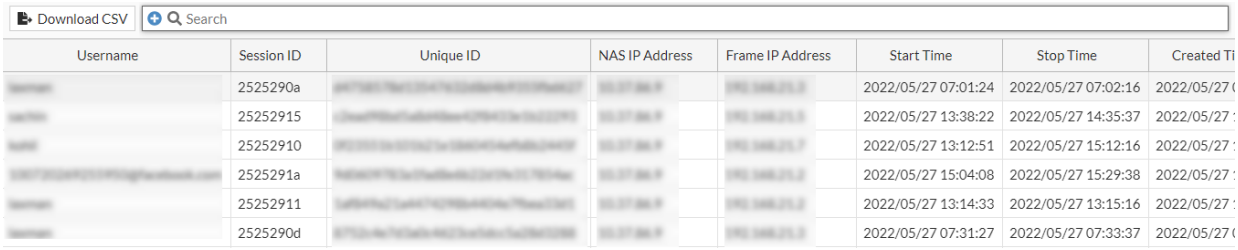
This report displays the successful or failed RADIUS authentications.


Download CSV | Search

Username	Success	IP Address	MAC Address	Request Time	Reply Time	NAS IP Address
[redacted]	No			2022/05/27 06:19:29	2022/05/27 06:19:29	
[redacted]	Yes		[redacted]	2022/05/27 06:59:05	2022/05/27 06:59:05	10.37.86.9
[redacted]	Yes		[redacted]	2022/05/27 07:01:24	2022/05/27 07:01:24	10.37.86.9
[redacted]	Yes		[redacted]	2022/05/27 07:02:45	2022/05/27 07:02:45	10.37.86.9
[redacted]	Yes		[redacted]	2022/05/27 07:06:05	2022/05/27 07:06:05	10.37.86.9
[redacted]	Yes		[redacted]	2022/05/27 07:31:27	2022/05/27 07:31:27	10.37.86.9
[redacted]	Yes		[redacted]	2022/05/27 13:11:10	2022/05/27 13:11:10	10.37.86.9

RADIUS Accounting

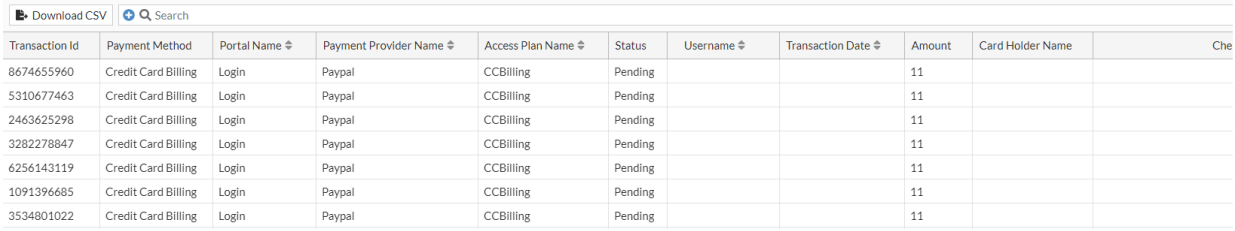
This report displays the status of the RADIUS accounting.


Download CSV | Search

Username	Session ID	Unique ID	NAS IP Address	Frame IP Address	Start Time	Stop Time	Created Ti
[redacted]	2525290a	[redacted]	[redacted]	[redacted]	2022/05/27 07:01:24	2022/05/27 07:02:16	2022/05/27 (
[redacted]	25252915	[redacted]	[redacted]	[redacted]	2022/05/27 13:38:22	2022/05/27 14:35:37	2022/05/27 1
[redacted]	25252910	[redacted]	[redacted]	[redacted]	2022/05/27 13:12:51	2022/05/27 15:12:16	2022/05/27 1
[redacted]	2525291a	[redacted]	[redacted]	[redacted]	2022/05/27 15:04:08	2022/05/27 15:29:38	2022/05/27 1
[redacted]	25252911	[redacted]	[redacted]	[redacted]	2022/05/27 13:14:33	2022/05/27 13:15:16	2022/05/27 1
[redacted]	2525290d	[redacted]	[redacted]	[redacted]	2022/05/27 07:31:27	2022/05/27 07:33:37	2022/05/27 (

Payment

This report displays the credit card billing and PMS payment transactions.


