

# FortiConnect User Guide

Rel 17.0

2020



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)

# About This Guide

This preface includes the following sections:

- Audience
- Purpose

## Audience

---

This guide is for network administrators who are implementing FortiConnect to manage secure User and Device connectivity on their networks. FortiConnect works alongside Wireless Controllers, LAN Switches, NAC Systems, Firewalls and other Network Enforcement devices which provide the captive portal and enforcement point for User connectivity and Smart Connect functionality for onboarding devices.

## Purpose

---

The FortiConnect Installation and Configuration Guide describes how to install and configure the FortiConnect appliance. It describes the simple initial installation of the appliance via CLI and the configuration and administration of the FortiConnect Portal through the web-based interface.



# Welcome to FortiConnect

FortiConnect is a complete provisioning, management, and reporting system that provides temporary network access for guests, visitors, contractors, consultants, or customers. FortiConnect works alongside Wireless Controllers, LAN Switches, NAC Systems, Firewalls and other Network Enforcement devices which provide the captive portal and enforcement point for User access.

FortiConnect allows any user with privileges to easily create temporary User accounts and sponsor those users for network access. FortiConnect performs full authentication of sponsors, the users who create accounts, and allows sponsors to provide account details to the User by printout, email, or SMS. The entire experience, from user account creation to network access, is stored for audit and reporting.

When User accounts are created, they are stored within the built-in database on the FortiConnect server. When using FortiConnect's built-in database, external network access devices, such as the Wireless LAN Controller, can authenticate users against FortiConnect using the RADIUS (Remote Authentication Dial In User Service) protocol.

FortiConnect provisions the User account for the amount of time specified when the account is created. Upon expiry of the account, FortiConnect 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 should remove the user.

FortiConnect provides vital network access accounting by consolidating the entire audit trail from account creation to actual use of the account so that reports can be performed through a central management interface.

## FortiConnect Concepts

---

FortiConnect makes use of a number of terms to explain the components needed to provide User access.

### The Guest/User

The Guest/User is the person who needs an account to access the network. A Guest or a User normally accesses the network using their own device, connecting to a wired or wireless hotspot provided by an organization. They normally have their browser connection redirected to a portal where they can login by the Network Enforcement Device. Throughout the documentation you will see references to a Guest or a User whereas these are essentially the same person.

## **Sponsor**

The sponsor user is the person who creates the User account. This person is often an employee of the organization that provides the network access. Sponsors can be specific individuals with certain job roles, or can be any employee who can authenticate against a corporate directory such as Microsoft Active Directory (AD).

## **Admin**

The admin user is the administrator who configures and maintains the FortiConnect appliance.

## **Network Enforcement Device**

These devices are the network infrastructure components that provide the network access. Additionally, network enforcement devices are responsible for pushing Users to a captive portal where they can enter their account details. The captive portal can sit on either the Network Enforcement Device, or FortiConnect. When a User enters his or her temporary user name and password, the network enforcement device checks those credentials against the accounts created by the FortiConnect.

## **FortiConnect**

FortiConnect ties together all the pieces of User access. FortiConnect links the sponsor creating the account, the account details passed to the User, the User authentication against the network enforcement device, and the network enforcement device's verification of the User with the FortiConnect. Additionally, FortiConnect consolidates accounting information from network enforcement devices to provide a single point of User access reporting from who created the account, to when the User accessed the network and exactly what they did while on the network.

# Installing FortiConnect

FortiConnect is supported on the following platforms:

- VMware ESXi
- Microsoft Hyper-V
- Linux KVM

The following sections walk you through installing FortiConnect on each of these platforms.

## Prerequisites

---

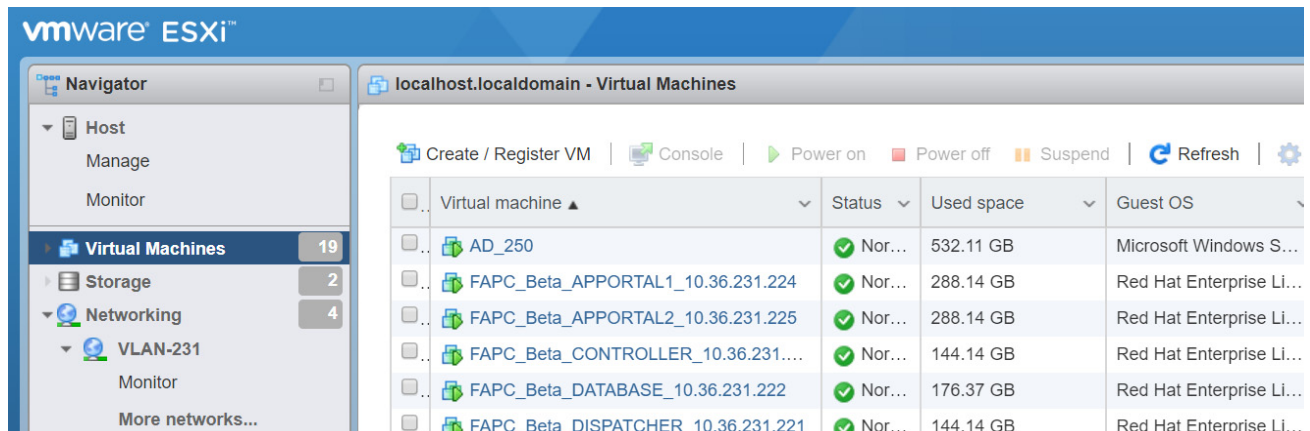
FortiConnect can be installed into a virtual machine. The following platforms are supported for install

- ESXi 6.5 and above
- Microsoft Hyper V on Windows 2008 or later
- Linux KVM virtual server version 1.5.3 and above

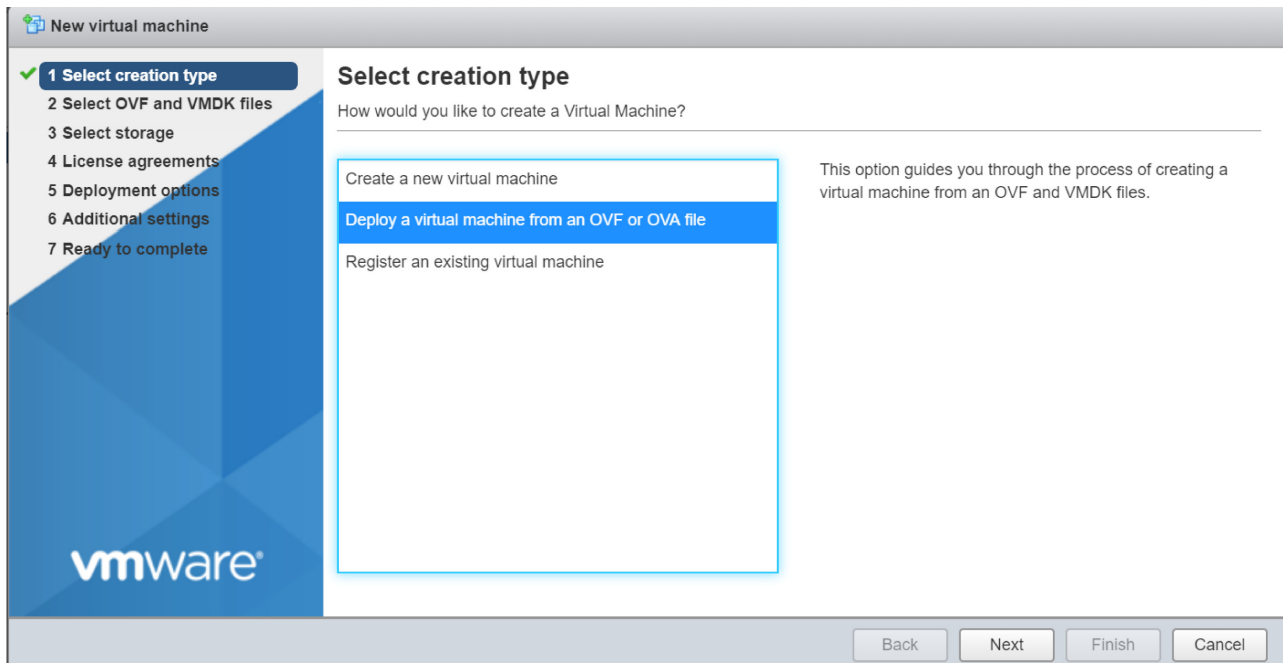
## Installing FortiConnect on VMWare ESXi

---

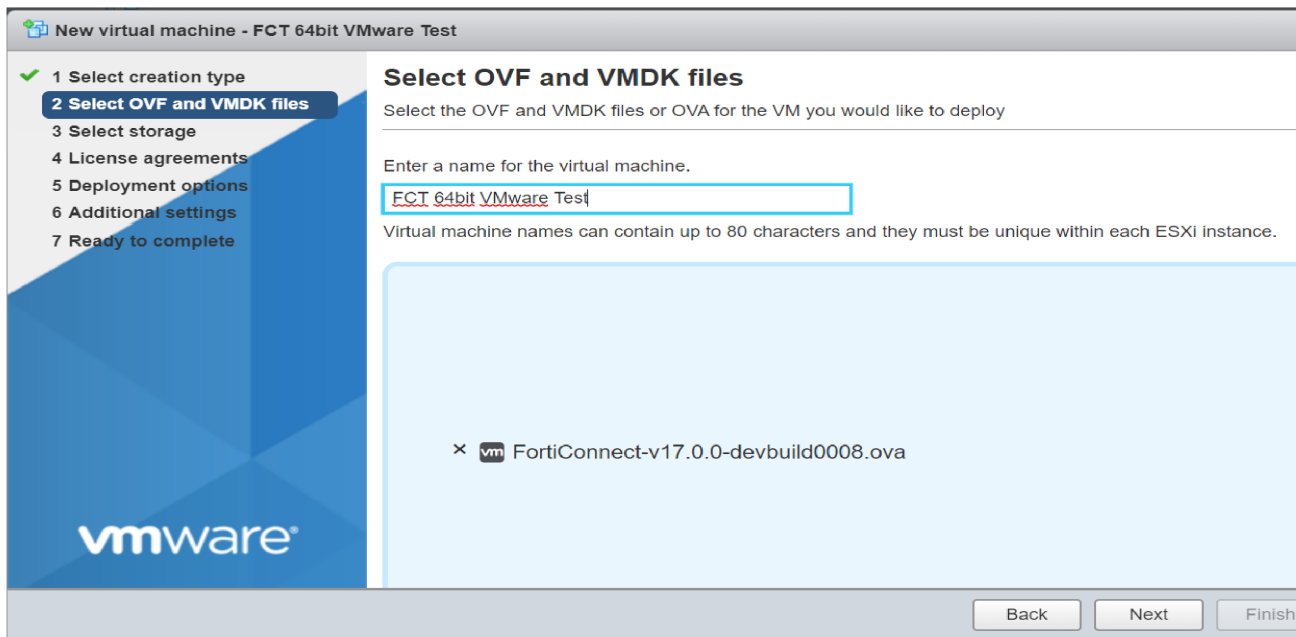
1. Login to your ESXi server.



2. Click **Create/Register VM** to create a new virtual machine and select **Deploy a virtual machine from an OVF or OVA file**. Click **Next**.



3. Enter a name for the new virtual machine and drag/drop the OVA file to deploy the virtual machine. Click **Next**.
4. Modify the **Select Storage** settings, if required. Click **Next**.





5. Click I agree in the License agreements page. Click Next.

New virtual machine - FCT 64bit VMware Test

- 1 Select creation type
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements**
- 5 Deployment options
- 6 Ready to complete

11. Notice to United States Government End Users. The Software and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

12. Free Software. The Software may include software elements that are licensed (or sublicensed) to you under the GNU General Public License (GPL) or other similar free software licenses. The list free software contained in the Software may be viewed in Fortinet's standard product end user license agreement, available at the following web page <http://www.fortinet.com/legal.html>.

13. Audit for Volume Licenses. Fortinet reserves the right to periodically audit you to ensure that you are not using any Software in violation of this Agreement. During standard business hours and upon

vmware

Back Next Finish

6. Select the appropriate Network Mappings as per ESXi configuration and select Thick as the Disk provisioning setting. Click Next.

New virtual machine - FCT 64bit VMware Test

- 1 Select creation type
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements
- 5 Deployment options**
- 6 Ready to complete

### Deployment options

Select deployment options

Network mappings	VM Network	VLAN-226
Disk provisioning	<input type="radio"/> Thin	<input checked="" type="radio"/> Thick
Power on automatically	<input checked="" type="checkbox"/>	

vmware

Back Next Finish

7. Click **Finish**. The new virtual machine is created.


New virtual machine - FCT 64bit VMware Test

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 License agreements
- ✓ 5 Deployment options
- ✓ 6 **Ready to complete**

### Ready to complete

Review your settings selection before finishing the wizard




Product	A Virtual Machine
VM Name	FCT 64bit VMware Test
Disks	FortiConnect-v17.0.0-devbuild0008-disk FortiConnect-v17.0.0-devbuild0008-disk
Datastore	DATA
Provisioning type	Thin
Network mappings	VM Network: VLAN-231
Guest OS Name	Unknown


 Do not refresh your browser while this VM is being deployed.

Back

8. [Optional] Right-click the new virtual machine and select **Edit Settings** to modify configurations. This may not be required as the OVA file has all requisite configurations to set up the virtual machine.

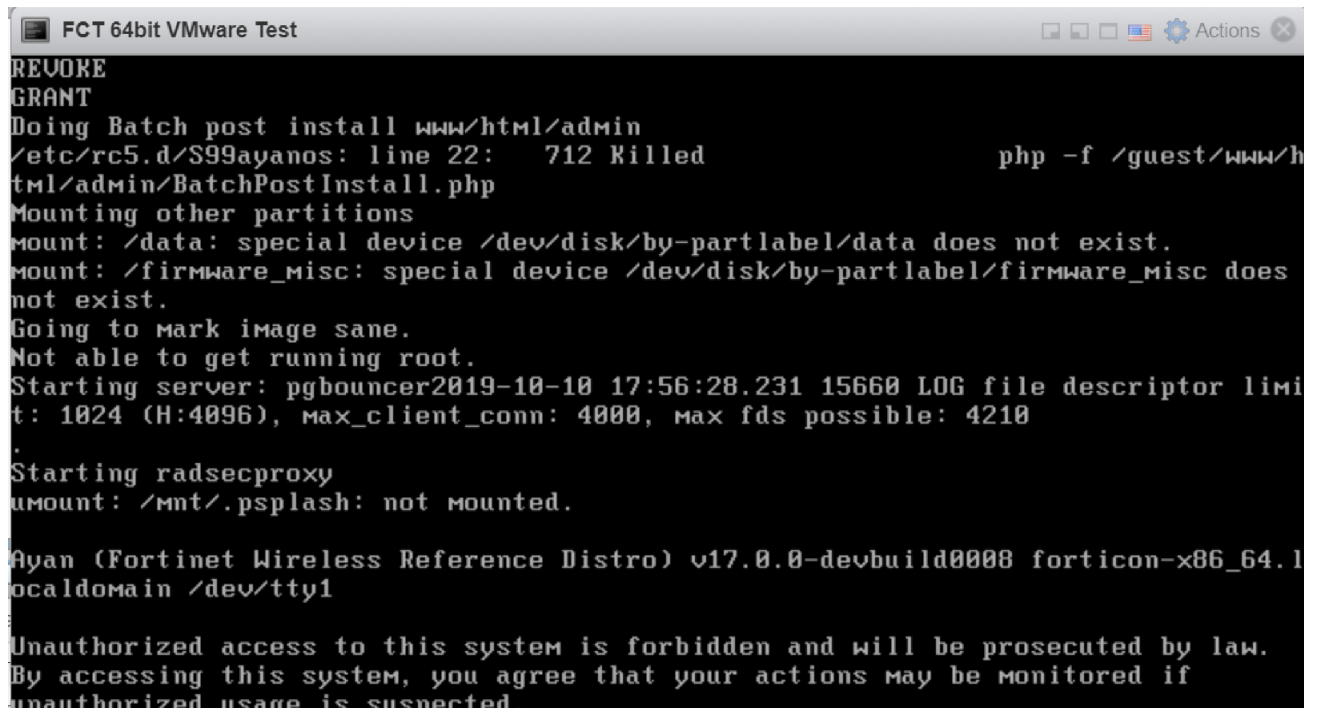
Virtual Hardware VM Options

 Add hard disk  Add network adapter  Add other device

CPU	4	
Memory	4096	MB
Hard disk 1	8	GB
Hard disk 2	500	GB
SATA Controller 0		
Network Adapter 1	VLAN-231	<input checked="" type="checkbox"/> Connect
Floppy drive 1	Use existing floppy image	
Video Card	Specify custom settings	

Save Cancel

9. Right-click the new virtual machine and click **Power On**.



```
REVOKE
GRANT
Doing Batch post install www/html/admin
/etc/rc5.d/S99ayanos: line 22: 712 Killed          php -f /guest/www/html/admin/BatchPostInstall.php
Mounting other partitions
mount: /data: special device /dev/disk/by-partlabel/data does not exist.
mount: /firmware_misc: special device /dev/disk/by-partlabel/firmware_misc does not exist.
Going to mark image sane.
Not able to get running root.
Starting server: pgbouncer2019-10-10 17:56:28.231 15660 LOG file descriptor limit: 1024 (H:4096), max_client_conn: 4000, max_fds possible: 4210
.
Starting radsecproxy
mount: /mnt/.psplash: not mounted.

Ayan (Fortinet Wireless Reference Distro) v17.0.0-devbuild0008 forticon-x86_64.1
localhost /dev/tty1

Unauthorized access to this system is forbidden and will be prosecuted by law.
By accessing this system, you agree that your actions may be monitored if
unauthorized usage is suspected.
```

10. The install can take around 2-3 minutes and may appear to pause at times. When the login prompt appears installation is complete.

Installing VMWare on ESXi 6.7 and above will throw an OS error. This is due to the OVA generated with **Other Linux 3.x 64 bit** as the default setting for backward compatibility to support older versions.



You can either ignore this message or go to **VM Options** and change the OS type to **Other Linux 4.x 64 bit**. To obtain the **Other Linux 4.x 64 bit** option, go to **Edit Settings** and upgrade the VM compatibility.



Power on the virtual machine.

# Installing FortiConnect on Microsoft Hyper-V

FortiConnect can be installed on Microsoft Hyper-V.

1. Open the Hyper-V manager.

The screenshot displays the Hyper-V Manager interface. The main window shows a list of virtual machines under the heading "Virtual Machines". The table below contains the data from this list:

Name	State	CPU Usage	Assigned Memory	Uptime	Status
FCT_Nagraj_17.0	Running	0 %	4096 MB	6:23:08:44	8.0
Scale-Controller1	Running	0 %	4096 MB	56:23:55:56	8.0
Scale-Controller-2	Running	0 %	4096 MB	56:23:56:03	8.0

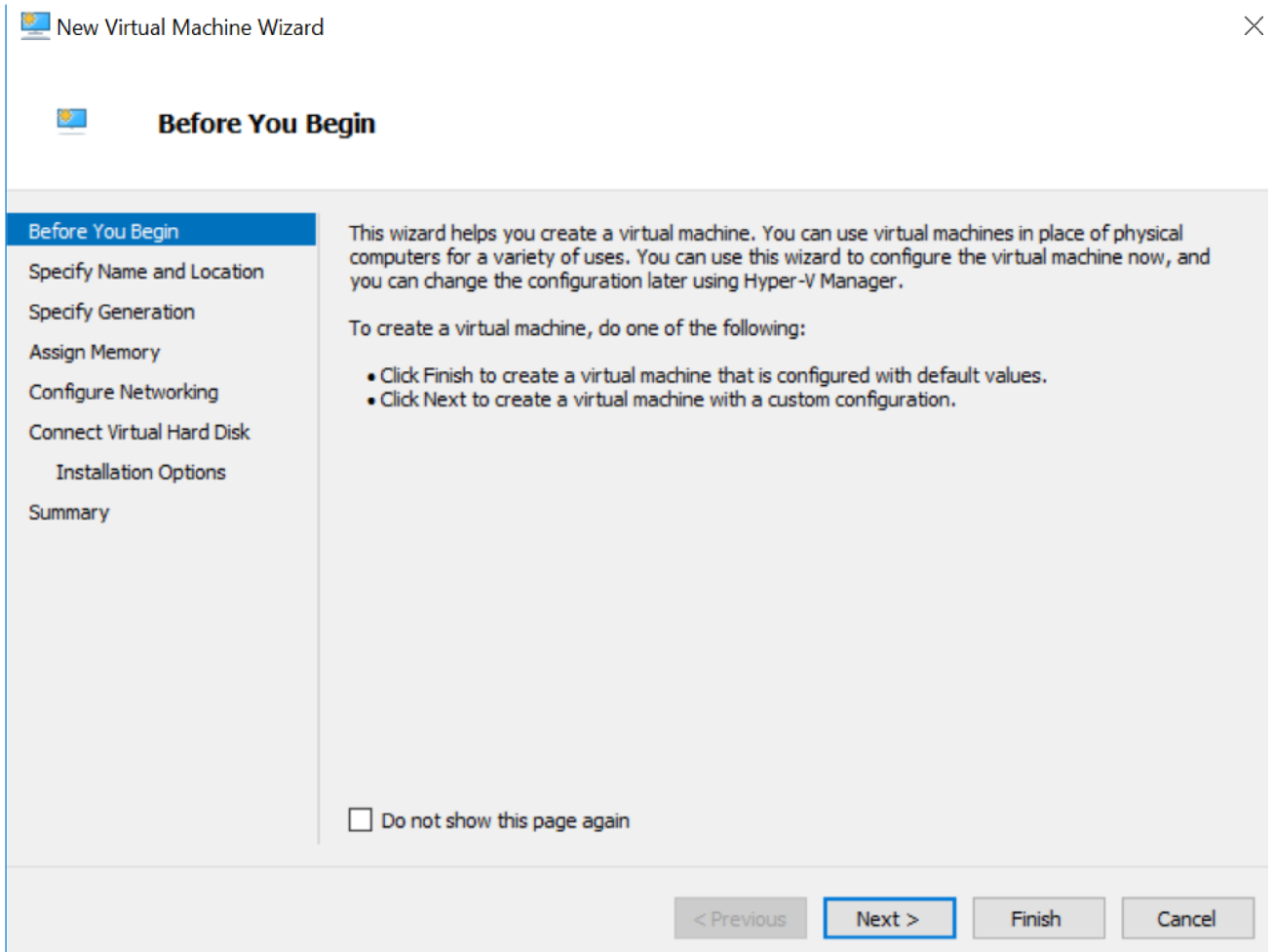
Below the table, the "Checkpoints" section indicates: "The selected virtual machine has no checkpoints."

The bottom section shows details for the selected virtual machine, "FCT\_Nagraj\_17.0":

- Created:** 9/30/2019 4:06:27 PM
- Configuration Version:** 8.0
- Generation:** 1
- Notes:** None
- Clustered:** No
- Heartbeat:** No Contact

At the bottom, there are tabs for "Summary", "Memory", "Networking", and "Replication". On the right side, the "Actions" pane is visible, listing various operations such as "New", "Import Virtual Machine...", "Hyper-V Settings...", "Virtual Switch Manager...", "Virtual SAN Manager...", "Edit Disk...", "Inspect Disk...", "Stop Service", "Remove Server", "Refresh", "View", "Help", "Connect...", "Settings...", "Turn Off...", "Shut Down...", "Save", "Pause", "Reset", and "Checkpoint".

2. To bring up the New Virtual Machine Wizard, click on **New** in the **Actions** column and select **virtual machine**.



3. Click **Next** to create a virtual machine with a custom configuration.

4. Enter a **Name** and select a **Location** for the virtual machine. Click **Next**.

 New Virtual Machine Wizard



## Specify Name and Location

Before You Begin

**Specify Name and Location**

Specify Generation

Assign Memory

Configure Networking

Connect Virtual Hard Disk

Installation Options

Summary

Choose a name and location for this virtual machine.


The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name:

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

Store the virtual machine in a different location

Location:

 If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.


< Previous

**Next >**

Finish

Cancel

## 5. Select **Generation1**. Click **Next**.

 New Virtual Machine Wizard



### Specify Generation

Before You Begin

Specify Name and Location

**Specify Generation**

Assign Memory

Configure Networking

Connect Virtual Hard Disk

Installation Options

Summary


Choose the generation of this virtual machine.

Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

 Once a virtual machine has been created, you cannot change its generation.

[More about virtual machine generation support](#)


< Previous

**Next >**

Finish

Cancel

6. Select the amount of memory you wish to allocate to your virtual machine, a minimum of 4GB is required. Click **Next**.

 New Virtual Machine Wizard



## Assign Memory

Before You Begin

Specify Name and Location

Specify Generation

Assign Memory

Configure Networking

Connect Virtual Hard Disk

Installation Options

Summary

Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory:  MB

Use Dynamic Memory for this virtual machine.

**i** When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

< Previous

Next >

Finish

Cancel



7. The **Connection** is set to your default switch. Click **Next**.  
You can connect to any switch configured in your network.