Download CSV | Search

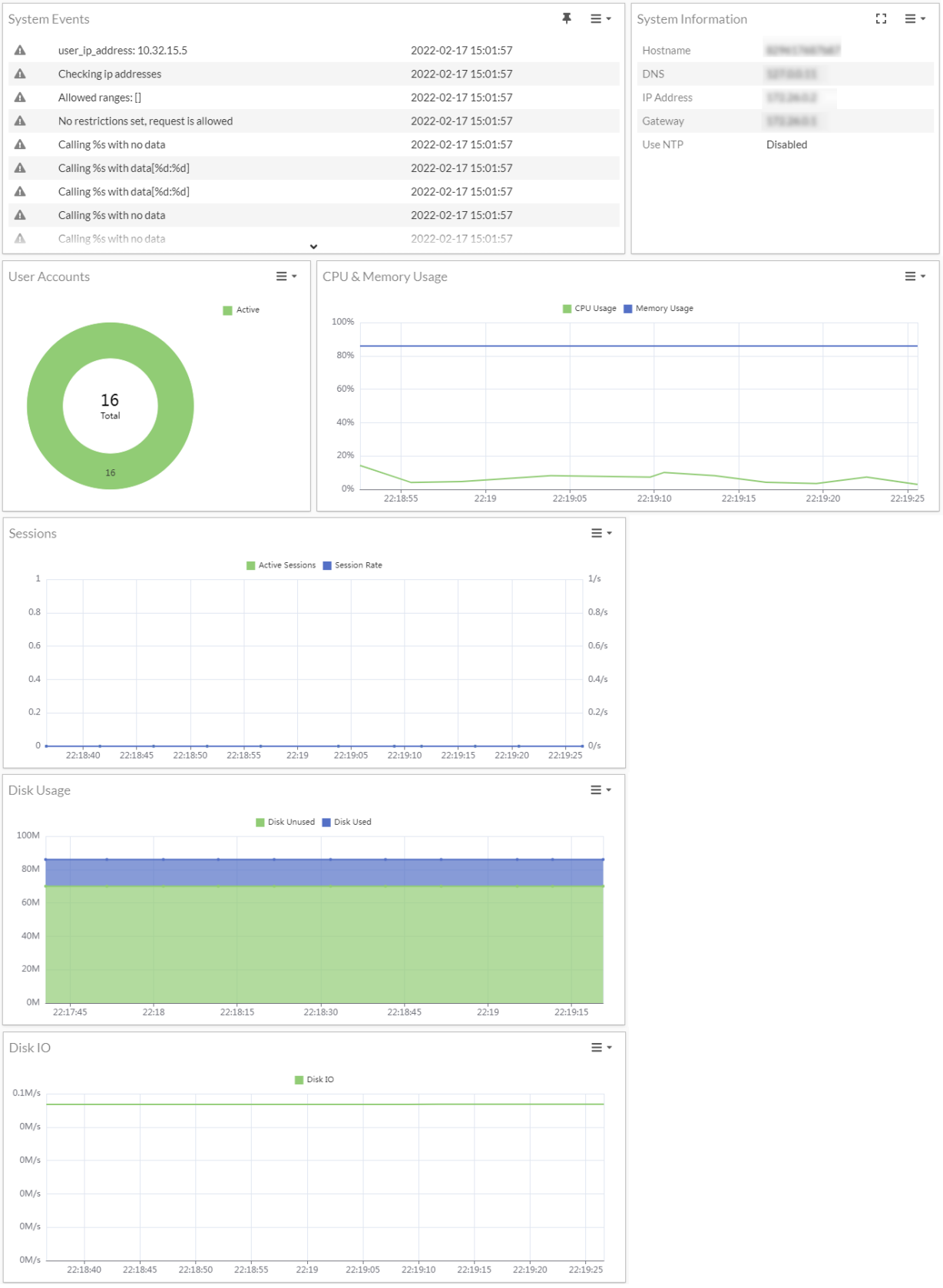
Transaction Id	Payment Method	Portal Name	Payment Provider Name	Access Plan Name	Status	Username	Transaction Date	Amount	Card Holder Name	Che
8674655960	Credit Card Billing	Login	Paypal	CCBilling	Pending			11		
5310677463	Credit Card Billing	Login	Paypal	CCBilling	Pending			11		
2463625298	Credit Card Billing	Login	Paypal	CCBilling	Pending			11		
3282278847	Credit Card Billing	Login	Paypal	CCBilling	Pending			11		
6256143119	Credit Card Billing	Login	Paypal	CCBilling	Pending			11		
1091396685	Credit Card Billing	Login	Paypal	CCBilling	Pending			11		
3534801022	Credit Card Billing	Login	Paypal	CCBilling	Pending			11		

Dashboard

The FortiGuest provides a customizable dashboard that allows you to view and monitor performance data and other statistics. The dashboard provides a graphical representation of data within the administrative scope of the logged in user of the overall system events and statistics, user login sessions, and user accounts. You can also view system information, CPU and memory usage, disk usage, and disk IO of the FortiGuest instance. Navigate to **Home > Dashboard**.

- You can resize all widgets displayed in the dashboard as per your requirement. Click on the menu option and select **Resize**.

- You can configure the display settings for each widget, that is, the time interval to refresh data on the widget. Click on the menu and select **Settings**.


System Events
user_ip_address: 10.32.15.5 2022-02-17 15:01:57
Checking ip addresses 2022-02-17 15:01:57
Allowed ranges: [] 2022-02-17 15:01:57
No restrictions set, request is allowed 2022-02-17 15:01:57
Calling %s with no data 2022-02-17 15:01:57
Calling %s with data[%d:%d] 2022-02-17 15:01:57
Calling %s with data[%d:%d] 2022-02-17 15:01:57
Calling %s with no data 2022-02-17 15:01:57
Calling %s with no data 2022-02-17 15:01:57
System Information
Hostname
DNS
IP Address
Gateway
Use NTP Disabled
User Accounts
Active
16
Total
16
CPU & Memory Usage
CPU Usage
Memory Usage
100%
80%
60%
40%
20%
0%
22:18:55
22:19
22:19:05
22:19:10
22:19:15
22:19:20
22:19:25
Sessions
Active Sessions
Session Rate
1
0.8
0.6
0.4
0.2
0
1/s
0.8/s
0.6/s
0.4/s
0.2/s
0/s
22:18:40
22:18:45
22:18:50
22:18:55
22:19
22:19:05
22:19:10
22:19:15
22:19:20
22:19:25
Disk Usage
Disk Unused
Disk Used
100M
80M
60M
40M
20M
0M
22:17:45
22:18
22:18:15
22:18:30
22:18:45
22:19
22:19:15
Disk IO
Disk IO
0.1M/s
0M/s
0M/s
0M/s
0M/s
0M/s
22:18:40
22:18:45
22:18:50
22:18:55
22:19
22:19:05
22:19:10
22:19:15
22:19:20
22:19:25

www.fortinet.com