 New Virtual Machine Wizard



## Configure Networking

Before You Begin

Specify Name and Location

Specify Generation

Assign Memory

**Configure Networking**

Connect Virtual Hard Disk

Installation Options

Summary

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection:

< Previous

**Next >**

Finish

Cancel

8. Select Use an existing virtual hard disk and browse to the Hyper-V disk (.vhd). Click **Next**. The new virtual machine is created.



## Connect Virtual Hard Disk

Before You Begin

Specify Name and Location

Specify Generation

Assign Memory

Configure Networking

Connect Virtual Hard Disk

Summary

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name:

Location:

Browse...

Size:  GB (Maximum: 64 TB)

Use an existing virtual hard disk

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location:

Browse...

Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

< Previous

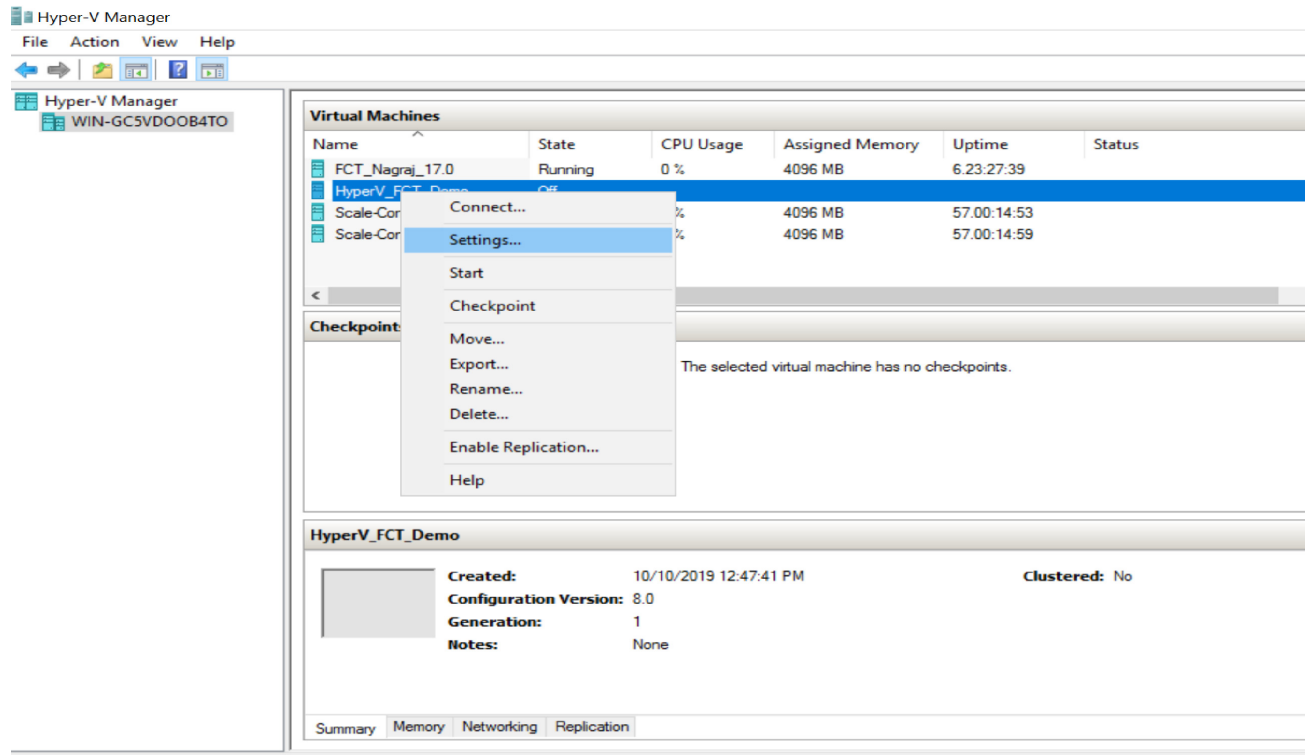
Next >

Finish

Cancel

# Creating a Virtual Disk

1. Right-click the new VM instance and select **Settings**.



2. Select SCSI Controller and select Hard Drive. Click Add.

Settings for HyperV\_FCT\_Demo on WIN-GC5VDOOB4TO

HyperV\_FCT\_Demo

**Hardware**

- Add Hardware
- BIOS  
Boot from CD
- Security  
Key Storage Drive disabled
- Memory  
4096 MB
- Processor  
1 Virtual processor
- IDE Controller 0
  - Hard Drive  
FortiConnect-v17.0.0-dev...
- IDE Controller 1
  - DVD Drive  
None
- SCSI Controller**
- Network Adapter  
Intel(R) 82574L Gigabit Networ...
- COM 1  
None
- COM 2  
None
- Diskette Drive  
None

**Management**

Name  
HyperV\_FCT\_Demo

SCSI Controller

You can add hard drives to your SCSI controller or remove the SCSI controller from the virtual machine.

Click Add to add a new hard drive to this SCSI controller.

Hard Drive  
Shared Drive

Add

You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.

To remove the SCSI controller from this virtual machine, click Remove. All virtual hard disks attached to this controller will be removed but not deleted.

Remove

### 3. Click **New** to create a new virtual hard disk.

Settings for HyperV\_FCT\_Demo on WIN-GC5VDOOB4TO

HyperV\_FCT\_Demo

**Hardware**

- Add Hardware
- BIOS
  - Boot from CD
- Security
  - Key Storage Drive disabled
- Memory
  - 4096 MB
- Processor
  - 1 Virtual processor
- IDE Controller 0
  - Hard Drive
    - FortiConnect-v17.0.0-dev...
- IDE Controller 1
  - DVD Drive
    - None
- SCSI Controller
  - Hard Drive**
    - <file>
- Network Adapter
  - Intel(R) 82574L Gigabit Networ...
- COM 1
  - None
- COM 2
  - None
- Diskette Drive
  - None

**Hard Drive**

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: SCSI Controller Location: 0 (in use)

**Media**

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

Virtual hard disk:

New Edit Inspect Browse...

Physical hard disk:

**i** If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

Remove

4. Select VHDX as the virtual disk format. Click **Next**.

 New Virtual Hard Disk Wizard



## Choose Disk Format

Before You Begin

**Choose Disk Format**

Choose Disk Type

Specify Name and Location

Configure Disk

Summary

What format do you want to use for the virtual hard disk?

VHD

Supports virtual hard disks up to 2,040 GB in size.

VHDX

This format supports virtual disks up to 64 TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012.


< Previous

**Next >**

Finish

Cancel

5. Select **Fixed size** (recommended) as the disk type. Click **Next**.

 New Virtual Hard Disk Wizard



## Choose Disk Type

Before You Begin

Choose Disk Format

**Choose Disk Type**

Specify Name and Location

Configure Disk

Summary

What type of virtual hard disk do you want to create?

Fixed size

This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.

Dynamically expanding

This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual hard disk file that is created is small initially and changes as data is added.

Differencing

This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).


< Previous

**Next >**

Finish

Cancel

6. Enter the **Name** of the virtual hard disk and browse to the **Location** to store it. Click **Next**.

 New Virtual Hard Disk Wizard



## Specify Name and Location

Before You Begin

Choose Disk Format

Choose Disk Type

Specify Name and Location

Configure Disk

Summary

Specify the name and location of the virtual hard disk file.

Name:

Location:



7. Enter the **Size** of the virtual hard disk. The minimum size is 500 GB. Click **Next** and then **Finish**.

New Virtual Hard Disk Wizard



## Configure Disk

Before You Begin

Choose Disk Format

Choose Disk Type

Specify Name and Location

Configure Disk

Summary

You can create a blank virtual hard disk or copy the contents of an existing physical disk.

Create a new blank virtual hard disk

Size:  GB (Maximum: 64 TB)

Copy the contents of the specified physical disk:

Physical Hard Disk	Size
\\.\PHYSICALDRIVE0	299 GB

Copy the contents of the specified virtual hard disk

Path:

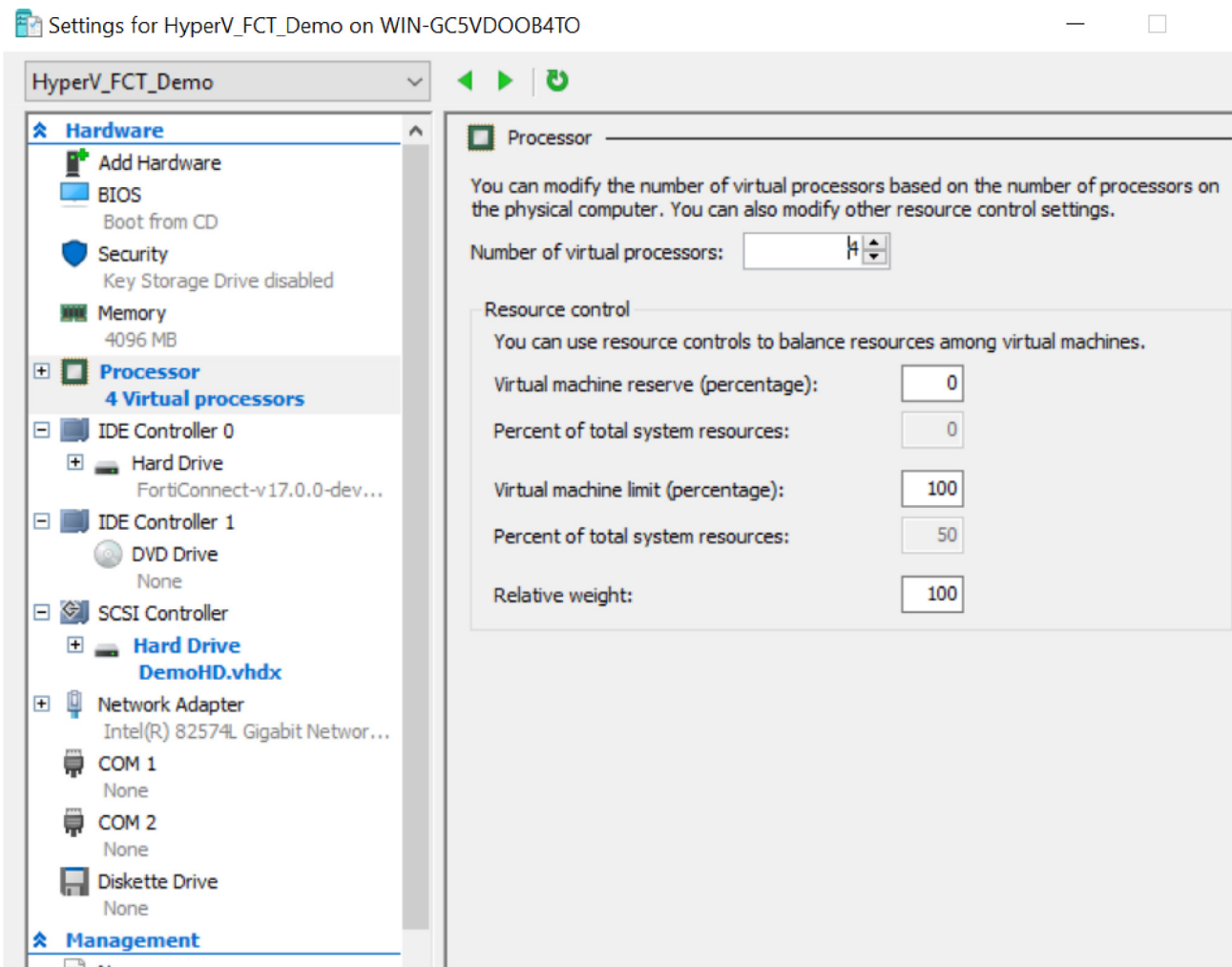
< Previous

Next >

Finish

Cancel

8. Select the **Processor** and enter the **Number of virtual processors**. The minimum supported number of processors is 4. Click **Apply** and then **OK**.



9. Right-click the new VM instance and click **Start**.
10. Ensure that the **Install an operating system later** option is checked then click on **Next**.
11. The install can take around 5-10 minutes and may appear to pause at times. When the login prompt appears installation is complete.


## Installing FortiConnect on Linux KVM

---

FortiConnect can be installed on the Linux KVM virtual server (version 1.5.3).

1. Create a new virtual machine. Enter the name of the VM and select **Import existing disk image**. Click **Forward**.

### New VM ✕

 **Create a new virtual machine**  
Step 1 of 4


Connection: QEMU/KVM

Choose how you would like to install the operating system

- Local install media (ISO image or CDROM)
- Network Install (HTTP, FTP, or NFS)
- Network Boot (PXE)
- Import existing disk image

2. Select the image file (.tar), set the OS type as Linux and the Version as CentOS 6.0 (recommended). Click Forward.

### New VM ✕

 Create a new virtual machine  
Step 4 of 4

Ready to begin the installation

Name:

OS: CentOS 6.0

Install: Import existing OS image

Memory: 4096 MiB

CPUs: 4

Storage: ...rtiConnect-v17.0.0-devbuild0008.img

Customize configuration before install

▼ Network selection

3. Enter the **Memory (RAM)** size and the number of **CPUs**. The minimum required RAM is 4GB and the number of CPUs is 4. Click **Forward**.

### New VM

Create a new virtual machine  
Step 3 of 4

Choose Memory and CPU settings

Memory (RAM):  - +  
Up to 16383 MiB available on the host

CPUs:  - +  
Up to 8 available

4. Enter the **Name** of the new VM and select **Customize configuration before install**. Retain the other default settings. Click **Forward**.

Create a new virtual machine  
Step 4 of 4

Ready to begin the installation

Name: KVMDemo\_FCT

OS: CentOS 6.0

Install: Import existing OS image

Memory: 4096 MiB

CPUs: 4

Storage: ...rtiConnect-v17.0.0-devbuild0008.img

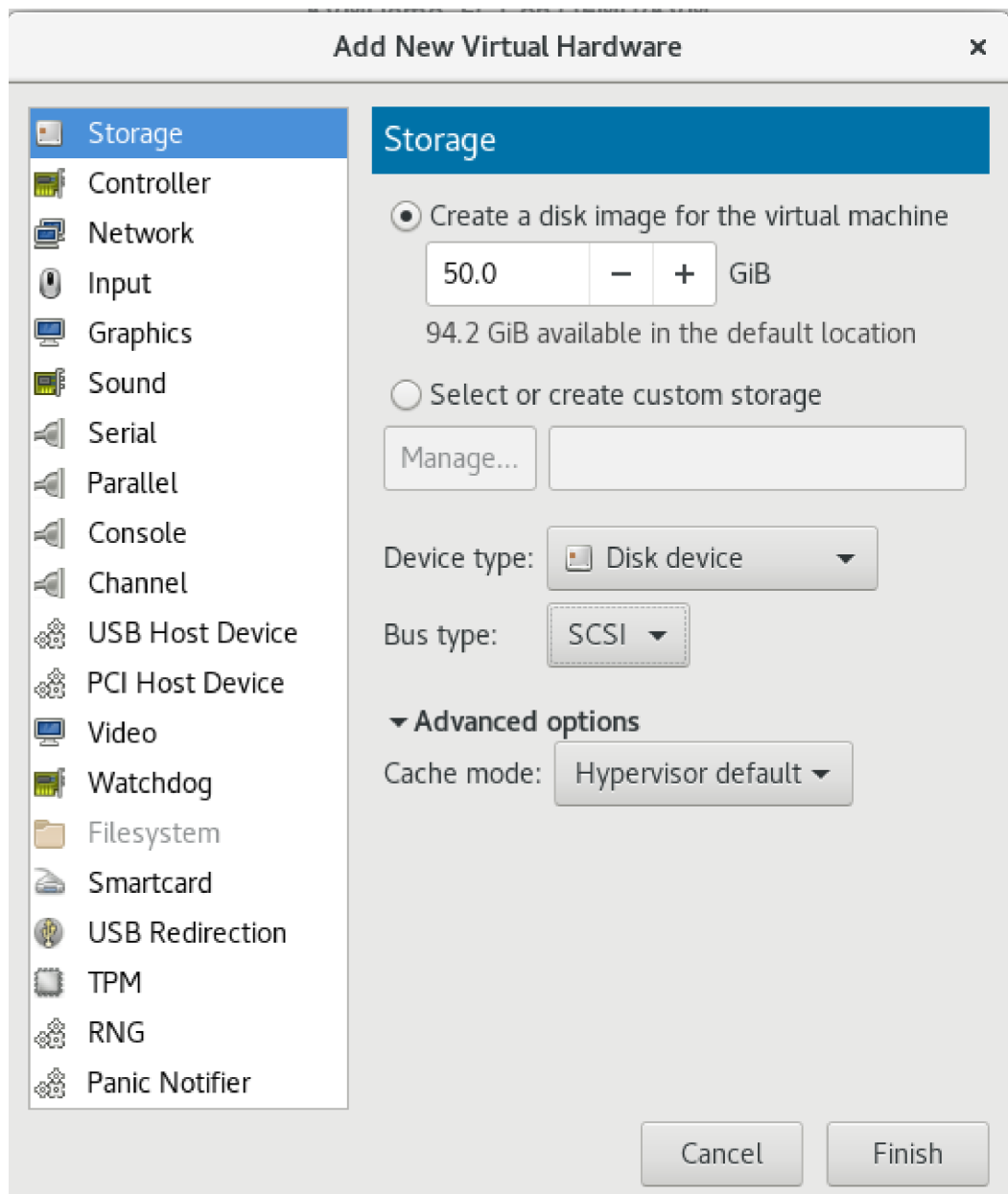
Customize configuration before install

▼ Network selection

Bridge br0: Host device vnet0 ▼

Cancel Back Finish

5. Click **Add Hardware** to create a new hard disk. Enter the required disk size (minimum 500 GB) and select the **Device type** and **Bus type** as **SCSI**.



6. Click **Begin Installation**. The install can take around 5-10 minutes and may appear to pause at times. When the login prompt appears installation is complete.

# Post Installation

---

After successful installation of FortiConnect, configure the network parameters and the DNS server IP address.

Run the `set interface ipv4` and `set interface ipv6` commands configure and IPv4 and IPv6 addresses for the network.

Run the `set interface dns` command configures the DNS server.



FortiConnect is administered using a web interface over either HTTP or HTTPS, or via the FortiConnect CLI. However, after initial installation, the system needs to be configured through the CLI to provide the networking configuration for the appliance so it can be accessed via the web interface to perform other admin tasks.

This chapter includes the following sections:

- Command Line Configuration
- Installing the Product License and Accessing the Administration Interface
- Setup Wizard
- Configuring Network Settings
- Date and Time Settings
- Configuring SSL Certificates
- Configuring Administrator Authentication

## Command Line Configuration

---

This section describes the commands available at the FortiConnect Command Line interface.

### Initial Login

When logging in for the first time after initial installation, you need to set up a password.

1. Connect to the command line interface
2. Login as the admin user. The login user name for the console is admin.
3. Change the password at the admin prompt. Type a password and then confirm the password by re-entering it at the prompt. Once completed you are presented with the CLI administration menu.

# set Commands

## set certs

This command resets certificates; you can generate new temporary certificates and private keys with corresponding certificates.

- The `set certs cert` command generates a new temporary/self-signed certificate.
- The `set certs key` command generates a new private key and the corresponding certificate.

### Syntax

```
set certs cert
```

```
set certs key
```

## set interface

This command configures the network parameters.

- The `set interface ipv4` and `set interface ipv6` commands configure and IPv4 and IPv6 addresses for the network.
- The `set interface dns` command configures the DNS server.

### Syntax

```
set interface ipv4
```

```
set interface ipv6
```

```
set interface dns
```

## set reset

This command resets the admin and sponsor portal settings.

- The `set reset cli-admin-password` command resets the admin CLI password to *admin*.
- The `set reset admin-password` command resets the admin portal user password.
- The `set reset admin-auth-source` command resets the admin authentication source.
- The `set reset allowed-ips` command resets the admin/sponsor portal allowed IP addresses.

### Syntax

```
set reset cli-admin-password
```

```
set reset admin-password
```

```
set reset admin-auth-source
```

```
set reset allowed-ips
```

## set system

This command configure system settings.

- The `set system date`, `set system time`, and `set system timezone` commands set the system date, time, and timezone
- The `set system cli timeout` command sets the CLI idle timeout limit.

### Syntax

```
set system date
set system time
set system timezone
set system cli timeout
```

## request Commands

### request firmware upgrade

This command upgrades the device firmware.

#### Syntax

```
request firmware upgrade <file path>
```

For example, `request firmware upgrade ftp://administrator@dc01.wl-cse.net:/FortiConnect-v17.0.0-build0007.tar.fwout`

### request system

This command requests the system to perform specific tasks such as reboot, halting the system, and drops in system shell.

#### Syntax

```
request system reboot
request system shell
request system halt
```

# show Commands

## show interface

This command displays the system interface configurations such as the configured DNS for the NIC and the configured IPv4 and IPv6 addresses.

The `show interface routing` command displays the network routing table.

### Syntax

```
show interface
```

```
show interface routing
```

## show system

This command displays the system configurations.

- The `show system backups` command displays the available backup files.
- The `show system time` command displays the configured system time.
- The `show system ntp` command displays the NTPD status.
- The `show system process` command displays the processes running on the system.
- The `show system service` command displays the services running on the system and their status.
- The `show system cli timeout` command displays the configured CLI session timeout.

### Syntax

```
show system backups
```

```
show system time
```

```
show system ntp
```

```
show system process
```

```
show system service
```

```
show system cli
```

```
show system cli timeout
```

# debug Commands

Run `debug` at the CLI prompt to enter the debug mode.

## dns-lookup

This command performs a DNS lookup.

- The `dns-lookup lookup/ip lookup/ipv6 lookup` commands perform DNS lookup to determine the IPv4/IPv6 address for the specified host name.
- The `dns-lookup reverse/ip reverse/ipv6 reverse` commands reverse the DNS lookup to determine the host name for the specified IPv4/IPv6 addresses.

### Syntax

```
dns-lookup lookup <hostname>
dns-lookup reverse <ip address>
dns-lookup ip lookup <hostname>
dns-lookup ip reverse <ip address>
dns-lookup ipv6 lookup <hostname>
dns-lookup ipv6 reverse <ip address>
```

## ping

This command tests basic network connectivity to a device.

- The `ping` and `ping ip` commands send ICMP IPv4 messages to network hosts.
- The `ping ipv6` command sends ICMP IPv6 messages to network hosts.
- The `ping arp` command sends ARP requests to the neighboring hosts.

### Syntax

```
ping <ip address>|<hostname>
ping ip <ip address>|<hostname>
ping ipv6 <ip address>|<hostname>
ping arp <ip address>|<hostname>
```

## traceroute

This command prints the route of packets across a network for the specified IP address/host name.

### Syntax

```
traceroute <ip address>|<hostname>
traceroute ip <ip address>|<hostname>
traceroute ipv6 <ipv6 address>|<hostname>
```

# General

## ?

This command displays the list of commands and subcommands available at the command level. Help is available at any level of the CLI by typing ?.

### Syntax

?

## exit

This command exits you from the current CLI mode or from the CLI session.

### Syntax

exit

## help

This command displays help information that describes each command.

### Syntax

help

## history

This command configures the size of the history list, that is, the number of entries the user can navigate back to using the arrow key.

### Syntax

history <size>

## logout

This command logs you out of the current CLI session.

### Syntax

logout

## failsafe Mode

FortiConnect operates in the failsafe mode when it reboots due to issues or is manually booted into the failsafe mode. When booted in the failsafe mode, login using the *admin/admin* username/password combination. The failsafe mode has an idle timeout of 5 minutes.

- The `set reset cli-admin-password` command resets the password.

- The `system check file-system` command checks the file systems for errors.
- The `request system shell` command grants access to the system shell.

### Syntax

```
set reset cli-admin-password
system check file-system
request system shell
```

# Installing the Product License and Accessing the Administration Interface

---

Before accessing the web administration interface of FortiConnect, you need to install a product license.

This section describes the following:

- Obtain and Install a FortiConnect License
- Access the FortiConnect Interface.

## Obtain and Install a FortiConnect License

To obtain a product license please follow the instructions on the Entitlement Certificate that ships with the product.

## Access the FortiConnect Interface

1. If you have installed a license, the admin login is automatically displayed. Otherwise, open a web browser to the FortiConnect Administration interface by entering the IP address that you configured through the command line as the URL, followed by `/admin` :
  - For HTTP access, open `http://<Forticonnect_ip_address>/admin`
  - For HTTPS access, open `https://<Forticonnect_ip_address>/admin`
2. The FortiConnect Administration interface is displayed as shown below. This is the administrator interface to the appliance.
3. Login as the admin user. The default user name/password for the admin console is **admin/admin**.



# FortiConnect Administration

Version: 17.0.0, Build 0007 (GA)

Username:

Password:

Login

**Note:** Fortinet recommends setting up SSL access and also to change the default admin user password for security.

**Note:** Entering the FortiConnect Appliance IP address without the "/admin" as the URL brings up the Sponsor Interface, details about the Sponsor Interface are detailed later in the document.

## Setup Wizard

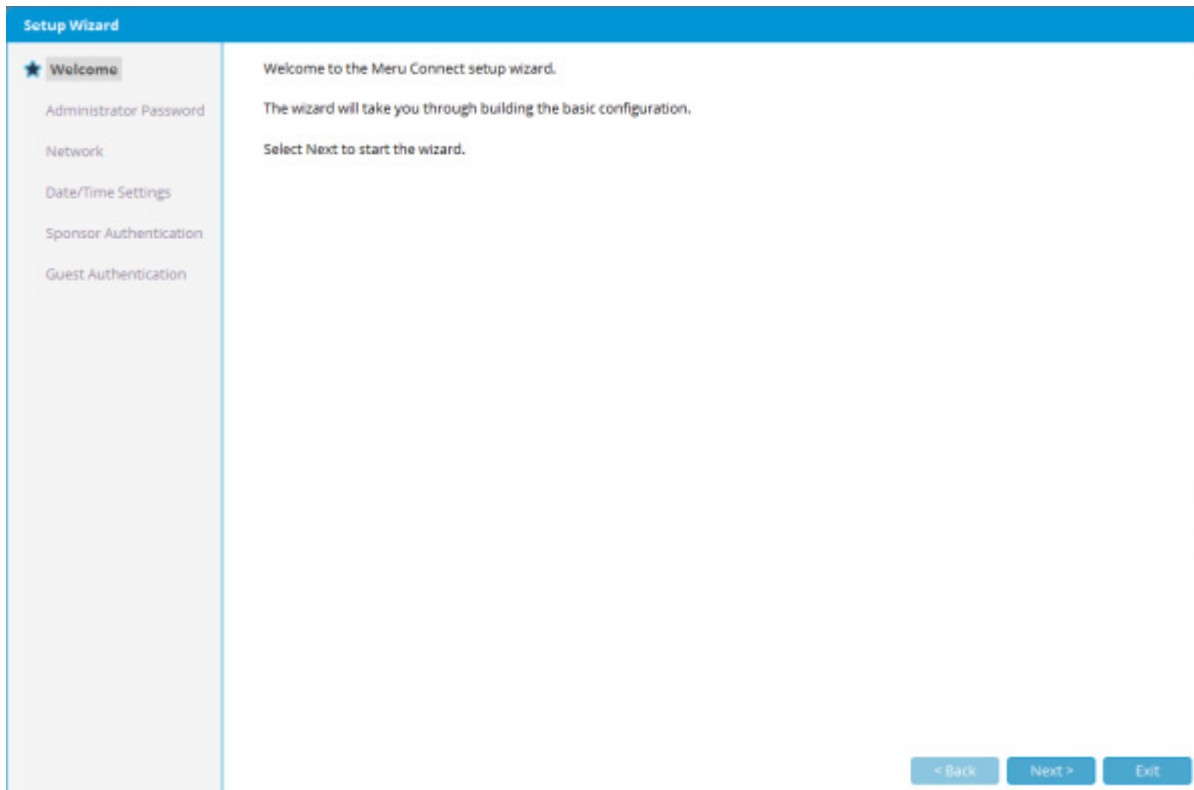
Getting started within FortiConnect is made easy using a Setup Wizard to help configure basic settings before performing any other operations. This minimizes the need to restart the appliance later on.

1. Upon logging into the FortiConnect Administration Interface for the first time the **SetupWizard** will automatically start as seen below.

**Note:** To access the Setup Wizard at anytime after exiting navigate to **Home-->Setup Wizard**

2. Click **Next** to continue.





**Note:** Clicking on the Exit button at anytime will exit the Setup Wizard and any changes made up to that point will be saved.

3. The next step in the Setup Wizard allows you to change the Administrator Password, this must be changed the first time you go through the setup wizard, the Administrator Password is the password for the default admin account. Enter and repeat the new password, or simply leave blank if you wish to keep the existing password.

**Note:** The password must be at least six characters and must contain at least four different characters

4. Click **Next** to continue

Setup Wizard

- ✓ Welcome
- ★ Administrator Password
- Network
- Date/Time Settings
- Sponsor Authentication
- Guest Authentication

In order to continue the default admin password must be changed now.

Admin Password:       Confirm:

Your password must be at least six characters long and contain a minimum of four different characters

< Back      Next >      Exit

5. Now enter any DNS settings in the next step below, you will be required to enter :

- **Hostname** - Hostname of your server
- **Domain** - Domain name
- **Primary DNS** - IP address of Primary DNS server
- **Secondary DNS** - IP address of secondary DNS server

**Note:** If you don't setup a valid DNS server the setup process may take longer as DNS requests time out.

Setup Wizard

- ✓ Welcome
- ✓ Administrator Password
- ★ Network
- Date/Time Settings
- Sponsor Authentication
- Guest Authentication

Hostname:  .localdomain

Domain:

Primary DNS:

Secondary DNS:

< Back   Next >   Exit

6. Click **Next** to continue

7. You will then be required to enter in your Date/Time Settings as shown below, you can manually enter your Date/Time Settings or use an NTP server.

**Note:** Upon changing the date and time settings you will be shown a pop up message saying "Please wait, system services are being restarted". The system is rebooting to allow the date and time settings to take effect.

**Setup Wizard**

- ✓ Welcome
- ✓ Administrator Password
- ✓ Network
- ★ **Date/Time Settings**
- Sponsor Authentication
- Guest Authentication

NTP is used to automatically synchronize your server time. If your organization has its own NTP server(s) you should use them. If not you may be able to use servers from <http://www.pool.ntp.org>.

The system timezone is used by the server administrators (it affects shell logins, system services and the dates displayed in log files).

**Date/Time**

System Date: 1 Dec 2014 📅

05:35:24

System Timezone: America/Los\_Angeles

---

**NTP**

Use NTP to sync System Date & Time:

NTP Server 1: 0.merunetworks.pool.ntp.org

NTP Server 2: 1.merunetworks.pool.ntp.org

NTP Server 3: 2.merunetworks.pool.ntp.org

< Back   Next >   Exit

**NOTE: NTP is automatically used to synchronize server time. If your organization has your own NTP Server (s) use them, if not you may be able to use server (s) from <http://www.pool.ntp.org>.**

- To Manually enter your Date/Time Settings - set the **System Date** using the Date Picker and **System Timezone** from the drop down menu.
- To use an NTP Server - Click inside the check box **Use NTP to sync System Date & Time:** and enter NTP server settings.

8. Click **Next** to continue

9. Then you can set up the Sponsor Authentication, below. Sponsors are users within your organization who are responsible for offering access to guests. Sponsor Authentication settings determine how these Sponsors are authenticated in FortiConnect.

The screenshot shows a 'Setup Wizard' window with a blue header. On the left is a sidebar with a list of steps: 'Welcome', 'Administrator Password', 'Network', 'Date/Time Settings', 'Sponsor Authentication' (highlighted with a star), and 'Guest Authentication'. The main area contains text explaining that sponsors are users within the organization responsible for offering access to guests. It states that after the wizard is complete, additional authentication methods can be specified in the Sponsor Portal. Below this text are two input fields: 'Authentication Type' with a dropdown menu currently set to 'Microsoft Active Directory', and 'Server' with a text box. A label 'Hostname or IP Address' is positioned below the 'Server' text box. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

10. From the **Authentication Type** dropdown menu, select from the following methods of Authentication (for the purpose of documentation the most popular methods have been captured below) :

**Microsoft Active Directory** - Enter Hostname or IP Address. Upon entering this, click Next and you will then be asked to enter more information

- Name - Server name
- Server - Server IP Address
- Domain - Server Domain Name
- Encryption - From the dropdown menu select the required encryption method.
- Base DN - Base DN information

With this information entered, click Next. You will then be prompted to enter the Search Credentials for the Active Directory server. Enter the appropriate Username and Password for your Active Directory server.

**OpenLDAP** - Enter Hostname or IP Address. Upon entering this, click Next and you will then be asked to enter more information

- Name - Server name
- Server - Server IP Address

- Encryption - From the dropdown menu select the required encryption method.
- Base DN - Base DN information

**Novell eDirectory** - Enter Hostname or IP Address

- Name - Server name
- Server - Server IP Address
- Encryption - From the dropdown menu select the required encryption method.
- Base DN - Base DN information

**LDAP** - Enter Hostname or IP Address

- Name - Server name
- Server - Server IP Address
- Encryption - From the dropdown menu select the required encryption method.
- Base DN - Base DN information

**RADIUS** - Enter Hostname or IP Address

- Name - Server name
- Server - Server IP Address
- Port - Port number
- Secret - Secret information, and confirm.

**Internal Sponsor Database**

- First name - First name of Sponsor to be created.
- Last name - Last name of Sponsor to be created.
- Email - Email Address of Sponsor to be created.
- User Name - User Name of Sponsor to be created.
- Password - Password and confirmation.
- Click **Add** to Add Sponsor

**11.** Click **Next** to continue

**Note:** If Sponsor Authentication has already been set up, you will see the screen below.

Setup Wizard

- ✓ Welcome
- ✓ Administrator Password
- ✓ Network
- ✓ Date/Time Settings
- ★ **Sponsor Authentication**

Guest Authentication

Create local sponsors who are permitted to issue guest accounts.

Sponsors					
Username	First Name	Surname	Email	Group	
No sponsors defined					

First Name:

Last Name:

Email:

Username:

Password:  Confirm:

< Back   Next >   Exit

12. Then you can setup User Authentication as per below, Users are authenticated by network devices acting as a policy enforcement point in the network. These are normally the devices that intercept the Users web requests and redirect them to a login page.

The screenshot shows the 'Setup Wizard' interface for Meru Connect. On the left is a vertical navigation pane with the following steps: Welcome, Administrator Password, Network, Date/Time Settings, Sponsor Authentication, and Guest Authentication (which is highlighted with a star). The main content area is titled 'Guest Authentication' and contains the following text: 'Guests are authenticated by network devices acting as the policy enforcement point in the network. These are normally the devices that intercept the guests web requests and redirect them to a login page.' Below this, it states: 'Meru Connect supports authenticating the guests from these devices using RADIUS in the case of wireless controllers, LAN switches, firewalls etc.' and 'Enter the details of the initial device that you would like to authenticate the guests.' There are two input fields: 'Network Device Type:' with a dropdown menu showing 'RADIUS', and 'Network Device:' with a text box. Below the text box is the label 'Hostname or IP Address'. At the bottom right of the wizard are three buttons: '< Back', 'Next >', and 'Exit'.

13. From the **Network Device Type** drop down menu, select which Authentication method you wish to use:

**RADIUS** - Enter the network device's IP Address and click on **Next** to continue.

- Name - Enter the RADIUS Server name
- Network Device IP / mask - Enter the Network Devices Hostname or IP Address
- Secret - Enter the RADIUS Secret and confirm
- Type - From the drop down menu select the type of authentication device being used.
- Description - Enter any description necessary.

14. Click **Next** to complete

15. You have now completed the Setup Wizard, click on **Close** to exit.

## Configuring Network Settings

Any network settings not configured during the Setup Wizard can be setup at any time. To configure remaining network settings follow the steps below:



1. From the administration interface, select **Server > Network Settings** from the left panel to go to the Network Settings page. This page provides all the network settings that can be changed on FortiConnect as shown below.

**Network Settings**

**Hostname**

Hostname: localhost localdomain

Domain: localdomain

---

**DNS**

Primary DNS: 192.168.137.2

Secondary DNS:

---

**IPv4**

IP Address: 192.168.137.20

Subnet Mask: 255.255.255.0

Gateway: 192.168.137.2

---

**IPv6**

Enable:

IP Address:

Prefix Length: 68

Gateway:

You can change the following Network Settings:

- **Hostname**—Assign the name of the appliance as defined in DNS (without DNS suffix).
- **Domain**—Enter the domain name for your organization (e.g. fortinet.com).
- **Primary DNS**—Enter the IP address of the primary DNS server.
- **Secondary DNS**—Enter the IP address of the secondary DNS server.

IPv4 Addresses - Enter your IP Address settings for Networks using IPv4

- **IP Address**—Modify the IP address on the appliance.
- **Subnet Mask**—Enter the corresponding subnet mask.
- **Gateway**—Modify the default gateway for the network to which the appliance is connected.

IPv6 Addresses - Click the **Enable** checkbox if your Network uses IPv6

- **IP Address**—Modify the IP address on the appliance.

- **Prefix Length** - From the drop down list select the Prefix Length.
- **Gateway**—Modify the default gateway for the network to which the appliance is connected.

2. Click the **Save** button to save the changes that you made.

**Note:** For any changes of the Network Settings to take effect FortiConnect requires a restart. Clicking Save will initiate the restart process on FortiConnect within 60 seconds.

## Date and Time Settings

Correct date and time are critical to FortiConnect as FortiConnect authenticates Users based upon the time their accounts are valid. It is important for the time to be correct so that User accounts are Activated and Expired at the correct time. If possible, Fortinet recommends using a Network Time Protocol (NTP) server to synchronize the time and date.

1. From the administration interface, select **Server > Date/Time Settings** to display the Date/Time Settings page as shown below.

The screenshot shows the 'Date/Time Settings' configuration page. It is divided into two main sections: 'Date/Time' and 'NTP'.  
In the 'Date/Time' section, the 'System Date' is set to 1 Dec 2014, and the 'System Timezone' is set to America/Los\_Angeles. The 'System Time' is displayed as 05:49:47.  
In the 'NTP' section, the checkbox 'Use NTP to sync System Date & Time' is currently unchecked. Below it, three NTP server addresses are listed: NTP Server 1, NTP Server 2, and NTP Server 3, all of which are set to 0.merunetworks.pool.ntp.org. At the bottom of the page, there are 'Save' and 'Cancel' buttons.

2. Select the correct **System Date** and **System Time** for the location of your FortiConnect.
3. Select the correct **System Timezone** for the location of your FortiConnect.
4. Click the **Save** button to apply any changes.

**Note:** Changing the System Timezone automatically adjusts the date and time on the FortiConnect appliance and during this time you will be alerted that the change is taking place by a notification -"The application may not respond for a short time while your changes are applied"

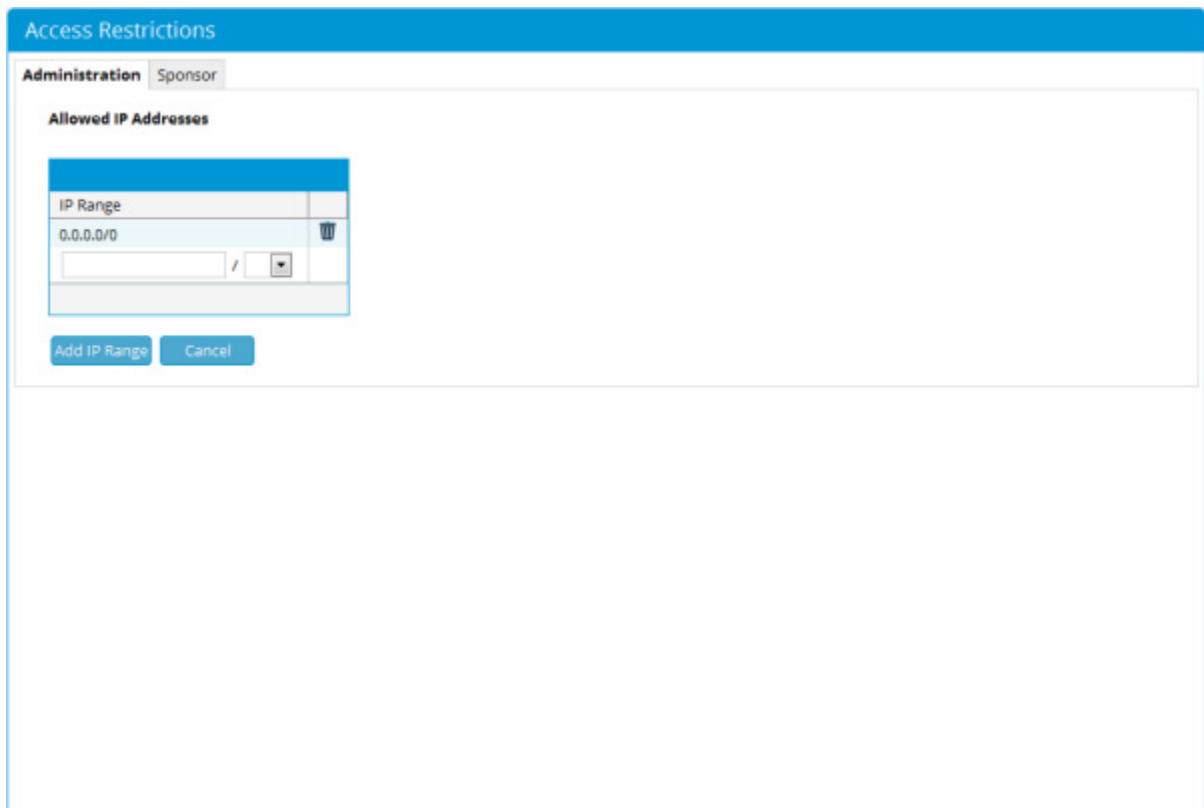
5. If you have one, two or three NTP servers available on the network, click the **Use NTP to set System Date & Time** checkbox.
6. Enter the IP address of each NTP server available into the fields provided.
7. Upon clicking the **Save** button, the system will automatically restart the services and start using NTP.

## Access Restrictions


You can configure FortiConnect to restrict access to only certain IP address ranges for the administration interface and the sponsor interface at any one time.

## Administration Access

1. From the administration interface, select **Server > Access Restrictions** and click the **Administration** tab as shown below.



The screenshot shows the 'Access Restrictions' configuration page in FortiConnect. The page has a blue header with the title 'Access Restrictions'. Below the header, there are two tabs: 'Administration' (which is selected) and 'Sponsor'. Under the 'Administration' tab, there is a section titled 'Allowed IP Addresses'. This section contains a table with one row. The table has two columns: 'IP Range' and a trash icon. The 'IP Range' column contains the text '0.0.0.0/0'. Below the table, there are two buttons: 'Add IP Range' and 'Cancel'.

IP Range	
0.0.0.0/0	

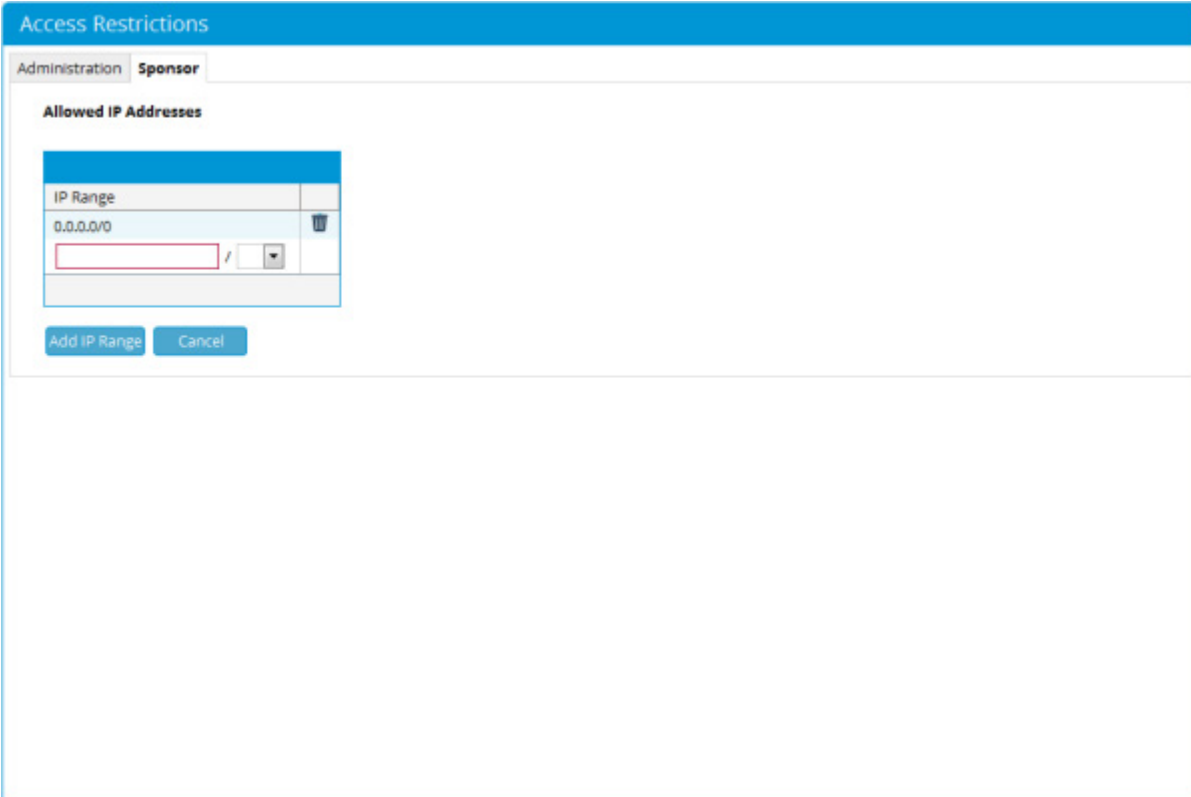
/

2. In the Allowed IP Addresses field, type a range of IP addresses that are allowed access to the FortiConnect Administration interface, and apply a CIDR subnet range using the dropdown menu.
3. Click **Add IP Range** to add the addresses to the list.


**Note:** Leaving the IP Range field blank allows all IP addresses to access the Administration interface, if users have the required admin account permissions.

## Sponsor Access

1. From the administration interface, select **Server > Access Restrictions** and click the **Sponsor** tab as shown below.



The screenshot shows the 'Access Restrictions' configuration page for the 'Sponsor' tab. The 'Allowed IP Addresses' section contains a table with one entry: '0.0.0.0/0'. Below the table are 'Add IP Range' and 'Cancel' buttons.

IP Range	
0.0.0.0/0	
<input type="text"/>	<input type="button" value="v"/>

2. Type the range of IP addresses that are allowed to access the Sponsor interface, and apply a CIDR subnet range using the dropdown menu.
3. Click on **Add IP Range** to add them to the list.

**Note:** Leaving the IP Range field blank allows all IP addresses to access the Sponsor interface, if users have the required sponsor account permissions.

# Configuring SSL Certificates

Both sponsors and administrators can access FortiConnect using either HTTP or HTTPS. For more secure access Fortinet recommends using HTTPS.

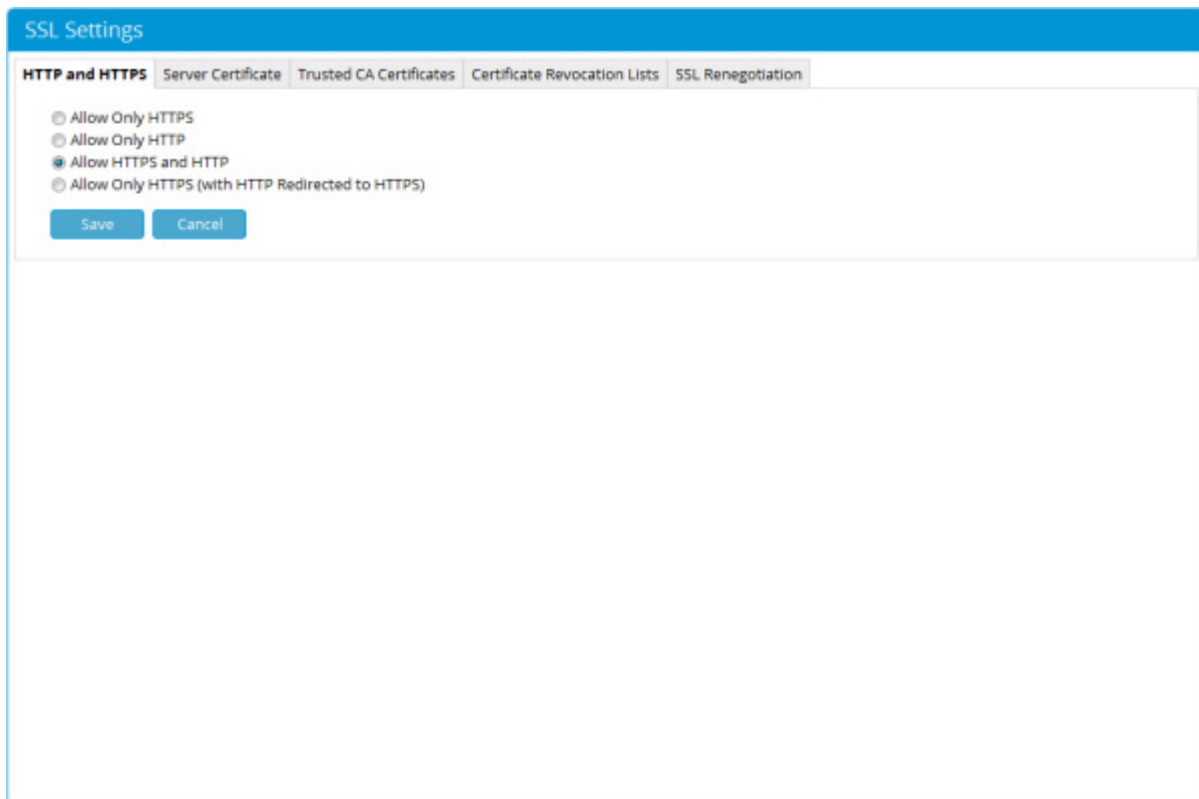
This section describes the following:

- Accessing FortiConnect Using HTTP or HTTPS
- Generating Temporary Certificates/CSRs/Private Key
- Downloading Certificate Files
- Uploading Certificate Files

## Accessing FortiConnect using HTTP or HTTPS

You can configure whether sponsors and administrators access the portal using HTTP, HTTP and HTTPS, or HTTPS only.

1. From the administration interface, select **Server > SSL Settings** from the left panel to display the SSL Settings page as shown below.



The screenshot shows the 'SSL Settings' page in the FortiConnect administration interface. The page has a blue header with the title 'SSL Settings'. Below the header, there are five tabs: 'HTTP and HTTPS', 'Server Certificate', 'Trusted CA Certificates', 'Certificate Revocation Lists', and 'SSL Renegotiation'. The 'HTTP and HTTPS' tab is currently selected. Under this tab, there are four radio button options for configuring access:

- Allow Only HTTPS
- Allow Only HTTP
- Allow HTTPS and HTTP
- Allow Only HTTPS (with HTTP Redirected to HTTPS)

At the bottom of the options, there are two buttons: 'Save' and 'Cancel'.

2. Click on the **HTTP and HTTPS** tab and select from one of the following options:
  - **Allow Only HTTPS**—When selected, only allows HTTPS access to the sponsor and administration interfaces of FortiConnect.
  - **Allow Only HTTP**—When selected, only allows HTTP access to the sponsor and administration interfaces of FortiConnect.
  - **Allow HTTPS and HTTP**—When selected, allows both HTTPS and HTTP access to the sponsor and administration interfaces of FortiConnect.
  - **Allow Only HTTPS (with HTTP Redirected to HTTPS)**—When selected, allows sponsors and administrators to access the portal with HTTPS only, however, sponsors and administrators are redirected via HTTPS if using a standard HTTP connection.
3. When you have made your selection, click the **Save** button.

## Security Assertion Markup Language (SAML) Support

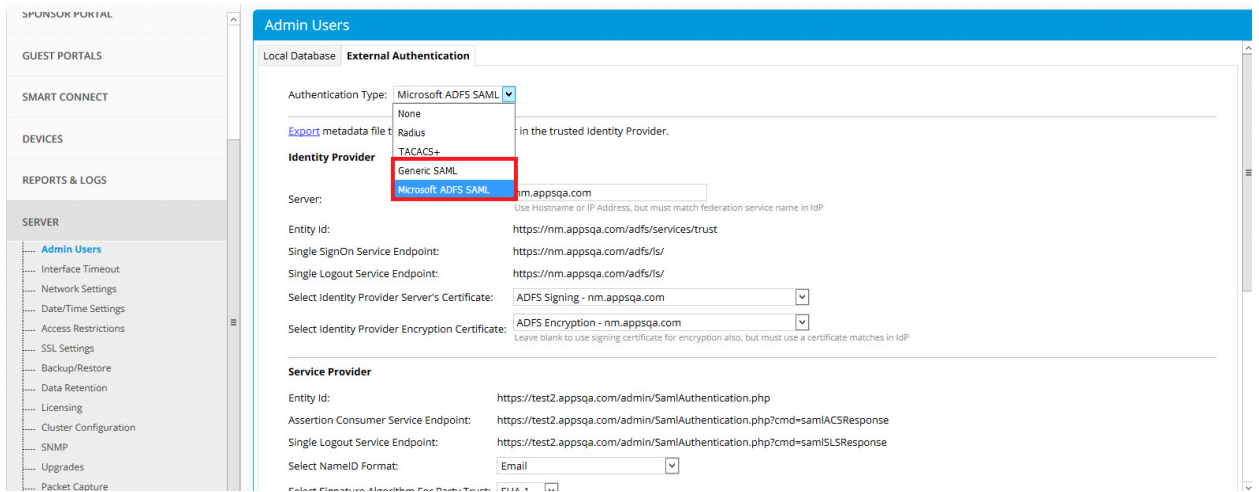
---

You can configure an authentication server that supports the SAML protocol to access the Admin Portal and the Sponsor Portal. A SAML supporting authentication server is the Identity Provider and FortiConnect is the Service Provider.

The FortiConnect login page provides the *Login with SAML* option, when SAML support authentication server is configured. After successful authentication, you can access the FortiConnect portal.

### Admin Users

Navigate to *Server > Admin Users > External Authentication*, select *Microsoft ADFS SAML* or *Generic SAML* as the *Authentication Type*. Configure the related data.



**Identity Provider:** Configures the data FortiConnect 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 FortiConnect is sent.
Single LogOut Service EndPoint	The URL where logout request from FortiConnect is sent.
Select Identity Provider Servers' Certificate	SAML response validators issued by the IDP servers.
Select Identity Provider Encryption Certificate	

**Service Provider** – Configures the data IDP requires connecting to FortiConnect.

Field	Description
Entity ID	The identifier of the FortiConnect.

Assertion Consumer Service Endpoint:	The target URL that specifies where and how messages must be returned.
Single Logout Service Endpoint:	The URL where logout request from is sent.
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.

**Authorization Mode:** Specify the group whose members will have access privileges.

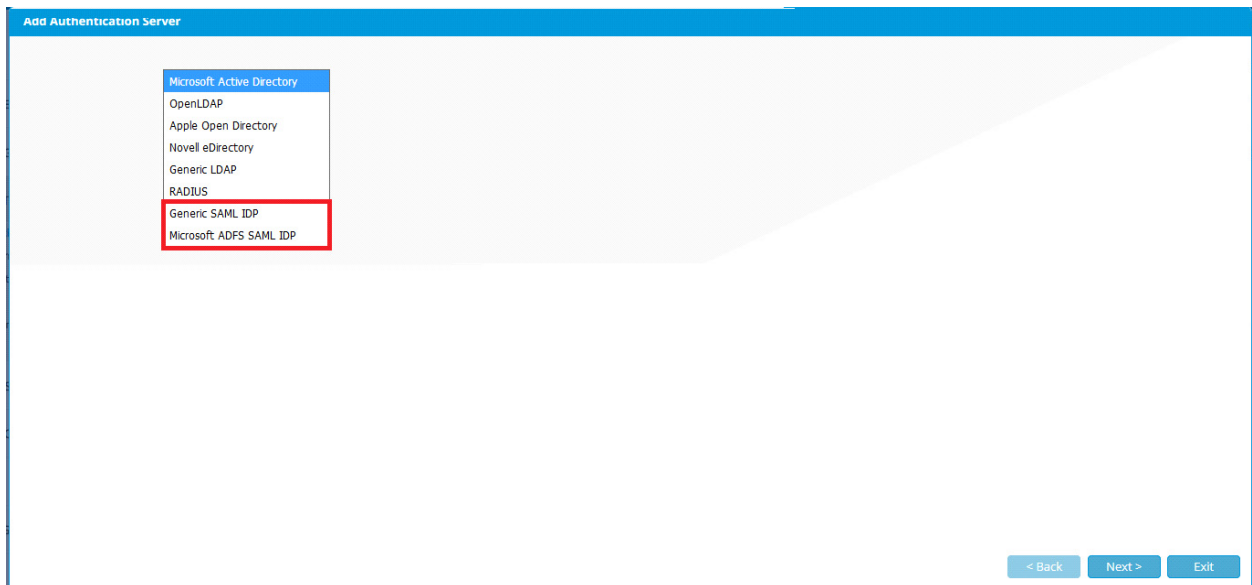
**Group:** Specify the access rights; users are placed in this group when authenticated.

You can export the metadata file to add the Service Provider in the trusted Identity Provider.

## Sponsor Portal

The Sponsor portal authentication allows SAML authentication when adding the authentication server type.

Navigate to *Sponsor Portal > Authentication > Add Authentication Server*.





# Generating Temporary Certificates/CSRs/Private Key

---

FortiConnect generates a default certificate when first installed. If you are planning on using HTTPS, Fortinet strongly recommends generating a new temporary certificate and private key. When doing this, a certificate signing request (CSR) is also generated that can be used to obtain a Certificate Authority (CA) signed certificate.

1. From the administration interface, select **Server > SSL Settings** from the left hand menu. Select the **Server Certificate** tab and click the **Create CSR** link from the section of the page as shown below to bring up the Create CSR form shown below that.

The screenshot displays the 'SSL Settings' page in the FortiConnect administration interface. The 'Server Certificate' tab is selected, showing options for managing certificates. The 'Certificate Signing Request' section includes links for 'Create CSR', 'Create Temporary Certificate from CSR', and 'Download CSR'. The 'Download' section has links for 'Download Current SSL Certificate' and 'Download Current SSL Private Key'. The 'Upload Certificate' section has a file upload field for the server's SSL certificate. The 'Upload Certificate and Private Key' section has separate file upload fields for the server's SSL certificate and private key. At the bottom, there are 'Upload' and 'Cancel' buttons.

SSL Settings

HTTP and HTTPS **Server Certificate** Trusted CA Certificates Certificate Revocation Lists SSL Renegotiation

**Certificate Signing Request**

[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:  No file chosen

**Upload Certificate and Private Key**

Upload this Server's SSL Certificate:  No file chosen

Upload this Server's SSL Private Key:  No file chosen

Create CSR Form

**Create CSR**

HTTP and HTTPS **Server Certificate** Trusted CA Certificates Certificate Revocation Lists SSL Renegotiation

**CSR**

Common Name (FQDN or IP Address):

Organization:

Organizational Unit (Section):

Locality (e.g. City):

State or Province:

Country:

**Private Key Regeneration**

Warning: If you regenerate your private key your current certificate will be replaced by a self-signed temporary certificate

Regenerate Private Key:

2. Provide the details for the temporary certificate and CSR in the Create CSR form:
  - **Common Name (FQDN or IP Address)**—This is either the IP address of FortiConnect or the fully qualified domain name (FQDN) for the FortiConnect appliance. 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 from the dropdown menu.
3. The **Regenerate Private Key** checkbox is optional and should be used if you think your existing private key has been compromised. 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. Select this option to regenerate a private key.
4. Click **Create**.

5. The **Certificate Signing Request** page is again displayed as shown previously. If you chose to regenerate the private key, services will be restarted to enable you to use the new certificate and private key.
6. The **Create Temporary Certificate from CSR** and **Download CSR** options are now available as shown below.

The screenshot shows the 'SSL Settings' interface. At the top, there is a blue header with the text 'SSL Settings'. Below the header, a green checkmark icon is followed by the text 'CSR Created'. A horizontal tab bar contains five tabs: 'HTTP and HTTPS', 'Server Certificate' (which is selected), 'Trusted CA Certificates', 'Certificate Revocation Lists', and 'SSL Renegotiation'. Under the 'Server Certificate' tab, the section is titled 'Certificate Signing Request'. It contains three blue links: 'Create CSR', 'Create Temporary Certificate from CSR', and 'Download CSR'. Below this is a section titled 'Download' with two blue links: 'Download Current SSL Certificate' and 'Download Current SSL Private Key'. The next section is 'Upload Certificate', which has a label 'Upload this Server's SSL Certificate:' followed by a 'Choose File' button and the text 'No file chosen'. The final section is 'Upload Certificate and Private Key', which has two labels: 'Upload this Server's SSL Certificate:' and 'Upload this Server's SSL Private Key:'. Each label is followed by a 'Choose File' button and the text 'No file chosen'. At the bottom of this section are two buttons: 'Upload' and 'Cancel'.

7. Selecting **Create Temporary Certificate from CSR** generates a temporary certificate from the previously requested Certificate Signing Request that you created in Steps 1 to 4.
8. You can download the CSR by clicking the **Download CSR** option as shown above. Once you have sent the CSR to a Certificate Authority and obtained the CA-signed certificate in return, you can upload it by following the instructions in the Uploading Certificate Files section.

**Note:** The installed and generated private keys are 2048 bits in length

## Downloading the Certificate

Fortinet strongly recommends backing up the certificate and private key. The certificate can be downloaded from the administration interface for manual backup to a secure location.

1. From the administration interface, select **Server > SSL Settings** from the left hand menu. Open the **Server Certificate** tab
2. Select **Download Current SSL Certificate** from the Download Certificate section of the page as shown below.

SSL Settings

HTTP and HTTPS **Server Certificate** Trusted CA Certificates Certificate Revocation Lists SSL Renegotiation

**Certificate Signing Request**

[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:  No file chosen

**Upload Certificate and Private Key**

Upload this Server's SSL Certificate:  No file chosen

Upload this Server's SSL Private Key:  No file chosen

3. Save the SSL Certificate to a secure backup location.

## Uploading Certificate and Private Key Files

FortiConnect provides a method of importing/uploading certificate files to the appliance. The Upload Certificates option is used to install a CA-signed certificate or to restore Base 64 PEM format certificate files previously backed up.

**NOTE:** 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 as described in **Downloading Certificate Files**

1. From the administration interface, select **Server > SSL Settings** from the left hand menu. Select the **Server Certificate** tab.
2. View the Upload Certificates section at the bottom of the page as shown below.

The screenshot shows the 'SSL Settings' page with the 'Server Certificate' tab selected. The page is divided into several sections:

- Certificate Signing Request:** Contains links for 'Create CSR', 'Create Temporary Certificate from CSR', and 'Download CSR'.
- Download:** Contains links for 'Download Current SSL Certificate' and 'Download Current SSL Private Key'.
- Upload Certificate:** Includes a label 'Upload this Server's SSL Certificate:' followed by a 'Choose File' button and the text 'No file chosen'.
- Upload Certificate and Private Key:** Includes two labels: 'Upload this Server's SSL Certificate:' and 'Upload this Server's SSL Private Key:'. Each is followed by a 'Choose File' button and the text 'No file chosen'.
- At the bottom of this section are two buttons: 'Upload' and 'Cancel'.

3. Click the **Choose File** button to locate the SSL Certificate file you want to upload and click the **Upload** button.
4. If the private key have been created separately, then you can select them both from different locations and upload them under the **Upload Certificate and Private Key** section on the same page.

WARNING -When uploading a certificate, it must match the private key installed.

## Uploading Trusted CA Certificates

FortiConnect allows you to upload Trusted CA Certificates so that it can trust devices that it makes SSL connections to.

1. From the FortiConnect interface select **Server > SSL Settings** and click on the **Trusted CA Certificates** tab as below.

SSL Settings

HTTP and HTTPS | Server Certificate | **Trusted CA Certificates** | Certificate Revocation Lists | SSL Renegotiation

Showing 1-10 of 19 | 10 per page | Go

Certificate ▲▼	Issued By ▲▼	Expires ▲▼	
<a href="#">Class 3 Public Primary Certification Authority</a>		02-Aug-2028 00:59:59	
<a href="#">Class 3 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - For authorized use only VeriSign Trust Network</a>		02-Aug-2028 00:59:59	
<a href="#">DigiCert High Assurance CA-3</a>	DigiCert High Assurance EV Root CA	03-Apr-2022 01:00:00	
<a href="#">DigiCert High Assurance EV Root CA</a>		10-Nov-2031 00:00:00	
<a href="#">Entrust Certification Authority - L1C</a>	Entrust.net Certification Authority (2048)	10-Dec-2019 21:13:54	
<a href="#">Entrust.net Certification Authority (2048)</a>		24-Dec-2019 18:20:51	
<a href="#">Entrust.net Secure Server Certification Authority</a>		25-May-2019 17:39:40	
<a href="#">Equifax Secure Certificate Authority</a>		22-Aug-2018 17:41:51	
<a href="#">GeoTrust Global CA</a>		21-May-2022 05:00:00	
<a href="#">identitynetworks.com</a>			

Page 1 of 2 | Go

Upload new Root CA:  No file chosen

[Download all certificates](#)

2. Click on the **Choose File** button next to the **Upload new Root CA** option and click on the **upload** button once you have selected the desired Certificate to upload.
3. 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, it is discovered that the Certificate Authority (CA) had improperly issued a certificate, or 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 such as publication of false documents, mis-representation of software behavior, or violation of any other policy 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 (e.g., the token containing the private key has been lost or stolen).

FortiConnect automatically uploads Trusted Certificates to a Revocation List and updates the Certificate at a set specific time period to ensure the Certificate is still valid.

1. The list can be viewed by navigating to **Server --> SSL Settings** and then clicking on the **Certificate Revocation List** tab on the FortiConnect Administration database as shown below.

SSL Settings

HTTP and HTTPS | Server Certificate | Trusted CA Certificates | **Certificate Revocation Lists** | SSL Renegotiation

CRLs are checked when Sponsors or Network Users authenticate using Client Certificates. For security reasons the web service will be stopped if a downloaded CRL expires, this can occur if the Meru Connect does not have internet access.

10 per page

URL ▲▼	Last Update ▲▼	Next Update ▲▼	Status ▲▼
No CRLs installed			

New CRL:   
URL, e.g. http://your.server.com/crl

Update Every:  minutes

2. CRL's can be manually added to this list by entering the URL of the stored CRL into the **New CRL** box.
3. Enter a time value that you wish this CRL to be updated and then click on the **Add** button to add this to the list.

## SSL Renegotiation

In October 2009 a serious SSL vulnerability (CVE-2009-3555) was disclosed that affected Client Certificate authentication on all common web server and browsers. The issue has been addressed by a change to the SSL protocol. FortiConnect has support for the updated protocol but many common browsers do not. To support browsers that have not been updated you can enable the previous behaviour.

From the FortiConnect Administration Interface go to **Server** --> **SSL Settings** and click on the **SSL Renegotiation** tab as shown below.

SSL Settings

HTTP and HTTPS | Server Certificate | Trusted CA Certificates | Certificate Revocation Lists | **SSL Renegotiation**

In October 2009 a serious SSL vulnerability ([CVE-2009-3555](#)) was disclosed that affected Client Certificate authentication on all common web servers and browsers. The issue has been addressed by a change to the SSL protocol. Meru Connect has support for the updated protocol but many common browsers do not. To support browsers that have not been updated you can enable the previous behaviour.

This setting will apply to all web SSL connections to the server.

Allow pre-CVE-2009-3555 SSL Renegotiation

Save Cancel

Click on the **Allow pre-CVE-2009-3555 SSL Renegotiation** box to enable renegotiation. This setting will apply to all web SSL connections to the server.

## Configuring Administrator Authentication

---

FortiConnect has a single default administrator account, called “admin.” The Admin Accounts pages under the Authentication menu allow you to create, edit and delete additional administrator accounts. You can additionally configure FortiConnect to authenticate administrators against an external RADIUS server.

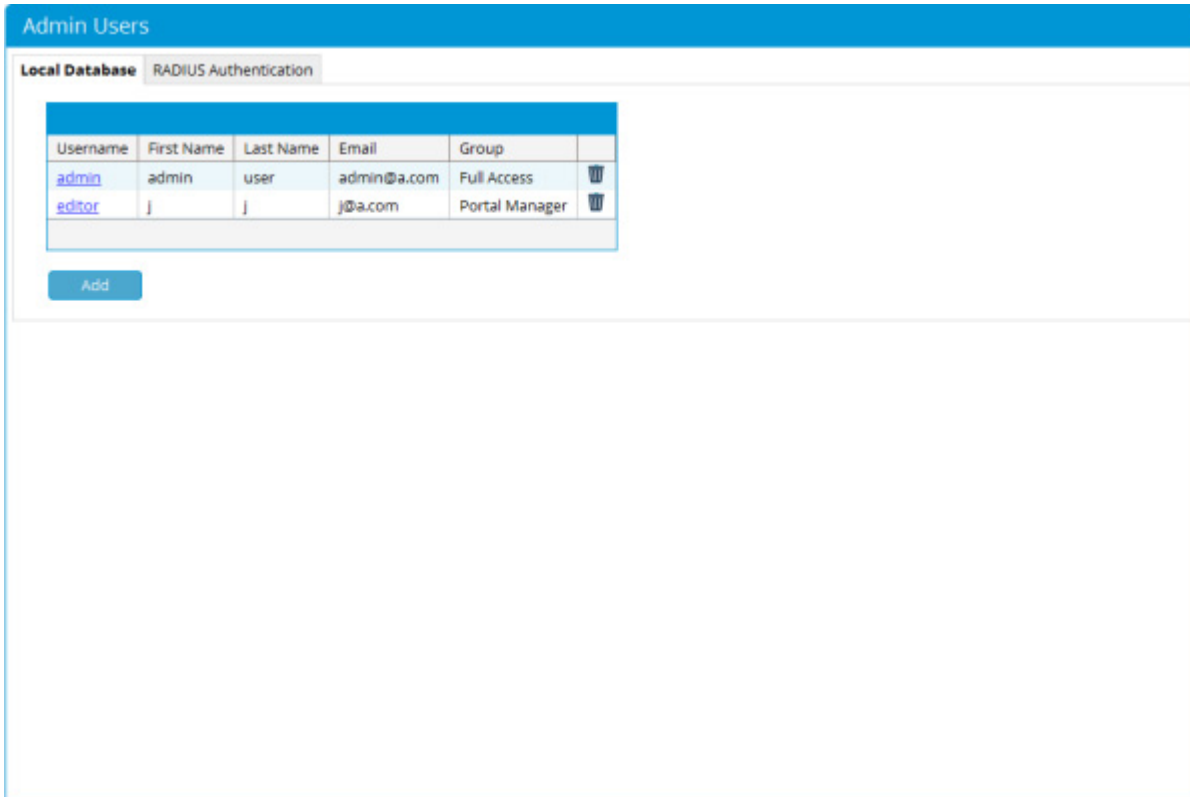
This section describes the following:

- Add New Admin Account
- Edit Existing Admin Account
- Delete Existing Admin Account
- Admin Session Timeout
- Configuring RADIUS for Administrator Authentication





# Add New Admin Account

1. From the administration interface, select **Server > Admin Users** from the left hand menu.
2. In the Local Database tab of the Administrators page as shown below, click the **Add Administrator** button.



The screenshot shows the 'Admin Users' interface. At the top, there is a blue header with the text 'Admin Users'. Below the header, there are two tabs: 'Local Database' (which is selected) and 'RADIUS Authentication'. The main content area contains a table with the following data:

Username	First Name	Last Name	Email	Group	
<a href="#">admin</a>	admin	user	admin@a.com	Full Access	
<a href="#">editor</a>	j	j	j@a.com	Portal Manager	

Below the table, there is a blue button labeled 'Add'.

3. In the Add Administrator page as shown below, enter all the admin user credentials.

## Add Administrator

Username:

First Name:

Last Name:

Email:

Password:  Confirm:   
Your password must be at least six characters long and contain a minimum of four different characters

Group:

- **First Name**—Type the first name of the admin user
- **Surname**—Type the last name of the admin user.
- **Email** —Type the email address of the admin user
- **Username**—Type the user name for the admin account.
- **Password**—Type the password for the admin account.
- **Confirm**—Retype the password for the admin account

**Note:** The password must be at least six characters long and contain at least four different characters

- **Group** - from the drop down menu add your Admin to a group based on access permissions -
  - Ⓢ **Full access** - Full Administration access
  - Ⓢ **Portal Manager** - can only see Portal, Portal Rules, Themes and Hosted Files entries.
  - Ⓢ **Portal Content Editor** - can only edit portal text, images and colours.

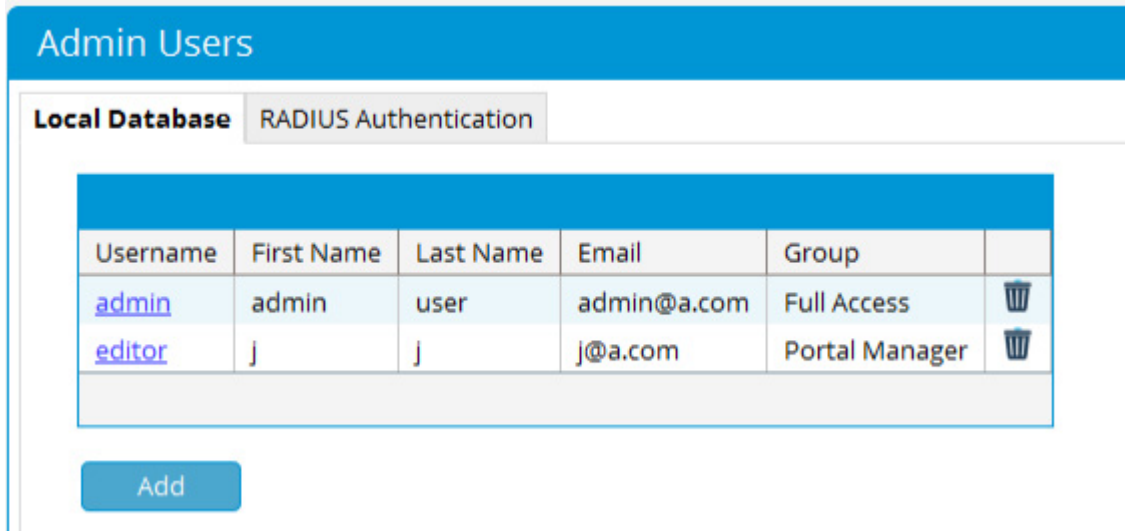
#### 4. Click the **Add** button.

- If there are any errors, the account is not added and an error message is displayed at the top of the page.
- If successfully added, a success message is displayed at the top of the page and you can add additional admin accounts.



# Edit Existing Admin Account

You can modify the settings of admin accounts that already exist.

1. From the administration interface, select **Server > Admin users** from the left hand menu.
2. In the Local Database tab of the Administrators page as shown below, click the username from the list.



The screenshot shows the 'Admin Users' interface. At the top, there is a blue header with the text 'Admin Users'. Below the header, there are two tabs: 'Local Database' (which is selected) and 'RADIUS Authentication'. Under the 'Local Database' tab, there is a table with the following columns: Username, First Name, Last Name, Email, Group, and an action column with a trash icon. The table contains two rows of data. Below the table, there is a blue button labeled 'Add'.

Username	First Name	Last Name	Email	Group	
<a href="#">admin</a>	admin	user	admin@a.com	Full Access	
<a href="#">editor</a>	j	j	j@a.com	Portal Manager	

[Add](#)

3. In the Edit Administrator page as shown below, edit the user credentials.

## Edit Administrator

Username: admin

First Name:

Last Name:

Email:

Password:  Confirm:   
Leave blank to keep existing password

Group:

- **First Name**—Edit the first name of the admin user
- **Surname**—Edit the last name of the admin user.
- **Email** —Edit the email address of the admin user
- **Password**—Edit the password for the admin account.
- **Confirm**—Edit the password for the admin account.
- **Group** - from the drop down menu add your Admin to a group based on access permissions -
  - Ⓢ **Full access** - Full Administration access
  - Ⓢ **Portal Manager** - can only see Portal, Portal Rules, Themes and Hosted Files entries.
  - Ⓢ **Portal Content Editor** - can only edit portal text, images and colours.

**Note:** Leaving the Password and Confirm Password fields empty keeps the existing password.

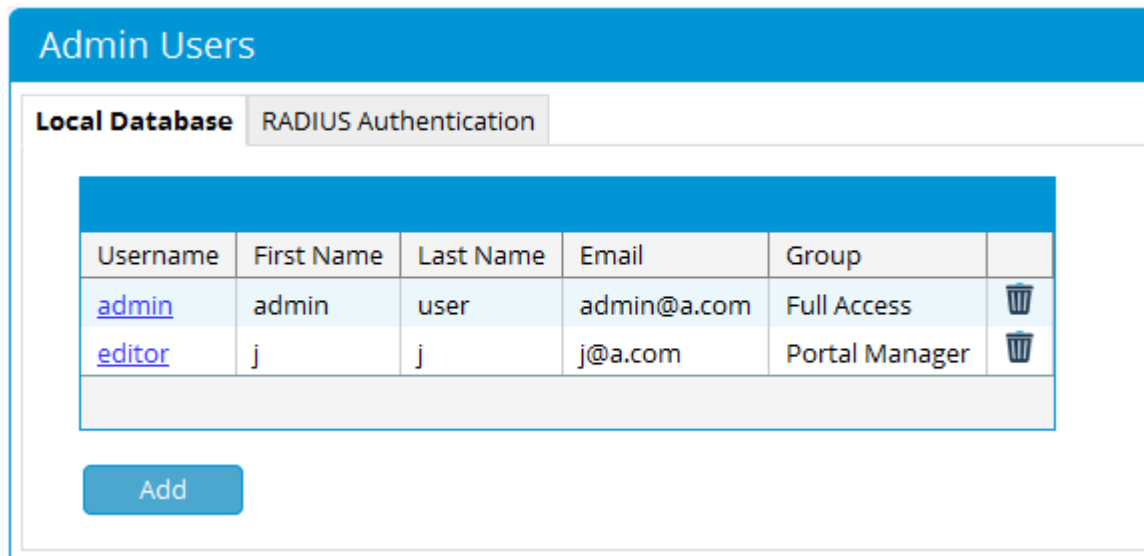
#### 4. Click the **Save Settings** button.

- If there are any errors, the account is not changed and an error message is displayed at the top of the page.
- If successfully changed, a success message is displayed at the top of the page and you can make additional changes to the same admin account.



# Delete Existing Admin Account

You can remove existing admin accounts from the administration interface.

1. From the administration interface, select **Server > Admin Users** from the left hand menu.



The screenshot shows the 'Admin Users' interface. At the top, there is a blue header with the text 'Admin Users'. Below the header, there are two tabs: 'Local Database' (selected) and 'RADIUS Authentication'. A table displays a list of users with columns for Username, First Name, Last Name, Email, and Group. Each user entry has a trash bin icon to its right. Below the table is a blue 'Add' button.

Username	First Name	Last Name	Email	Group	
<a href="#">admin</a>	admin	user	admin@a.com	Full Access	
<a href="#">editor</a>	j	j	j@a.com	Portal Manager	

2. In the Admin Accounts page as shown above, click the **bin** icon at the end of the user entry that you want to delete.
3. When prompted, click **OK** to delete the user or **Cancel** to cancel the deletion. If successfully deleted, a success message is displayed at the top of the page.

## Configuring RADIUS for Administrator Authentication

---

As an alternative to configuring local administrator accounts, you can configure admin users to be authenticated over RADIUS to a RADIUS server. To configure RADIUS authentication for Administrator Authentication, perform the following steps:

1. From the administration interface, select **Server > Admin Users**.

2. Click the **RADIUS Authentication** tab as shown below.

The screenshot shows the 'Admin Users' configuration page with the 'RADIUS Authentication' tab selected. The page is divided into several sections: 'Primary Server', 'Secondary Server', 'Group', and 'Authentication Mode'. The 'Primary Server' section has fields for 'Server IP Address' (10.10.1.38), 'Port' (1812), and 'RADIUS Secret' (with a 'Confirm' field). The 'Secondary Server' section has similar fields. The 'Group' section has a dropdown menu set to 'Portal Content Editor'. The 'Authentication Mode' section has a checkbox for 'Only allow local user authentication if both RADIUS servers cannot be contacted' which is checked. At the bottom, there are 'Save' and 'Cancel' buttons.

3. Type the **Server IP Address** for the Primary RADIUS Server.
4. Type the **Port** that RADIUS authentication is running on for that server (default is 1645 or 1812).
5. In the **RADIUS Secret** field, type the shared secret to be used between the RADIUS Server and FortiConnect.
6. **Confirm** the secret to make sure that it is set correctly.
7. Enter details for a Secondary RADIUS Server. These details are used when FortiConnect does not receive a response from the Primary RADIUS Server. These fields are optional.
8. **Group** - from the drop down menu add your Admin to a group based on access permissions -
  - Ⓢ **Full access** - Full Administration access
  - Ⓢ **Portal Manager** - can only see Portal, Portal Rules, Themes and Hosted Files entries.
  - Ⓢ **Portal Content Editor** - can only edit portal text, images and colours.
9. Check the **Authentication Mode** checkbox so that Local Admin account is only allowed if both the RADIUS Servers cannot be contacted. If this option is unchecked, Local Admin account is allowed if authentication is denied for any one of the RADIUS Servers.

10. Click the **Save** button to save the Administrator RADIUS settings.

**Note:** FortiConnect only allows access to admin users who are successfully authenticated. The RADIUS server must return the IETF Service-Type attribute set to 6 (administrative).

# Configuring TACACS+ for Administrator Authentication

---

Admin authentication can be configured with TACACS+ server. Authentication Type can be None, TACACS+ or RADIUS.

Select **None** if no external authentication (RADIUS or TACACS+) is used and Admin will be authenticated against the local FortiConnect database.

Select **TACACS+** is selected, you must specify a primary server and secondary server. Secondary server will be used if Primary server is not reachable/unable to connect.

Default port number is 49 and Secret can be any string which matches the Secret configured in TACACS+ server. FortiConnect should be added as AAA client in TACACS+ server. Only PAP mode authentication is supported.

The screenshot displays the 'Admin Users' configuration page in FortiConnect. The page is divided into a left sidebar and a main content area. The sidebar contains navigation links: HOME, NETWORK ACCESS POLICY, POLICY SETTINGS, SPONSOR PORTAL, GUEST PORTALS, SMART CONNECT, DEVICES, REPORTS & LOGS, and SERVER. Under the 'SERVER' section, 'Admin Users' is selected. The main content area has a blue header 'Admin Users' and two tabs: 'Local Database' and 'External Authentication'. The 'External Authentication' tab is active. The configuration fields are as follows:

- Authentication Type:** A dropdown menu with 'TACACS+' selected. Other options are 'None' and 'Radius'.
- Primary Server:** A dropdown menu with 'TACACS+' selected (highlighted with a red box).
- Server IP Address:** 172.18.1.5
- Port:** 49
- Secret:** [Empty field] **Confirm:** [Empty field]. Below the fields is the text: 'Leave blank to keep existing secret'.
- Secondary Server:** Fields for Server IP Address, Port, Secret, and Confirm are present but empty.
- Group:** A dropdown menu with 'Full Access' selected.
- Users will be placed in this group when authenticated.**
- Authentication Mode:** (Partially visible at the bottom)

# Data Retention

---

FortiConnect allows you to delete or archive old data from the system, to configure the **settings** from the administration interface go to **Server-->Data Retention**, you will see the screen below.

The screenshot shows the 'Data Retention' configuration page in FortiConnect. It has two tabs: 'Settings' (selected) and 'Schedule'. The 'Settings' section includes:

- Enable:** A checked checkbox.
- Process data older than:** A text input with '1' and a dropdown menu set to 'Days'.
- Policy:** A dropdown menu set to 'Delete only'.
- Server:** A text input field.
- Port:** A text input field.
- Passive Mode:** A checked checkbox.
- Directory:** A text input field.
- Username:** A text input field.
- Password:** A text input field and a **Confirm:** text input field.

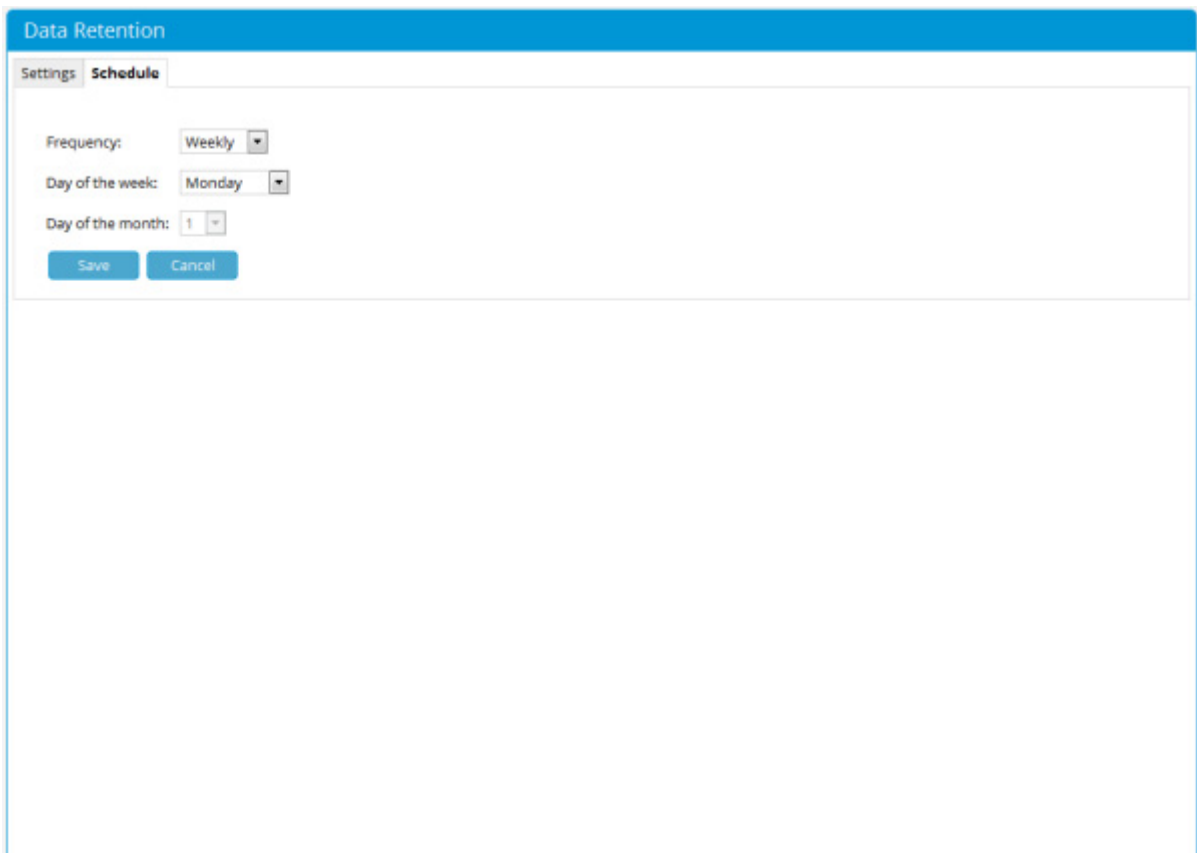
Below these fields are three buttons: 'Save', 'Cancel', and 'Process Now'. A horizontal line separates this section from the 'Unused Accounts' section, which includes:

- Expire inactive for:** A text input with '0' and a dropdown menu set to 'Days'. A blue information icon and the text 'This applies to all accounts' are to the right.
- A 'Process Unused Accounts' button.

1. Click on the **Settings** tab to set the archive details :-
  - Place a check in the **Enable** check box to enable Data Retention.
  - In the **Process data older than** fields use the drop down menu to select whether you wish to process data in **days, weeks, months** or **years**, then enter your desired figure into the field next to it.
  - From the **Policy** drop down menu select whether you wish to **Delete only** (no further action in this section will be needed) or whether you wish to **Archive to FTP and delete**, or **Archive to SFTP and delete**.
2. If you have selected to FTP or SFTP you will be required to enter further information :-
  - In the **Server** field, enter the **IP address** or **hostname** of your server.
  - In the **Port** field, enter the required **port** number.



- in the **Directory** field, enter the required **directory**.
  - In the **Username** field, enter the required **Username**
  - In the **Password** field, enter the required **Password** and then enter again to **Confirm**.
3. Click on **Save** to save your settings, or click on **Process Now** to start the process immediately.
  4. You can expire any **Unused Accounts** if they have been inactive for a certain amount of time.
    - From the drop down menu, choose from years, days, hours or minutes.
    - Enter a specified time in the **Expire inactive for** field
    - Click on **Process Unused Accounts**
  5. To configure the **schedule** from the administration interface go to **Server-->Data Retention**, you will see the screen below.



The screenshot shows a web interface titled "Data Retention" with a blue header. Below the header, there are two tabs: "Settings" and "Schedule", with "Schedule" being the active tab. The "Schedule" tab contains three configuration fields: "Frequency" with a dropdown menu set to "Weekly", "Day of the week" with a dropdown menu set to "Monday", and "Day of the month" with a dropdown menu set to "1". At the bottom of the configuration area, there are two buttons: "Save" and "Cancel".

6. Click on the **Schedule** tab to set the schedule details :-
  - From the **Frequency** drop down menu, select whether the schedule should run **Daily**, **Weekly** or **Monthly**.
  - If necessary, from the **Day of the week** drop down menu, select what day of the week the schedule should run.
  - If necessary, from the **Day of the month** drop down menu, select what day of the month the

schedule should run.

# Managing Sponsor Portals

## Configuring Sponsor Authentication

---

Sponsors are the people who use FortiConnect to create User accounts.

Sponsor authentication authenticates those sponsor users to the Sponsor interface of FortiConnect. There are five options available:

- Local User Authentication—Create local sponsor accounts directly on FortiConnect. See [Configuring Local Sponsor Authentication](#).
- Active Directory Authentication—Authenticate sponsors against an existing Active Directory (AD) infrastructure. See [Configuring Active Directory \(AD\) Authentication](#).
- LDAP Authentication—Authenticate sponsors against a Lightweight Directory Access Protocol (LDAP) server. See [Configuring LDAP Authentication](#).
- Novell eDirectory - Authenticate sponsors against a Novell eDirectory server. See [Configuring Novell eDirectory](#).
- RADIUS Authentication—Authenticate sponsors against a RADIUS server. See [Configuring RADIUS Authentication](#).
- Active Directory Single Sign-On—This option uses Kerberos between the client's web browser and FortiConnect to automatically authenticate a sponsor against an Active Directory Domain Controller. See [Configuring Active Directory Single Sign-On](#).
- Client Certificate Authentication - This option allows a sponsor to present a certificate through their browser to authenticate themselves. Once this has been done the sponsor can be mapped to a role based upon an LDAP server.

You can configure multiple authentication servers in FortiConnect as well as the order in which the authentication servers are used to authenticate sponsors. For details, see [Configuring Sponsor Authentication Settings](#).

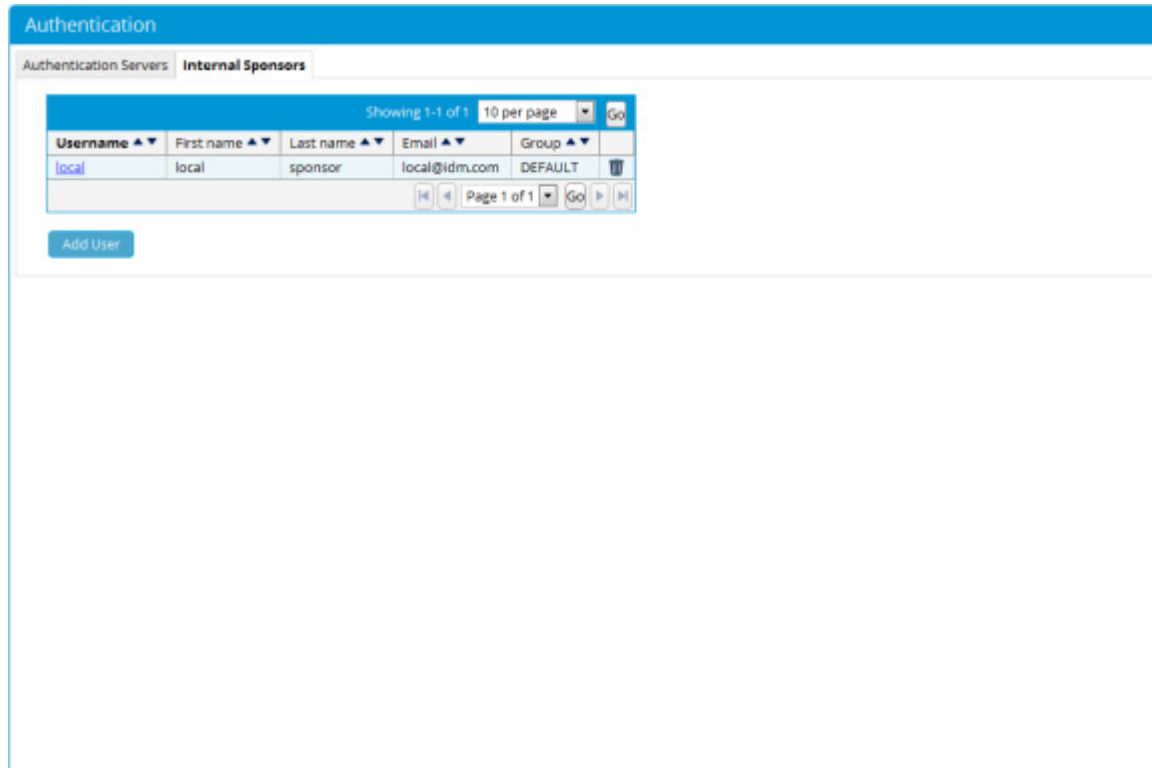
## Configuring Local Sponsor Authentication

Local authentication allows you to set up sponsor user accounts directly on FortiConnect. You can do the following with local authentication:


- Add New Local User Account
- Edit Existing User Account
- Delete Existing User Account

## Adding a Local User Account

1. From the administration interface, select **Sponsor Portal > Authentication** and then click on the **Internal Sponsors** tab from the menu as shown below.



The screenshot shows the 'Authentication' section of an administration interface, specifically the 'Internal Sponsors' tab. The page displays a table with one user account listed. The table has columns for Username, First name, Last name, Email, and Group. Below the table is a pagination control showing 'Page 1 of 1' and a 'Go' button. An 'Add User' button is located below the table.

Username ▲▼	First name ▲▼	Last name ▲▼	Email ▲▼	Group ▲▼	
local	local	sponsor	local@idm.com	DEFAULT	

Showing 1-1 of 1 | 10 per page | Go

Page 1 of 1 | Go

Add User

2. Click the **Add User** button to bring up the local sponsor configuration page as shown below.

**Add User**

Username:

Password:  Confirm:

Your password must be at least six characters long and contain a minimum of four different characters.

First Name:

Last Name:

Email:

Group:

3. In the Add a Local User Account page, enter all the sponsor user credentials:

- **Username** - Type the sponsors username.
- **Password** - Enter the sponsors password.
- **Confirm** - Confirm the sponsors password.

**Note:** The password must be at least six characters and must contain at least four different characters

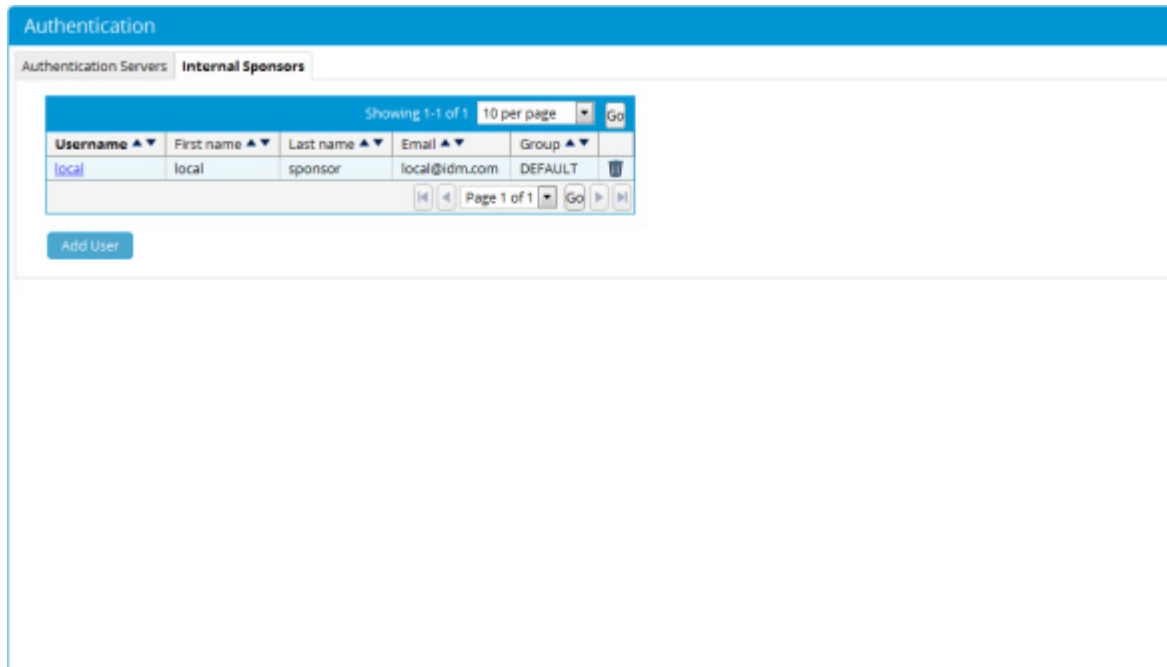
- **First Name**—Type the first name of the sponsor.
- **Last Name**—Type the last name of the sponsor.
- **Email** —Type email address of the sponsor.
- **Group**—Select the group for the sponsor account from the dropdown.

4. Click the **Save** button.

- If there are any errors, the account is not added and an error message is displayed at the top of the page.
- If successfully added, a success message is displayed at the top of the page and you can add additional user accounts.

## Editing a Local User Account

1. From the administration interface, select **Sponsor Portal > Authentication** and then click on the **Internal Sponsors** tab from the menu as shown below.



2. Click on the link of the sponsor you wish to edit, this will bring up the Edit User page as shown below.

**Edit User**

Username:

Password:  Confirm:

Leave blank to keep existing password

First Name:

Last Name:

Email:

Group:

3. In the Edit User page, enter all the sponsor user credentials:

- **Username** - Type the sponsors username.
- **Password** - Enter the sponsors password.
- **Confirm** - Confirm the sponsors password.

**Note:** Leave passwords blank to retain current password.

- **First Name**—Type the first name of the sponsor.
- **Last Name**—Type the last name of the sponsor.
- **Email** —Type email address of the sponsor.
- **Group**—Select the group for the sponsor account from the dropdown.

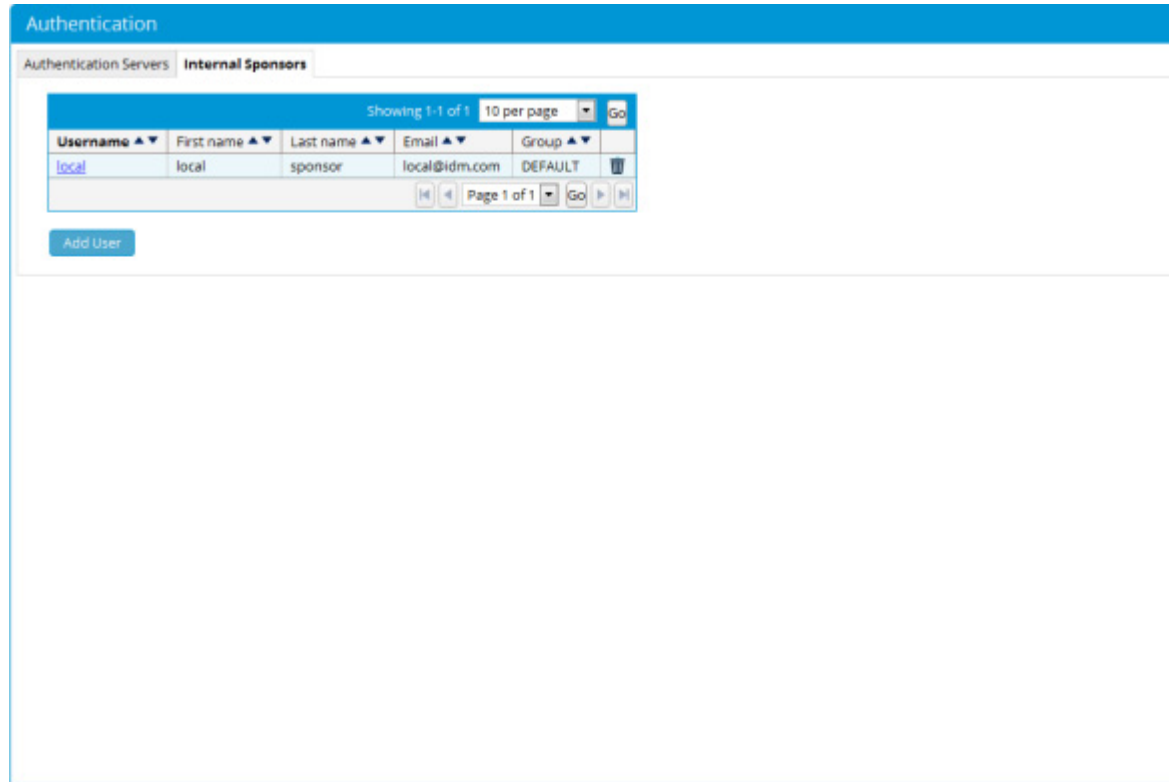
4. Click the **Save** button.

- If there are any errors, the account is not added and an error message is displayed at the top of the page.
- If successfully added, a success message is displayed at the top of the page and you can add additional user accounts.

## Deleting a Local User Account

You can delete existing sponsor user accounts from the administration interface.

1. From the administration interface, select **Sponsor Portal > Authentication** and then click on the **Internal Sponsors** tab from the menu as shown below.



2. A list of local users appears on the page. Choose the user you wish to delete by clicking the **dustbin** icon to the right of the **Group** field.
3. Confirm deletion of the user at the prompt.
  - If successfully deleted, a success message is displayed at the top of the page and you can perform additional local user account operations.

## Configuring Active Directory (AD) Authentication

Active Directory authentication authenticates sponsor users to FortiConnect using their existing AD user accounts. The sponsors need not have another set of user names and passwords to authenticate to the FortiConnect appliance. It also enables the administrator to quickly roll out User Access because there is no need to create and manage additional local sponsor accounts.

Active Directory authentication allows you to do the following:

- Add Active Directory Domain Controller
- Edit Existing Domain Controller
- Delete Existing Domain Controller Entry



AD authentication supports authentication against multiple domain controllers. The domain controllers can be part of the same Active Directory to provide resilience, or they can be in different Active Directories. FortiConnect can authenticate sponsor users from separate domains, even where no trust relationship is configured.

All Active Directory authentication are performed against individual domain controller entries.

FortiConnect attempts to authenticate sponsors against each Domain Controller entry according to the Authentication Order (specified in Configuring Sponsor Authentication Settings).

**Note:** If below security settings are present in Domain Controller Security

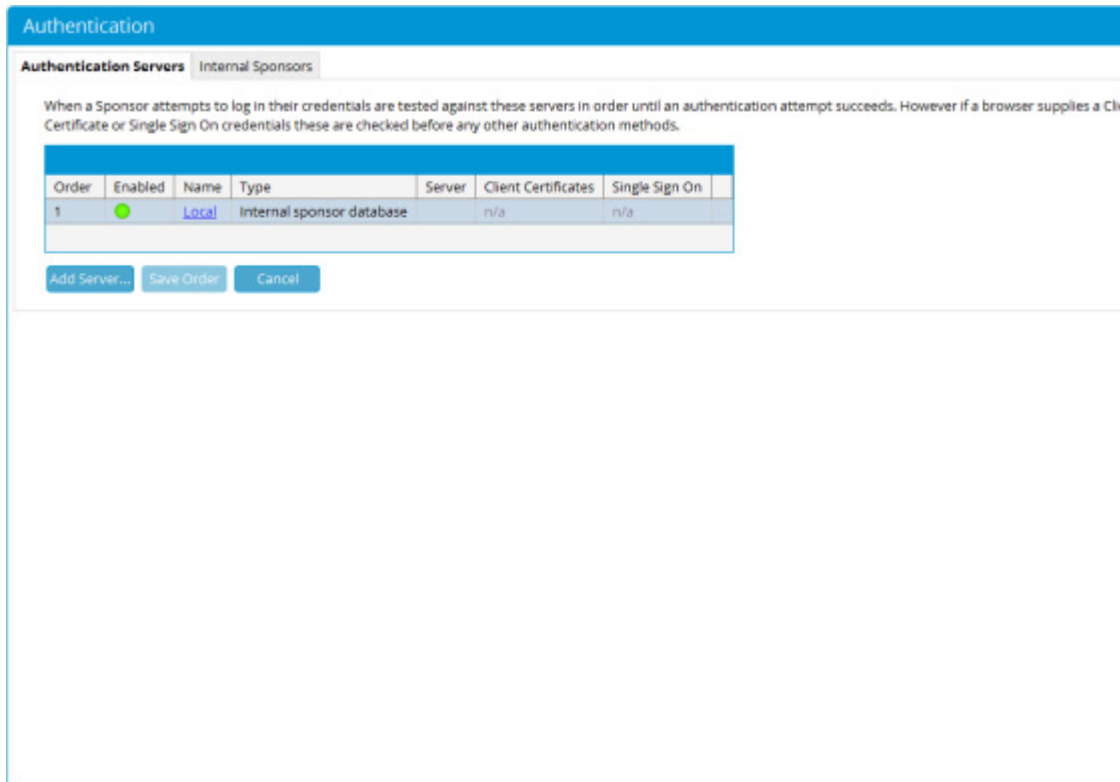
Domain controller: LDAP server signing requirements - Set to "Require Signing"

Network security: LDAP client signing requirements - Set to "Negotiate signing" or "Require signing"

Then the encryption type for the AD Server in MCT should not be "None".

## Adding Active Directory Domain Controller

1. From the administration interface, select **Sponsor Portal > Authentication**. Select the **Authentication Servers** tab below.



The screenshot displays the 'Authentication' configuration page in the FortiConnect administration interface. The page title is 'Authentication' and the active tab is 'Authentication Servers'. Below the tab, there is a sub-tab 'Internal Sponsors'. A descriptive text states: 'When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.' Below this text is a table with the following columns: Order, Enabled, Name, Type, Server, Client Certificates, and Single Sign On. The table contains one entry with Order 1, Enabled status (indicated by a green dot), Name 'Local', Type 'Internal sponsor database', Server 'n/a', Client Certificates 'n/a', and Single Sign On 'n/a'. At the bottom of the table, there are three buttons: 'Add Server...', 'Save Order', and 'Cancel'.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On
1	<input checked="" type="checkbox"/>	Local	Internal sponsor database	n/a	n/a	n/a

2. Click the **Add Server** button.
3. From the Authentication type drop down menu, select **Microsoft Active Directory**.
4. In the **Server** text box insert the Hostname or IP address of the AD server as shown below.

The screenshot shows a configuration window titled "Add Authentication Server". It features a blue header bar. Below the header, there are two main sections. The first section is labeled "Authentication Type:" and contains a dropdown menu with "Microsoft Active Directory" selected. The second section is labeled "Server:" and contains a text input field with the placeholder text "Hostname or IP Address". At the bottom right of the window, there are three buttons: "< Back", "Next >", and "Exit".

Enter details required as shown in the screenshot below.

- **Name**—Type a text description of the Server Name or IP Address.
- **Server Type** - Will auto populate with the server type.
- **Server** - Will auto populate with the servers IP address.
- **Domain** - Will auto populate with the system domain.
- **Encryption** - From the drop down menu, select the desired encryption method.
- **Base DN**— From the drop down menu, select the Base Distinguished Name (DN) of the domain controller. This is the name of the root of the directory tree. It is used so that when group searches are performed, the FortiConnect knows from where to start. An example of the base DN for the domain cca.identitynetworks.com is DC=cca,DC=identitynetworks,DC=com.

**Add Authentication Server**

Name:

Server Type: Microsoft Active Directory

Server:

Domain:

Encryption:

This server supports encryption, but its certificate cannot be validated. You must upload its certificate or its root certificate to continue:

Certificate:  No file chosen

Base DN:

[< Back](#) [Next >](#)

Click on **Next** and then Enter details required as shown below.

- **Username**—Type a username that has permissions to search the Active Directory using LDAP. This allows FortiConnect to find out details about users such as the list of groups to which they belong.
- **Password**—In addition to the AD Username, type the password for that account.
- **Confirm**— Retype the password for confirmation.

**Add Authentication Server**

**Connection**

Name: 10.10.1.2  
Server Type: Microsoft Active Directory  
Server: 10.10.1.2  
Domain: identitynetworks.com  
Encryption: None  
Base DN: DC=identitynetworks,DC=com

**Search Credentials**

Username: @identitynetworks.com  
Password:

< Back   Next >   Exit

Click on **next** to complete.

Once the above details have been entered you can enable/disable the server by clicking on the circle underneath the **Enabled** column.

## Editing Active Directory Domain Controller

1. From the administration interface, select **Sponsor Portal > Authentication** and click on the **Authentication Servers** tab from the menu.
2. Select the Active Directory Domain Controller from the list and click the underlined domain name to select and edit the domain controller as shown below.

## Authentication

### Authentication Servers Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a sponsor supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1	<input checked="" type="checkbox"/>	10.10.1.2	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	
2	<input checked="" type="checkbox"/>	Local	Internal sponsor database		n/a	n/a	

[Add Server...](#) [Save Order](#) [Cancel](#)

3. In the Edit Active Directory Domain Controller page as shown in the screenshot below, edit the details for authenticating against this AD domain controller

### Edit Authentication Server

Name:

Server Type: Microsoft Active Directory

Server: 10.10.1.2

Domain: identitynetworks.com

Encryption:

This server supports encryption, but its certificate cannot be validated. You must upload its certificate or its root certificate to continue:

Certificate:  No file chosen

Base DN:

[< Back](#)

[Next >](#)

4. Modify settings as needed:
  - **Name** - Type a text description of the Server Name or IP Address.
  - **Server Type** - Will auto populate with the server type.

- **Server** - Will auto populate with the servers IP address.
- **Domain** - Will auto populate with the system domain.
- **Encryption** - From the drop down menu, select the desired encryption method.
- **Base DN** - From the drop down menu, select the Base Distinguished Name (DN) of the domain controller. This is the name of the root of the directory tree. It is used so that when group searches are performed, FortiConnect knows from where to start. An example of the base DN for the domain cca.fortinet.com is DC=cca,DC=fortinet,DC=com.

Click on next and edit search credentials, below.

**Edit Authentication Server**

**Connection**

Name: 10.10.1.2  
 Server Type: Microsoft Active Directory  
 Server: 10.10.1.2  
 Domain: identitynetworks.com  
 Encryption: None  
 Base DN: DC=identitynetworks,DC=com

**Search Credentials**

Username:  @identitynetworks.com  
 Password:  Leave blank to keep existing password

< Back   Next >   Exit

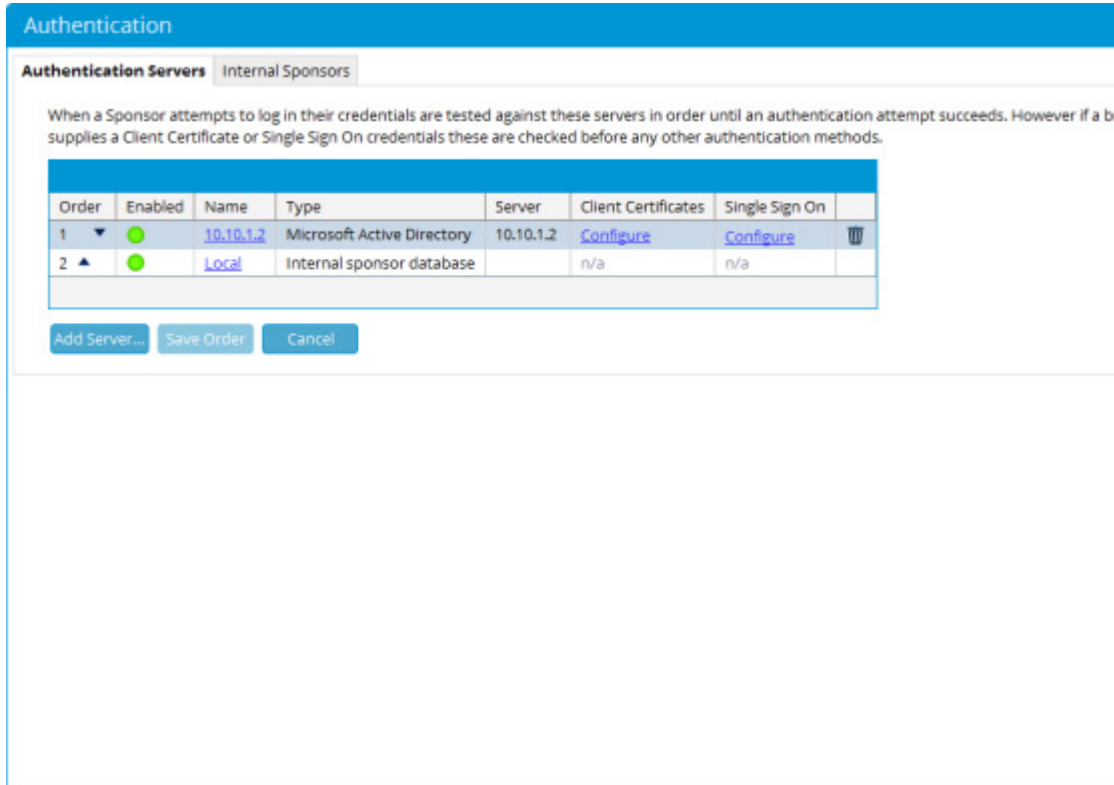
- **Username** - Type a username that has permissions to search the Active Directory using LDAP. This allows FortiConnect to find out details about users such as the list of groups to which they belong.
- **Password** - In addition to the AD Username, type the password for that account.
- **Confirm** - Retype the password for confirmation

Click on **Next** to finish

Once the above details have been entered you can enable/disable the server by clicking on the circle underneath the Enabled column.

## Deleting Active Directory Domain Controller


1. From the administration interface, select **Sponsor Portal** > **Authentication** from the menu and click on the **Authentication Servers** tab.
2. Click the underlined name of the domain controller from the list as shown below.



**Authentication**

**Authentication Servers** Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a sponsor supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1	<input checked="" type="checkbox"/>	<u>10.10.1.2</u>	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	
2	<input checked="" type="checkbox"/>	<u>Local</u>	Internal sponsor database		n/a	n/a	

[Add Server...](#) [Save Order](#) [Cancel](#)

3. Delete the domain controller by clicking the bin icon to the right of the **Enabled** field.
4. Confirm deletion of the Domain Controller at the prompt.

## Configuring LDAP Authentication

LDAP authentication allows FortiConnect to authenticate sponsor users using their existing LDAP user accounts. The sponsors need not have another set of user names and passwords to authenticate to FortiConnect. It also enables the administrator to quickly roll out User Access because there is no need to create and manage additional local sponsor accounts. LDAP authentication allows you to do the following:

- Add an LDAP Server

- Edit an Existing LDAP Server
- Delete an Existing LDAP Server Entry

LDAP authentication supports authentication against multiple LDAP Servers. An LDAP server entry consists of multiple items:

- LDAP Server Name—A text description to identify the LDAP Server.
- LDAP Server URL—This is the URL to access the LDAP server such as `ldap://ldap.fortinet.com`.
- Base DN—This is the Distinguished Name of the container object where an LDAP search to find the user begins, such as `OU=Engineering,O=fortinet`.
- User Search Filter—The User Search Filter defines how user entries are named in the LDAP server. For example, you can define them as `uid (uid=%USERNAME%)` or `cn (cn=% USERNAME%)`.
- Group Mapping—There are two main methods that LDAP servers use for assigning users to groups:

Storing the group membership in an attribute of the user object. With this method, the user object has one or more attributes that list the groups to which the user belongs. If your LDAP server uses this method of storing group membership, you need to enter the name of the attribute which holds the groups of which the user is a member.

Storing the user membership in an attribute of the group object. With this method, there is a group object that contains a list of the users who are members of the group. If your LDAP server uses this method, you need to specify the group to check under the LDAP mapping section of a User Group for which you want to match the user.

To determine the method to be used, Fortinet recommends checking the LDAP documentation for your server or using a third party LDAP browser e.g. from <http://directory.apache> to check the attributes of the server.

- Username—The user account that has permissions to search the LDAP server. This is needed so that FortiConnect can search for the user account and group mapping information.
- Password—The password for the user account that has permissions to search the LDAP server.

To provide resilience in the event of an LDAP server failure, you can enter multiple entries for high availability LDAP servers pointing to the same database. The Server name and URL need to be different in each entry.

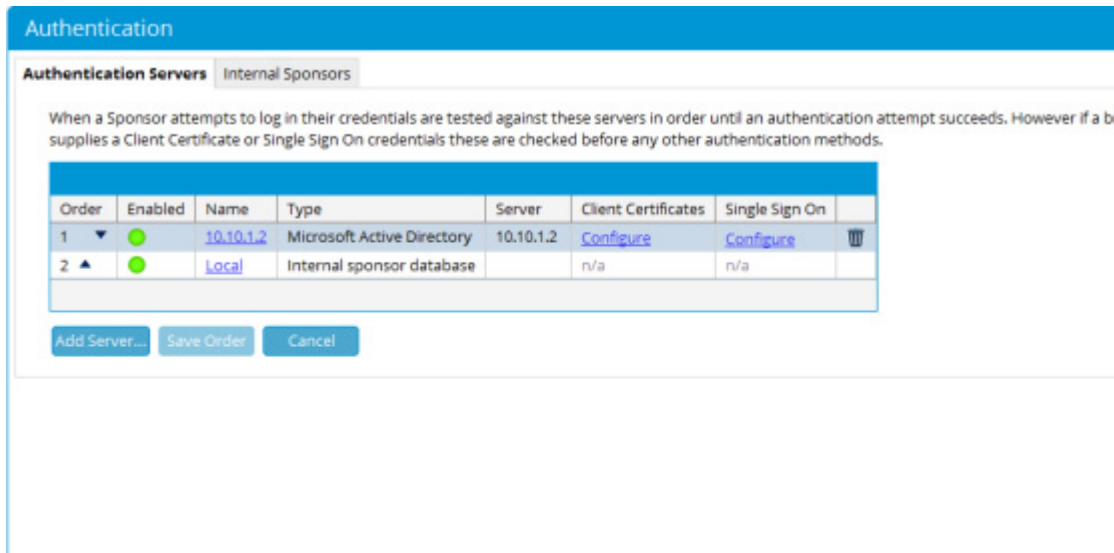
FortiConnect attempts to authenticate sponsors against each LDAP server entry in the order specified by Authentication Order (as detailed in Configuring Sponsor Authentication Settings)

To verify that you have the correct LDAP credentials for connecting to your LDAP server,



## Adding an LDAP Server

1. From the administration interface, select **Sponsor Portal > Authentication** from the menu and click on the **Authentication Servers** tab as shown below.



The screenshot shows the 'Authentication' section of the administration interface. The 'Authentication Servers' tab is selected, and the 'Internal Sponsors' sub-tab is active. A descriptive text explains that credentials are tested against these servers in order until successful, with Client Certificate or Single Sign On credentials checked first. Below this is a table with columns for Order, Enabled, Name, Type, Server, Client Certificates, Single Sign On, and an action icon. Two servers are listed: '10.10.1.2' (Microsoft Active Directory) and 'Local' (Internal sponsor database). At the bottom are buttons for 'Add Server...', 'Save Order', and 'Cancel'.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1	●	<a href="#">10.10.1.2</a>	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	🗑️
2	●	<a href="#">Local</a>	Internal sponsor database		n/a	n/a	

2. Click the **Add Server** button.
3. In the Add LDAP Server page, from the drop down menu select the type of LDAP server you wish to add and enter all the details for authenticating against a specific LDAP server as shown in the screenshot below.

**Add Authentication Server**

Authentication Type:

Server:

Hostname or IP Address

< Back   Next >   Exit

**Note:** When selecting Open LDAP the FortiConnect wizard will automatically populate and detect certain settings, For the purpose of the documentation, Generic LDAP will be used as an example as to detail all the settings FortiConnect requires.

4. Enter the following details as show below.

- **Name**—Type a text description of the LDAP Server Name or IP Address.
- **Server Type** - Server type is auto populated.
- **Server** - Server IP address is auto populated.
- **Encryption** - Select the Encryption method desired for this server. (If the certificate is not trusted then you will be given an option to upload a certificate. Click on **Choose File** to select one.)
- **Base DN**—This is the Distinguished Name of the container object from which an LDAP search to find the user is started, select the desired BASE DN from the drop down list such as OU=Users,O=fortinet.com or OU=Engineering,O=fortinet.

**Add Authentication Server**

Name:

Server Type: Generic LDAP

Server: 10.10.1.2

This server supports encryption, but you must use a hostname that matches the CN (Common Name) in the server's SSL certificate.

Encryption:

Base DN:

5. Now click on **next** to continue and enter further LDAP settings.

#### Server

- **Server** - Enter Server IP Address
- **Encryption** - Enter Encryption method
- **Non Default Port** - Enter non default port number.
- **Network Timeout** - Enter the network timeout in seconds.
- **BASE DN** - This is the Distinguished Name of the container object from which an LDAP search to find the user is started, select the desired BASE DN from the drop down list such as OU=Users,O=fortinet.com or OU=Engineering,O=fortinet.
- **Server Supports Paged Results** - Click box to support this.
- **Page Size** - Enter page size if Server Supports Paged Results is checked.

#### Users

- **Fixed Bind DN for login** - Enter the Fixed Bind DN for login, if left blank the system will determine the Bind DN's automatically.
- **User Name Query** - Returns information for a user. Enter query here.

#### Groups

- **Username Query Returns Groups** - Check box to enable. Some LDAP server

implementations (e.g. Active Directory or eDirectory) have the user's group memberships as an attribute of the user. Other implementations (e.g. OpenLDAP) require an additional query be run to find a user's group memberships.

- **User Group Membership Query** - Returns the groups that a user is in when the query is run.
- **Active Groups Query** - Returns a list of groups when a query is run.

#### Attributes

- **First Name** - Enter the attribute that contains a user's First name.
- **Last Name** - Enter the attribute that contains a user's Last name.
- **Email** - Enter the attribute that contains a user's email address.
- **Manager** - Some LDAP Servers or user configurations may not have a manager attribute.
- **Username** - Enter the attribute that contains a user's username.
- **Group name** - Enter the attribute that contains a user's group name, if supported by the LDAP Server.
- **UUID** - UUDI of the Server

6. Click on **next** to continue

**Add Authentication Server**

The following settings are common defaults that may work on many LDAP servers, some detailed knowledge of your LDAP server may be required to modify and complete the configuration.

**Server**

Server:

Encryption:  ▾

Port:

Network Timeout (seconds):

Base DN:

Server Supports Paged Results:

Page Size:

---

**Users**

Fixed Bind DN for Login:

If left blank the system will determine bind DN's automatically. %s in the value is replaced by the username.

Username Query:

Returns information for a user. When the query is run %s is replaced with the username.

Email Query:

Returns information for a user. When the query is run %s is replaced with the e-mail address.

7. Now enter the Search Credentials as shown in the screenshot below.
- **Use anonymous bind** – Select the check box to enable.
  - **Password** - The password for the user account that has permissions to search the LDAP server.
  - **Confirm** –Repeat the password for confirmation.

**Add Authentication Server**

**Connection**

Name: 10.10.1.2  
Server Type: Generic LDAP  
Server: 10.10.1.2  
Encryption: None  
Base DN: DC=identitynetworks.DC=com

---

**Search Credentials**

Use anonymous bind:

Bind DN:

Password:

< Back   Next >   Exit

8. Click **next** to complete setup

## Editing an LDAP Server

1. From the administration interface, select **Sponsor Portal > Authentication** from the menu and click on the **Authentication Servers** tab as shown below.

## Authentication

### Authentication Servers Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a sponsor supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1		<a href="#">10.10.1.2</a>	Generic LDAP	10.10.1.2	<a href="#">Configure</a>	n/a	
2		<a href="#">10.10.1.2</a>	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	
3		<a href="#">Local</a>	Internal sponsor database		n/a	n/a	

Add Server...

Save Order

Cancel

2. Click the underlined link of the LDAP Server you wish to edit.
3. In the Edit LDAP Server page, Edit the details as detailed below server as shown below.

### Edit Authentication Server

Name:

Server Type: Generic LDAP

Server: 10.10.1.2

This server supports encryption, but you must use a hostname that matches the CN (Common Name) in the server's SSL certificate.

Encryption:

Base DN:

< Back

Next >

- **Name**—Type a text description of the LDAP Server Name or IP Address.

- **Server Type** - Server type is auto populated.
  - **Server** - Server IP address is auto populated.
  - **Encryption** - Select the Encryption method desired for this server. (If the certificate is not trusted then you will be given an option to upload a certificate. Click on **Choose File** to select one.)
  - **Base DN**—This is the Distinguished Name of the container object from which an LDAP search to find the user is started, select the desired BASE DN from the drop down list such as OU=Users,O=fortinet.com or OU=Engineering,O=fortinet.
4. Now click on **next** to continue and edit further LDAP settings as shown in the screenshot below.

**Edit Authentication Server**

**Server**

Server: 10.10.1.2

Encryption: None

Port:

Network Timeout (seconds): 10

Base DN: DC=identitynetworks.DC=com

Server Supports Paged Results:

Page Size: 1000

---

**Users**

Fixed Bind DN for Login:

If left blank the system will determine bind DN's automatically. %s in the value is replaced by the username.

Username Query: (uid=%s)

Returns information for a user. When the query is run %s is replaced with the username.

Email Query: (&(objectClass=Person)(mail=%s))

Returns information for a user. When the query is run %s is replaced with the e-mail address.

---

**Groups**

Some LDAP server implementations (e.g. Active Directory or eDirectory) have the user's group memberships as an attribute of the user. Other implementations

## Server

- **Server** - Enter Server IP Address
- **Encryption** - Enter Encryption method
- **Non Default Port** - Enter non default port number.
- **Network Timeout** - Enter the network timeout in seconds.



- **BASE DN** - This is the Distinguished Name of the container object from which an LDAP search to find the user is started, select the desired BASE DN from the drop down list such as OU=Users,O=fortinet.com or OU=Engineering,O=fortinet.
- **Server Supports Paged Results** - Click box to support this.
- **Page Size** - Enter page size if Server Supports Paged Results is checked.

#### Users

- **Fixed Bind DN for login** - Enter the Fixed Bind DN for login, if left blank the system will determine the Bind DN's automatically.
- **User Name Query** - Returns information for a user. Enter query here.

#### Groups

- **Username Query Returns Groups** - Check box to enable. Some LDAP server implementations (e.g. Active Directory or eDirectory) have the user's group memberships as an attribute of the user. Other implementations (e.g. OpenLDAP) require an additional query be run to find a user's group memberships.
- **User Group Membership Query** - Returns the groups that a user is in when the query is run.
- **Active Groups Query** - Returns a list of groups when a query is run.

#### Attributes

- **First Name** - Enter the attribute that contains a user's First name.
- **Last Name** - Enter the attribute that contains a user's Last name.
- **Email** - Enter the attribute that contains a user's email address.
- **Username** - Enter the attribute that contains a user's username.
- **Group name** - Enter the attribute that contains a user's groups, if supported by the LDAP Server.

5. Click on **next** to continue

6. Now enter the Search Credentials as shown below.

- **Use anonymous bind** – Select the check box to enable.
- **Password** - The password for the user account that has permissions to search the LDAP server.
- **Confirm** –Repeat the password for confirmation.

**Edit Authentication Server**

**Connection**

Name: 10.10.1.2  
Server Type: Generic LDAP  
Server: 10.10.1.2  
Encryption: None  
Base DN: DC=identitynetworks,DC=com

---

**Search Credentials**

Use anonymous bind:

Bind DN:

Password:

< Back   Next >   Exit

7. Click **next** to complete setup

## Deleting an LDAP Server

1. From the administration interface, select **Sponsor Portal > Authentication** from the menu and click on the **Authentication Servers** tab.
2. Select the LDAP Server from the list as shown below.

Authentication

**Authentication Servers** Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a sponsor supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1		<a href="#">10.10.1.2</a>	Generic LDAP	10.10.1.2	<a href="#">Configure</a>	n/a	
2		<a href="#">10.10.1.2</a>	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	
3		<a href="#">Local</a>	Internal sponsor database		n/a	n/a	

[Add Server...](#) [Save Order](#) [Cancel](#)

3. Choose the server you wish to delete by clicking the **bin** icon to the right of the **Status** field.
4. Confirm deletion of the LDAP Server at the prompt.

If there are any errors, the LDAP Server is not changed and an error message is displayed at the top of the page. If successfully deleted, a success message is displayed at the top of the page and you can perform additional LDAP Server operations.

## Configuring Novell eDirectory Server Authentication

The following section describes how to Configure Novell eDirectory Server Authentication.

- Add a Novell eDirectory Server.
- Edit a Novell eDirectory Server.
- Delete a Novell eDirectory Server.

### Adding Novell eDirectory Server

1. From the administration interface, select **Sponsor Portal > Authentication** from the menu and click on the **Authentication Servers** tab as shown below.

## Authentication

### Authentication Servers Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1 ▼	●	<a href="#">10.10.1.2</a>	Generic LDAP	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
2 ▲▼	●	<a href="#">10.10.1.2</a>	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	🗑️
3 ▲	●	<a href="#">Local</a>	Internal sponsor database		n/a	n/a	

Add Server...

Save Order

Cancel

2. Click the Add Server button.
3. In the Add Authentication Server page, from the drop down menu select **Novell eDirectory** and enter the hostname or the IP address of the Novell eDirectory Server you wish to authenticate against.

Add Authentication Server

Authentication Type: Novell eDirectory

Server:

Hostname or IP Address

< Back Next >

4. Enter the following details as show below.
  - **Name**—Type a text description of the Novell eDirectory Server Server Name or IP Address.
  - **Server Type** - Server type is auto populated.
  - **Server** - Server IP address is auto populated.
  - **Encryption** - Select the Encryption method desired for this server. (If the certificate is not trusted then you will be given the option to upload a certificate. Click on **Choose file** to select)
  - **Base DN**—This is the Distinguished Name of the container object from which a Novell eDirectory Server search to find the user is started, select the desired BASE DN from the drop down list such as OU=Users,O=fortinet.com or OU=Engineering,O=fortinet.

**Add Authentication Server**

Name:

Server Type: Novell eDirectory

Server: 10.10.1.2

Encryption:

This server supports encryption, but its certificate cannot be validated. You must upload its certificate or its root certificate to continue:

Certificate:  No file chosen

Base DN:

5. Now enter the Search Credentials as shown in the screenshot below.
- **Use anonymous bind** – Select the check box to enable.
  - **Password** - The password for the user account that has permissions to search the Novell eDirectory server.
  - **Confirm** –Repeat the password for confirmation.

**Add Authentication Server**

**Connection**

Name: 10.10.1.2  
Server Type: Novell eDirectory  
Server: 10.10.1.2  
Encryption: None  
Base DN: DC=identitynetworks.DC=com

---

**Search Credentials**

Use anonymous bind:

Bind DN:

Password:

[< Back](#) [Next >](#)

6. Click **Next** to complete the setup.

## Editing Novell eDirectory Server

1. From the administration interface, select **Sponsor Portal > Authentication** from the menu and click on the **Authentication Servers** tab as shown below.

## Authentication

**Authentication Servers** Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1		<a href="#">10.10.1.2</a>	Novell eDirectory	10.10.1.2	<a href="#">Configure</a>	n/a	
2		<a href="#">10.10.1.2</a>	Generic LDAP	10.10.1.2	<a href="#">Configure</a>	n/a	
3		<a href="#">10.10.1.2</a>	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	
4		<a href="#">Local</a>	Internal sponsor database		n/a	n/a	

[Add Server...](#) [Save Order](#) [Cancel](#)

2. Click the underlined link of the Novell eDirectory Server you wish to edit.
3. In the Edit Authentication Server page, Edit the details as detailed below server as shown below.

## Edit Authentication Server

Name:

Server Type: Novell eDirectory

Server: 10.10.1.2

Encryption:

This server supports encryption, but its certificate cannot be validated. You must upload its certificate or its root certificate to continue:

Certificate:  No file chosen

Base DN:

[< Back](#) [Next >](#) [Exit](#)

- **Name**—Type a text description of the Novell eDirectory Server Name or IP



Address.

- **Server Type** - Server type is auto populated.
  - **Server** - Server IP address is auto populated.
  - **Encryption** - Select the Encryption method desired for this server. (If the certificate is not trusted then you will be given an option to upload a certificate. Click on **Choose File** to select one.)
  - **Base DN**—This is the Distinguished Name of the container object from which a Novell eDirectory Server search to find the user is started, select the desired BASE DN from the drop down list such as OU=Users,O=fortinet.com or OU=Engineering,O=fortinet.
4. Now click on **next** to continue and edit further Novell eDirectory Server settings as shown in the screenshot below.

**Edit Authentication Server**

**Connection**

Name: 10.10.1.2  
Server Type: Novell eDirectory  
Server: 10.10.1.2  
Encryption: None  
Base DN: DC=identitynetworks,DC=com

**Search Credentials**

Use anonymous bind:

Bind DN:

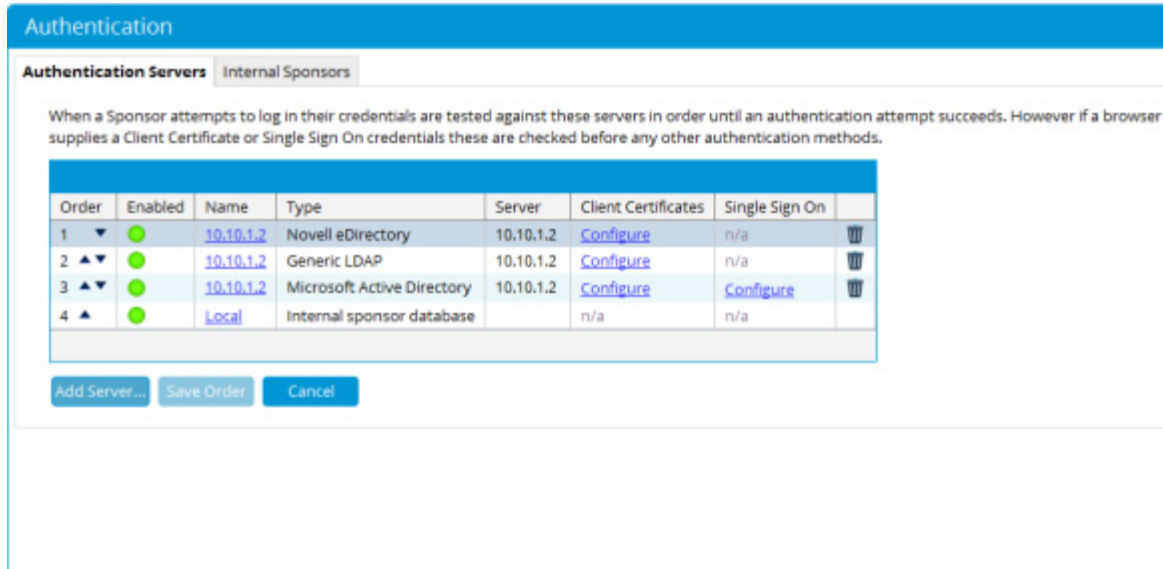
Password:

< Back    Next >

- **Use anonymous bind** – Select the check box to enable.
  - **Password** - The password for the user account that has permissions to search the Novell eDirectory Server.
  - **Confirm** –Repeat the password for confirmation.
5. Click on **Next** to complete.

## Deleting Novell eDirectory Server

1. From the administration interface, select **Sponsor Portal > Authentication** from the menu and click on the **Authentication Servers** tab.
2. Select the Novell eDirectory Server from the list as shown below.



The screenshot shows the 'Authentication Servers' configuration page. At the top, there is a blue header with the word 'Authentication'. Below it, there are two tabs: 'Authentication Servers' (selected) and 'Internal Sponsors'. A paragraph explains that when a sponsor attempts to log in, their credentials are tested against these servers in order until an authentication attempt succeeds. Below this is a table with the following data:

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1	●	<a href="#">10.10.1.2</a>	Novell eDirectory	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
2	●	<a href="#">10.10.1.2</a>	Generic LDAP	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
3	●	<a href="#">10.10.1.2</a>	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	🗑️
4	●	<a href="#">Local</a>	Internal sponsor database		n/a	n/a	

At the bottom of the table, there are three buttons: 'Add Server...', 'Save Order', and 'Cancel'.

3. Choose the server you wish to delete by clicking the **bin** icon to the right of the **Status** field.
4. Confirm deletion of the Novell eDirectory Server at the prompt.

## Configuring RADIUS Authentication

RADIUS authentication allows FortiConnect to authenticate sponsors using their existing RADIUS user accounts. The sponsors need not have another set of user names and passwords to authenticate to FortiConnect. It also enables the administrator to quickly roll out User Access because there is no need to create and manage additional local sponsor accounts. RADIUS authentication allows you to do the following:

- Add a RADIUS Server
- Edit an Existing RADIUS Server
- Delete an Existing RADIUS Server Entry

### Adding a RADIUS Server

1. From the administration interface, select **Sponsor Portal > Authentication**. Select the **Authentication Servers** tab as shown below.

## Authentication

### Authentication Servers Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a sponsor supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1 ▼	●	<a href="#">10.10.1.2</a>	Novell eDirectory	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
2 ▲▼	●	<a href="#">10.10.1.2</a>	Generic LDAP	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
3 ▲▼	●	<a href="#">10.10.1.2</a>	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	🗑️
4 ▲	●	<a href="#">Local</a>	Internal sponsor database		n/a	n/a	

Add Server...

Save Order

Cancel

2. Click the **Add Server** button
3. From the Authentication type drop down menu, select **Radius**.
4. In the Server text box insert the Hostname or IP address of the RADIUS server as shown below, and click **Next**

Add Authentication Server

Authentication Type:

Server:

Hostname or IP Address

< Back   Next >   Exit

5. Insert the requested Radius Server details into the appropriate fields as shown in the screenshot below.

Add Authentication Server

Name:

Authentication Type: RADIUS

---

**Primary RADIUS server**

Server IP Address:

Authentication Port:

Secret:    Confirm:

< Back   Next >   Exit

- **Server Name**—Type a text description of the RADIUS Server Name. For example: Fortinet RADIUS - radius.identitynetworks.com.
- **Server**—Enter the IP address or domain name of the RADIUS server.
- **Port**—Enter the UDP port used to connect to the RADIUS server. The common ports for RADIUS authentication are ports 1645 or 1812.
- **RADIUS Secret**—The shared secret used to secure the communications between FortiConnect and the RADIUS server.
- **Confirm**—Repeat the shared secret for confirmation.

6. Click the **Next** button to complete.

## Add Fortigate as a RADIUS server

Fortigate can be added as a Radius client in FortiConnect. However, there are following limitations:

- Device Authentication feature will not work as Fortigate does not send 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 AP name and AP id some guest reports and accounting logs will have empty fields against them.
- Redirection URL after successful guest authentication **must** be set in Fortigate configuration.
- In Mac / iPad, when using Safari to perform guest authentication, intermittently the browser will timeout or will take long time to redirect to the portal success page.

To integrate, start by creating a RADIUS client entry of type **Fortigate**. Provide Fortigate server IP address.

The screenshot displays the FortiConnect web interface for configuring a RADIUS client. On the left is a navigation sidebar with categories: HOME, NETWORK ACCESS POLICY, POLICY SETTINGS, SPONSOR PORTAL, GUEST PORTALS, SMART CONNECT, and DEVICES. Under DEVICES, 'RADIUS Clients' is selected. The main panel is titled 'RADIUS Clients' and contains several tabs: 'Client', 'Attributes', 'SNMP', 'MAC Authentication', and 'RadSec Authentication'. The 'Client' tab is active, showing the following configuration fields:

- Name:** Fortigate
- Device IP Address / Prefix Length:** 172.18.26.26/32 (with a note: For example 192.168.1.1/32 or fec0:0001/128)
- Secret:** (empty field) **Confirm:** (empty field) (with a note: Leave blank to keep existing secret)
- Type:** Fortigate (dropdown menu)
- Description:** (empty text area)

At the bottom of the configuration area are two buttons: 'Save' and 'Cancel'.

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

The screenshot shows the FortiGate WebUI configuration page for RADIUS Clients. The left sidebar contains navigation options: HOME, NETWORK ACCESS POLICY, POLICY SETTINGS, SPONSOR PORTAL, GUEST PORTALS, SMART CONNECT, and DEVICES. Under DEVICES, 'RADIUS Clients' is selected. The main content area is titled 'RADIUS Clients' and has tabs for 'Client', 'Attributes', 'SNMP', 'MAC Authentication', and 'RadSec Authentication'. The 'Attributes' tab is active, showing a table with one attribute: Vendor: IETF, Attribute: Access-Loop-Encapsulation, and Value: Acct-Interim-Interval = 600. There are buttons for 'Add AV Pair', 'Move up', 'Remove', 'Move down', 'Save', and 'Cancel'.

After you have completed configuring Fortigate server details in the FortiConnect server, log in to your Fortigate server and do the following to complete the integration.

**Step 1** In the Fortigate server WebUI, go to **WiFi Controller > SSID**. Create a new SSID and ensure that you provide details as listed after the following screenshot.

The screenshot shows the FortiGate WebUI configuration page for WiFi Settings. The left sidebar contains navigation options: HOME, NETWORK ACCESS POLICY, POLICY SETTINGS, SPONSOR PORTAL, GUEST PORTALS, SMART CONNECT, and DEVICES. Under DEVICES, 'WiFi Settings' is selected. The main content area is titled 'WiFi Settings' and has a tab for 'SSID'. The 'SSID' field is 'fortinet-clear'. The 'Security Mode' is 'Captive Portal'. The 'Portal Type' is 'Authentication'. The 'Authentication Portal' is 'External' with address '172.19.40.249/portal/172.18.26.26'. The 'User Groups' is 'Guest-group'. The 'Redirect after Captive Portal' is 'Specific URL' with address 'http://172.19.40.249/portal/login/172.18.26.26/success'. Other options like 'Broadcast SSID', 'Block Intra-SSID Traffic', and 'Optional VLAN ID' are also visible.

1. Set **Security Mode** to *Captive Portal*.

2. Select **Portal Type** as *Authentication*.

3. Enter the **Authentication Portal** address in this format: <FortiConnect-serverIP>/portal/Fortigate-serverIP>.

For example, if FortiConnect server IP is 172.19.40.249 and Fortigate server IP is 172.18.26.26, then your IP address is 172.19.40.249/portal/172.18.26.26.

4. Provide a destination URL to **Redirect after Captive Portal** authentication.

**Step 2** Go to **Wifi Controller > FortiAP Profiles** and create or edit a profile. In the profile, set the SSID of each radio to the SSID created in step 1.

Channel Width: 20MHz

Channel:  36  40  44  48  149  153  157  161  165

Auto TX Power Control:  Disable  Enable

TX Power: 100 %

SSID:  **Please Select**  forti-clear (SSID: fortinet-clear)

Radio 2

Mode:  Duplexed Monitor

Spectrum Analysis:  Click to set...

IDS Profile:  Click to set...

Radio Resource Provision:

Client Load Balancing:  Frequency Handoff  AP Handoff

Band: 2.4GHz 802.11n/g/b

Channel:  1  2  3  4  5  6  7  8  9  10  11

Auto TX Power Control:  Disable  Enable

TX Power: 100 %

SSID:  **Please Select**  forti-clear (SSID: fortinet-clear)

**Step 3** Go to **Policies and Objects > Objects > Addresses**. Create a new entry with a name for the FortiConnect Server and its IP address.

Name: Meru Connect RADIUS

IP/Netmask: 172.18.26.26/255.255.255.255

Interface: any

Visibility in Address List:

Comments: 0/255

**Step 4** Go to Policies and Objects > Policy > IPv4. Create the following rules:

From	To	Source	Destination	Schedule	Service	Action	NAT	SSL Inspection	Log
forti-clear (SSID: fortinet-clear)		Meru Connect	all	always	ALL	ACCEPT	Enable		All
(SSID: tortinet-clear)	any	all	Meru Connect	always	ALL	ACCEPT	Enable		All
	any	all	all	always	DNS DHCP	ACCEPT	Enable		All
(SSID: fortinet-clear)	any	all Guest-group	all	always	ALL	ACCEPT	Enable		UTM

**Step 5** Go to User & Device > Authentication > RADIUS Servers. Create a new entry of the FortiConnect server. The secret key entered here should be used while adding the Fortigate server in FortiConnect. Ensure that you enter the Fortigate server IP address as the **NAS IP / Called Station ID**.

Primary Server IP/Name

Primary Server Secret

Secondary Server IP/Name

Secondary Server Secret

Authentication Method  Default  Specify

IP / Called Station ID 
This Fortigate Serv

Enable in every User Group

**Step 6** Now, go to the Fortigate CLI, and execute the following commands to complete the integration:

Allow external web access

```
# set captive portal exempt enable
```

Configure accounting time interval

```
# set acct-interim-interval [duration] (between 600 - 86400 seconds)
```

Configure FortiConnect as the Radius accounting server

```
# config accounting-server
```

```
# edit 1
```

```
# set status enable
```



```
# set server <IP Address of FortiConnect>
# Set secret <Secret>
```

## Editing a RADIUS Server

1. From the administration interface, select **Sponsor Portal > Authentication** and select the **Authentication Servers** tab.
2. Select the RADIUS server from the list and click the underlined name of the server you wish to edit as shown below.

Authentication

**Authentication Servers** Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a sponsor supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1 ▼	●	<u>10.10.1.2</u>	RADIUS	10.10.1.2	n/a	n/a	🗑️
2 ▲▼	●	10.10.1.2	Novell eDirectory	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
3 ▲▼	●	10.10.1.2	Generic LDAP	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
4 ▲▼	●	10.10.1.2	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	🗑️
5 ▲	●	Local	Internal sponsor database		n/a	n/a	

[Add Server...](#) [Save Order](#) [Cancel](#)

3. In the Edit RADIUS Server Details page as shown below, edit the details for authenticating against this RADIUS server.

**Edit Authentication Server**

Name:

Authentication Type: RADIUS

---

**Primary RADIUS server**

Server IP Address:

Authentication Port:

Secret:  Confirm:

< Back   Next >   Exit

4. Modify settings as needed:

- **Server IP Address**—Enter the IP address or domain name of the RADIUS server.
- **Port**—Enter the UDP port used to connect to the RADIUS server. The common ports for RADIUS authentication are ports 1645 or 1812.
- **RADIUS Secret**—The shared secret used to secure the communications between FortiConnect and the RADIUS server.

**Note:** If you do not want to change the shared secret, leave the Secret and Confirm fields to retain the existing shared secret.

- **Enabled**—Check the checkbox to enable FortiConnect to use this RADIUS server to authenticate sponsors. If not checked, the RADIUS server will not be used.

5. Click the **Next** button.

## Deleting a RADIUS Server

1. From the administration interface, select **Sponsor Portal > Authentication** and select the **Authentication Servers** tab.
2. Find the RADIUS server in the list that you wish to delete and click the **bin** icon to the right of the **Status** field as shown below.

Authentication

**Authentication Servers** Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a sponsor supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1 ▼	●	<a href="#">10.10.1.2</a>	RADIUS	10.10.1.2	n/a	n/a	🗑️
2 ▲▼	●	<a href="#">10.10.1.2</a>	Novell eDirectory	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
3 ▲▼	●	<a href="#">10.10.1.2</a>	Generic LDAP	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
4 ▲▼	●	<a href="#">10.10.1.2</a>	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	🗑️
5 ▲	●	<a href="#">Local</a>	Internal sponsor database		n/a	n/a	

Add Server... Save Order Cancel

3. Confirm deletion of the RADIUS server at the prompt.

If there are any errors, the RADIUS server is not changed and an error message is displayed at the top of the page. If successfully deleted, a success message is displayed at the top of the page and you can perform additional RADIUS operations.

## Active Directory Single Sign-On

The Active Directory Single Sign-On (AD SSO) feature uses Kerberos between the client's web browser and FortiConnect to automatically authenticate a Sponsor against an Active Directory Domain Controller.

An Active Directory Domain Controller in the same domain as the single sign on configuration must have been previously configured as described in Configuring Active Directory (AD) Authentication.

### Requirements for Active Directory Single Sign-On

The following requirements must be met for Active Directory Single Sign-On to be configured successfully:

- DNS must be configured and working on FortiConnect
- DNS must be configured and working on the Domain Controller
- Both of the following DNS entries for FortiConnect must be defined and must be available to both FortiConnect and all Windows servers in the domain:
  - i. Forward ("A") record

- ii. Reverse (“PTR”) record
  - Both of the following DNS entries for the Domain Controller must be defined must be defined and must be available to both FortiConnect and all Windows servers in the domain:
    - i. Forward (“A”) record
    - ii. Reverse (“PTR”) record
  - FortiConnect time settings must be synchronized with the Active Directory Domain
  - Sponsors web browser may require configuration to allow the single sign on function
  - Single Sign on must be configured separately for each replicated server

If any of these setting are not met, then AD SSO configuration will fail.

**Note:** Fortinet strongly recommends configuring NTP so that time is synchronized with the Active Directory Domain. Single Sign-On will fail if the time on the FortiConnect appliance differs by more than 5 minutes from the client or the domain.

## Configuring Active Directory Single Sign-On

1. Configure an Active Directory Server as described in Configuring Active Directory (AD) Authentication. An Active Directory Server is needed so that users performing Single Sign-On can be correctly mapped against a sponsor group. The Active Directory Server must be in the same domain as in the Single Sign-On settings that you undertake.
2. From the administration interface, select **Sponsor Portal > Authentication** from the left menu and click on **Configure** under the **Single Sign On** column for the domain that you want to enable AD Single Sign On, as shown below.

**Authentication Servers** Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a sponsor supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1	●	10.10.1.2	RADIUS	10.10.1.2	n/a	n/a	🗑️
2	●	10.10.1.2	Novell eDirectory	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
3	●	10.10.1.2	Generic LDAP	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
4	●	10.10.1.2	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	🗑️
5	●	Local	Internal sponsor database		n/a	n/a	

[Add Server...](#) [Save Order](#) [Cancel](#)

3. Enter the **Domain Admin Username** and **Password** in the fields provided.

4. Click on **Next** then click on **Close** to finish.

Sponsors you have created on Active Directory should now be able to login to the domain and access the Sponsor user interface. Sponsors should be entering the Domain name in the browser and not the IP Address of FortiConnect.

**Note:** If you have multiple FortiConnect appliances you will need to configure single sign on each appliance. This is so the account for each FortiConnect is successfully created in Active Directory.

## Managing Client Certificates

If your infrastructure is set up to use Client Certificates you may configure FortiConnect to accept a sponsor's Client Certificate as an alternative to logging in with a username and password.

The Client Certificate is installed on each sponsor's browser and typically the management of these certificates is managed by your local administrators.

- The following chapter details how to install and use your client certificates with FortiConnect.

**Note:** Client Certificate Authentication is not supported with RADIUS and local sponsor authentication.

# Installing Client Certificates

In order to configure Client Certificate support you must possess a sample Client Certificate (possibly your own) that is in PKCS#12, PEM or DER format. FortiConnect will inspect this certificate and attempt to find a user in the selected authentication server based upon the certificate contents.

To use client certificates with FortiConnect follow the instructions below.

1. From the FortiConnect administration interface select **Sponsor Portal --> Authentication**.

**Authentication Servers** Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a browser supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1	●	<a href="#">10.10.1.2</a>	RADIUS	10.10.1.2	n/a	n/a	🗑️
2	●	<a href="#">10.10.1.2</a>	Novell eDirectory	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
3	●	<a href="#">10.10.1.2</a>	Generic LDAP	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
4	●	<a href="#">10.10.1.2</a>	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	🗑️
5	●	<a href="#">Local</a>	Internal sponsor database		n/a	n/a	

[Add Server...](#) [Save Order](#) [Cancel](#)

2. Click on the **Configure** link underneath the **Client Certificates** column.

**Configure Client Certificates**

To configure client certificates you can upload a sample user certificate. By inspecting this certificate the system will automatically determine how to map the certificate to a user on an authentication server.

Parse a sample PKCS#12 file

PKCS#12 File:  No file chosen  
Files usually end in a p12 or pkcs12 extension

Password:   
The password is only used to extract the certificate from the PKCS#12 file. It is not stored.

---

Parse a sample X.509 certificate in PEM or DER format

Certificate:  No file chosen  
Files usually end in a pem, cer, der or crt extension

3. Depending on your certificates file type, select the appropriate parsing method and then click on the **browse** button to browse to and select your certificate file. If **PKCS#12** has been selected as your format you must also enter the **Password** of the file and then click on **next**.

#### Sample Client Certificate

Common Name (CN): John Carter  
Subject DN: /C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd/CN=John Carter/emailAddress=johncarter@merutest.com  
Parsed Subject DN: CN=John Carter,O=My Company Ltd,L=Newbury,ST=Berkshire,C=GB  
Email Address: johncarter@merutest.com  
User ID: <Not part of certificate>  
User Principal Name: <Not part of certificate>

Find user on server by mapping Client Certificate  to user attribute .

[Advanced >](#)

#### User Search Results

 No user found

< Back

Next >

Exit

4. FortiConnect will attempt to find a user on your authentication server using the certificate properties. If an initial search finds no matching results, you will be required to change your server mapping accordingly using the drop down menus to obtain the results as shown in the example below.

**Note:** The advanced setting lets you perform regular expression replacements on certificate properties before searching in your authentication server.



#### Sample Client Certificate

Common Name (CN): John Carter  
Subject DN: /C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd/CN=John Carter/emailAddress=johncarter@merutest.com  
Parsed Subject DN: CN=John Carter,O=My Company Ltd,L=Newbury,ST=Berkshire,C=GB  
Email Address: johncarter@merutest.com  
User ID: <Not part of certificate>  
User Principal Name: <Not part of certificate>

Find user on server by mapping Client Certificate  to user attribute

[Advanced »](#)

#### User Search Results

User found  
CN: John Carter  
DN: CN=John Carter,CN=Users,DC=merutest,DC=com  
Email Address: <Not set>  
Username: johncarter  
User Principal Name: johncarter@merutest.com

< Back

Next >

5. Some authentication servers have a copy of the full client certificate of a user as part of the user properties. As an additional check FortiConnect can directly compare that Client Certificate with the one supplied by the browser. The SSL renegotiation option allows FortiConnect to support the old and insecure method of authenticating with Client Certificates. If your browsers have been updated you may deselect this option.

### Certificate Matching

Some authentication servers have the client certificate of each user. We can compare that certificate with the one supplied by the browser and the user will only be logged in if the certificates match.

This authentication server does not appear to store the user's certificate.

Verify the user's certificate stored on the server matches the client certificate supplied by the browser.

### SSL Renegotiation

In October 2009 a serious SSL vulnerability ([CVE-2009-3555](#)) was disclosed that affected Client Certificate authentication on all common web servers and browsers. The issue has been addressed by a change to the SSL protocol. Identity Manager has support for the updated protocol but many common browsers do not. To support browsers that have not been updated you can enable the previous behaviour.

This setting will apply to all web SSL connections to the server.

Allow pre-CVE-2009-3555 SSL Renegotiation

< Back    Next >    Exit

6. Click on the **next** button and then **close**.

Administrators can then apply certificates ready for sponsor use using Internet Options on the sponsor's browser. After the certificate has been successfully imported onto the browser, the sponsors can login automatically to the sponsor interface using an SSL connection.

## Defining the Order of Authentication Servers

When a sponsor authenticates against FortiConnect it tries each authentication server that has been defined, in order, until it successfully authenticates a sponsor. If none of the authentication servers can authenticate the sponsor, an error message is returned.

As you can define many different authentication servers of different kinds, you can order them in any way you want on a server-by-server basis.

1. From the administration interface, select **Sponsor Portal > Authentication** and click on the **Authentication Servers Tab** from the menu as shown below.

**Authentication**

**Authentication Servers** Internal Sponsors

When a Sponsor attempts to log in their credentials are tested against these servers in order until an authentication attempt succeeds. However if a sponsor supplies a Client Certificate or Single Sign On credentials these are checked before any other authentication methods.

Order	Enabled	Name	Type	Server	Client Certificates	Single Sign On	
1 ▼	●	<a href="#">10.10.1.2</a>	RADIUS	10.10.1.2	n/a	n/a	🗑️
2 ▲▼	●	<a href="#">10.10.1.2</a>	Novell eDirectory	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
3 ▲▼	●	<a href="#">10.10.1.2</a>	Generic LDAP	10.10.1.2	<a href="#">Configure</a>	n/a	🗑️
4 ▲▼	●	<a href="#">10.10.1.2</a>	Microsoft Active Directory	10.10.1.2	<a href="#">Configure</a>	<a href="#">Configure</a>	🗑️
5 ▲	●	<a href="#">Local</a>	Internal sponsor database		n/a	n/a	

Add Server... Save Order Cancel

The first server to be authenticated against is at the top of the list and the last one at the bottom.

2. Select the server that you want to re-order from the list and click either the **up** or **down** button. Perform this action with all the servers until they are in the correct order.
3. To save the authentication order click the **Save Order** button.

## Configuring Sponsor User Groups

---

Sponsor user groups are the method by which you 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 by email or SMS.

Once you have created a User group, create mapping rules to map the sponsor to a group based upon information returned from the authentication server such as Active Directory Group, LDAP Group membership, or RADIUS Class attribute.

TIP - By default, all Users are assigned to the DEFAULT group. If you only want to have a single classification of sponsors, you can edit the DEFAULT group.

This chapter describes the following:

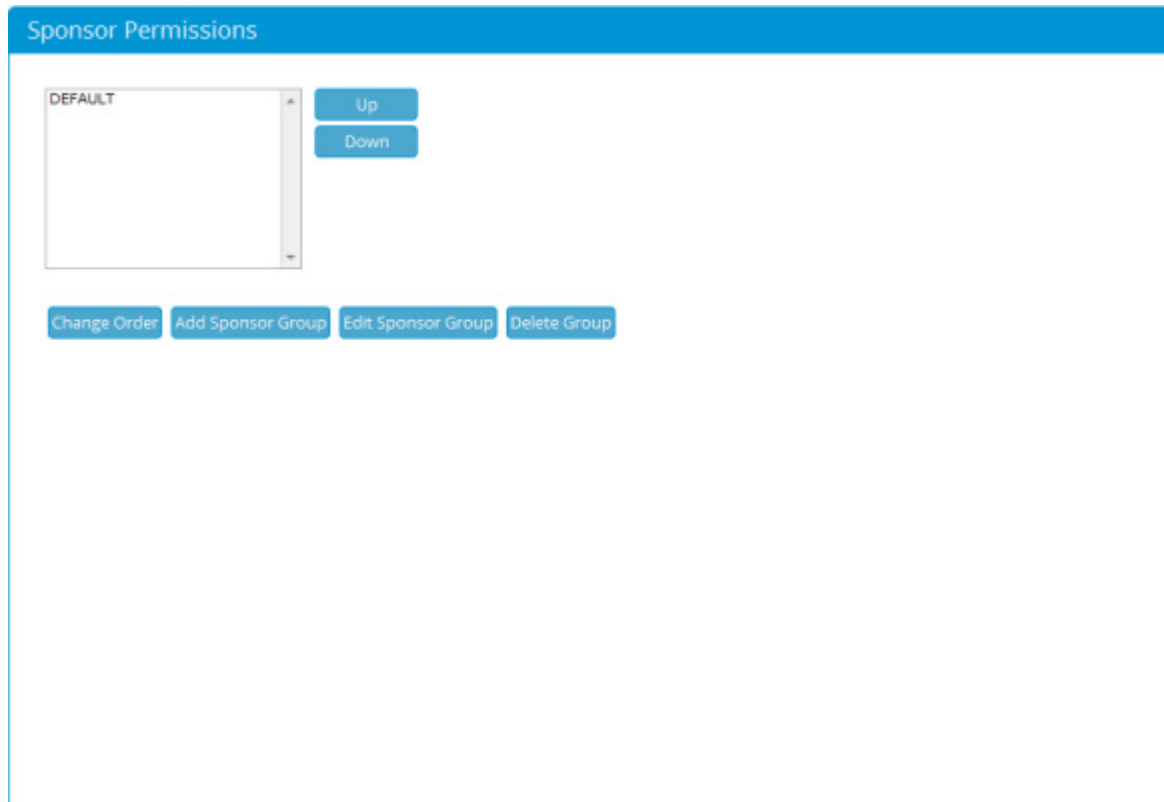
- Adding Sponsor User Groups
- Editing Sponsor User Groups

- Deleting User Groups
- Specifying the Order of Sponsor User Groups
- Mapping to Active Directory Groups
- Mapping to LDAP Groups
- Mapping to RADIUS Groups
- Assigning User Account Groups
- Assigning Usage Profiles

## Adding Sponsor User Groups

You can create a new sponsor user group using the following steps.

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** as shown below.



2. Click the **Add Sponsor Group** button to add a new user group.
3. From the Add a New Sponsor Group page as shown below, type the name for a new user group in the Sponsor Group Name field.

## Add Sponsor Group

Name:

Add

Cancel

4. Click the **Add Sponsor Group** button to add a user group. You can now edit the settings for the new user group as detailed below.
5. Edit and set the permissions for the new User Group as follows:
  - **Allow Login**—Select **Yes** to allow sponsors in this group to access FortiConnect.
  - **Create Guest Accounts**—Select **Yes** to allow sponsors to create accounts.
  - **Create Multiple Guest Accounts**—Select **Yes** to allow sponsors to be able to create multiple accounts at a time by pasting in the details.
  - **Create Random Guest Accounts**—Select **Yes** to allow sponsors to be able to create multiple random accounts without initially capturing the Users details.
  - **Email Manager on Guest Account Creation** - Automatically email a sponsors manager when an account has been created. (LDAP setup only)
  - **Create Device Accounts** - Select **Yes** to allow sponsors to be able to create device accounts.
  - **Create Multiple Device Accounts** - Select **Yes** to allow sponsors to be able to create multiple accounts at a time by filling in the appropriate form or importing a csv in the details.

- **Email Manager on Device Account Creation** - Automatically email a sponsor's manager when a device account has been created. (LDAP setup only)
- **Send Email**—Select **Yes** to allow sponsors to send account details via email from FortiConnect to the user.
- **Send SMS**—Select **Yes** to allow sponsors to send account details via SMS from the FortiConnect to the User.
- **View Guest Account Password**—Select **Yes** to allow sponsors to view the password that has been created for the User.
- **Print Account Details**—Select **Yes** to allow sponsors to print out the account details.

**Note:** Select No, if you want to disable any of the above permissions.

- **Reset Account Password** - Choose one of the following options to allow a sponsor to reset account passwords.
  - No**—Sponsors are not allowed to reset any account passwords.
  - Own Account**—Sponsors are allowed to reset only the account passwords they created.
  - Group Accounts**—Sponsors are allowed to reset account passwords created by anyone in the same sponsor user group.
  - All Accounts**—Sponsors are allowed to reset any account passwords in any User accounts
- **Suspend Account**—Choose one of the following options for suspending accounts:
  - No**—Sponsors are not allowed to suspend any User accounts.
  - Own Account**—Sponsors are allowed to suspend only the User accounts they created.
  - Group Accounts**—Sponsors are allowed to suspend User accounts created by anyone in the same sponsor user group.
  - All Accounts**—Sponsors are allowed to suspend any User accounts.
- **Edit Account**—Choose one of the following permissions for editing the end date/time on User accounts:
  - No**—Sponsors are not allowed to edit any guest accounts.
  - Own Account**—Sponsors are allowed to edit only the User accounts they created.
  - Group Accounts**—Sponsors are allowed to edit User accounts created by anyone in the same sponsor user group.
  - All Accounts**—Sponsors are allowed to edit any User accounts.
- **UnSuspend Account**—Choose one of the following options for suspending accounts:
  - No**—Sponsors are not allowed to unsuspend any User accounts.
  - Own Account**—Sponsors are allowed to unsuspend only the User accounts they created.
  - Group Accounts**—Sponsors are allowed to unsuspend User accounts created by anyone in the same sponsor user group.

**All Accounts**—Sponsors are allowed to unsuspend any User accounts.

- **Reactivate Expired Account :**

**No**—Sponsors are not allowed to reactivate any accounts.

**Own Account**—Sponsors are allowed to reactivate only the accounts they created.

**Group Accounts**—Sponsors are allowed to reactivate accounts created by anyone in the same sponsor user group.

**All Accounts**—Sponsors are allowed to reactivate User accounts.

- **Report & Manage Accounts**—Choose one of the following permissions for viewing reporting details for full reporting. See Reporting on Users for additional details.

**No**—Sponsors are not allowed to view reporting details on any User accounts.

**Own Account**—Sponsors are allowed to view reporting details for only the User accounts they created.

**Group Accounts**—Sponsors are allowed to view active User accounts created by anyone in the same sponsor user group.

**All Accounts**—Sponsors are allowed to view reporting details on any active User accounts.

- **Guest Accounts Detailed Reports-Accounting Log** —Choose one of the following permissions for running a full report on accounting logs:

**No**—Sponsors are not allowed to run accounting log reporting on any User accounts.

**Own Account**—Sponsors are allowed to run full accounting log reporting for only the User accounts they created.

**Group Accounts**—Sponsors are allowed to run full reporting on User accounts created by anyone in the same sponsor user group.

**All Accounts**—Sponsors are allowed to run full accounting log reporting on any active User accounts.

- **Guest Accounts Detailed Reports - Audit Log**—Choose one of the following permissions for running a full report on audit logs:

**No**—Sponsors are not allowed to run an audit log report on logs on any accounts. **Own Account**—Sponsors are allowed to run an audit log report on logs for only the User accounts they created.

**Group Accounts**—Sponsors are allowed to run an audit log report on logs for User accounts created by anyone in the same sponsor user group.

**All Accounts**—Sponsors are allowed to a run an audit log report on logs on any active User accounts.

- **Guest Accounts Detailed Reports - Activity Log**—Choose one of the following permissions for running a full report on activity logs.

**No**—Sponsors are not allowed to run detailed reports on activity logs on any User accounts.

**Own Account**—Sponsors are allowed to run detailed reports on activity logs for only the User accounts they created.

**Group Accounts**—Sponsors are allowed to run a detailed report on activity logs for User accounts created by anyone in the same sponsor user group.

**All Accounts**—Sponsors are allowed to run detailed reports on activity logs on any active User accounts.

- **View Guest Payments Report** - Choose one of the following permissions for viewing User Payments
  - No** - Sponsors are not allowed to run detailed reports on User Payments.
  - Own Account** - Sponsors are allowed to run detailed reports on User Payments for accounts only they have created.
  - Group Accounts** - Sponsors are allowed to run reports on User Payments for only accounts created by anyone in the same sponsor group.
  - All Accounts** - Sponsors are allowed to run reports on User Payments on any active User account.
- **Charge/Refund Paid User Accounts** - Choose one of the following permissions for allowing sponsors to charge or refund paid User accounts.
  - No** - Sponsors are not allowed to charge or refund paid User accounts.
  - Own Account** - Sponsors are allowed to charge or refund paid User accounts on accounts only they have created.
  - Group Accounts** - Sponsors are allowed to charge or refund paid User accounts created by anyone in the same sponsor group.
  - All Accounts** - Sponsors are allowed to charge or refund paid User accounts on any active User account.
- **Concurrent User Reports** –Select Yes to allow the sponsors to run the concurrent User reports. If you select No, the sponsors are not allowed to run the reports.
- **Management Reports**–Select Yes to allow the sponsors to run the management reports. If you select No, the sponsors are not allowed to run the reports.
- **Create Event Codes** - Select Yes to allow the sponsors to Create Event Codes.
- **Edit Event Codes** - Choose one of the following permissions for Editing Event Codes
  - No** - Sponsors are not allowed to Edit Event Codes
  - Own Event Codes** - Sponsors can only Edit Event Codes they create.
  - Group Event Codes** - Sponsors can Edit Event Codes within a Group.
  - All Event Codes** - Sponsors can Edit All Event Codes.
- **Suspend Event Codes** - Choose one of the following permissions for Suspending Event Codes
  - No** - Sponsors are not allowed to Suspend Event Codes.
  - Own Event Codes** - Sponsors can only Suspend Event Codes they create.
  - Group Event Codes** - Sponsors can only Suspend Event Codes in a Group.
  - All Event Codes** - Sponsors can Suspend all Event Codes
- **Manage Event Codes** - Choose one of the following permissions for Managing Event Codes.
  - No** - Sponsors are not allowed to Manage Event Codes
  - Own Event Codes** - Sponsors can only Manage Event Codes they create.
  - Group Event Codes** - Sponsors can only Manage Event Codes in a Group.
  - All Event Codes** - Sponsors Manage all Event Codes.



- **Approve Accounts** - Select Yes to allow the sponsors to Approve Accounts.
  - **Account start time within** - Select the amount of days the account should start in. Specify the time interval in days, hours, or minutes.
  - **Maximum duration of User account**—This specifies the maximum duration for which the sponsor can configure an account. Specify the duration in days, hours, or minutes.
  - **Maximum duration of device account** - This specifies the maximum duration for which the sponsor can configure a device account. Specify the duration in days, hours, or minutes.
  - **Maximum duration restriction calculated from** - From the drop down menu select whether restrictions apply **from current time** or **from start time**.
  - **User Account limit** - Specify the maximum number of allowed active User accounts a sponsor from this group can have at any given time, 0 for unlimited.
  - **Device Account limit** - Specify the maximum number of allowed active device accounts a sponsor from this group can have at any given time, 0 for unlimited.
6. Click the **Save** button to add the group with the permissions specified.

**Note:** Until you click the Save button, the group is not created.

7. Execute one of the following set of instructions to correctly map sponsor users to your group based upon group information from the authentication server:
- Mapping to Active Directory Groups
  - Mapping to LDAP Groups
  - Mapping to RADIUS Groups See “Adding Sponsor User Groups” on page 126.

## Editing Sponsor User Groups

The following steps describe how to edit sponsor user groups.

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** from the left hand menu.
2. Select and highlight the group you wish to edit, then click **Edit Sponsor Group** button to get the screen as shown below

Sponsor Permissions: Sponsor Group One

Group Permissions | Group Mappings | Guest Account Groups | Guest Usage Profiles | Device Account Groups | Device Usage Profiles | Sponsor Preferences

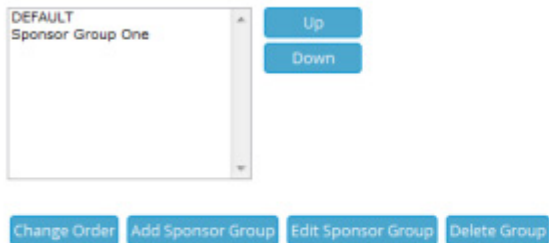
Allow Login:	No
Create Guest Accounts:	No
Create Multiple Guest Accounts:	No
Create Random Guest Accounts:	No
Set Random Account Price:	No
Email Manager on Guest Account Creation:	No
Create Device Accounts:	No
Create Multiple Device Accounts:	No
Email Manager on Device Account Creation:	No
Send Email:	No
Send SMS:	No
View Account Password:	No
Print Account Details:	No
Reset Account Password:	No
Suspend Account:	No
Edit Account:	No

3. Edit and set **Group Permissions**; See “Adding Sponsor User Groups” on page 126. To edit other tabs on this page see See “Managing Sponsor User Groups” on page 134.

## Deleting User Groups

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** from the left hand menu.

## Sponsor Permissions



2. Select and highlight the group you wish to delete and click the **Delete Group** button as shown above.
3. Confirm deletion at the prompt.

**Note:** If any Local Users are part of this group, you must delete the user before deleting the user group. Alternatively, you can move Local Users to another group to “empty” the user group before deleting it.

## Defining the Order of Sponsor User Groups

When a sponsor logs into the FortiConnect, the system checks each group in turn to see if the sponsor should be given the privileges of that group. The groups are processed in the order in which they appear in the Sponsor User Groups list box. If a user does not match a user group, they are given the privileges of the DEFAULT group.

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** from the left hand menu.



2. Select the group you wish to order. Each group can be ordered by clicking the **up** or **down** arrow icon button until the group is in position as shown in above.
3. Repeat for all groups until they appear in the required order.
4. Click the **Change Order** button to save the order.

## Managing Sponsor User Groups

### Mapping to User Groups

#### Mapping to Active Directory Groups

If a sponsor authenticates to the FortiConnect using Active Directory authentication, the FortiConnect can map the sponsors into a user group using their membership in Active Directory groups.

**Note:** FortiConnect does support recursive group lookups.

If you have configured AD authentication (as described in [Configuring Active Directory \(AD\) Authentication](#)), then the FortiConnect automatically retrieves a list of all the groups configured within all the AD servers.

Selecting an Active Directory Group from the dropdown provides all sponsor users in this AD group the permissions assigned to this Sponsor Group.

## Mapping to LDAP Groups

If a sponsor authenticates to the FortiConnect using LDAP authentication, the FortiConnect can map the sponsor into a user group by their membership of LDAP groups.

**Note:** FortiConnect does support recursive group lookups.

Based on the settings of the LDAP server that you authenticate against, the FortiConnect uses one of the following methods for mapping the sponsor using group information.

## Mapping to RADIUS Groups

If a sponsor authenticates to the FortiConnect using RADIUS authentication, the FortiConnect can map the sponsor into a user group by using information returned to the FortiConnect in the authentication request.

The information must be placed into the class attribute on the RADIUS server.

## Mapping the Group

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** from the left hand menu.
2. Select and highlight the group you wish to edit, then click **Edit Sponsor Group** button.
3. Click on the **Group Mappings** tab.
4. Using the rule underneath the Sponsor Group table, shown below, you can create new rules using the Sponsor Authentication methods you have added.

Sponsor Permissions: Sponsor Group One

Group Permissions | **Group Mappings** | Guest Account Groups | Guest Usage Profiles | Device Account Groups | Device Usage Profiles | Sponsor Preferences

The Sponsor will be in this group if they match any of the following rules:

10 per page Go

Server ▲▼	Rule ▲▼
No Group Mappings defined	

If the Sponsor is authenticated against server 10.10.1.2 check class attribute equals Add Rule

- From the drop down menu, select the desired server you wish to create a rule for.
  - Then select whether the group class names **equals** or **contains** the term from the drop down menu.
  - Enter the **term** the mapping should be based on into the empty field and click **Add Rule**.
5. The rule is then added to the table.
  6. To remove a rule click on the bin icon to the right of the rule.

**Note:** By default, Active Directory only returns a maximum of 1000 groups in response to a FortiConnect search. If you have more than 1000 groups and have not increased the LDAP search size, it is possible that the group you want to match does not appear. In this situation, you can manually enter the group name in the Active Directory Group combo box.

## Assigning Guest Account Groups

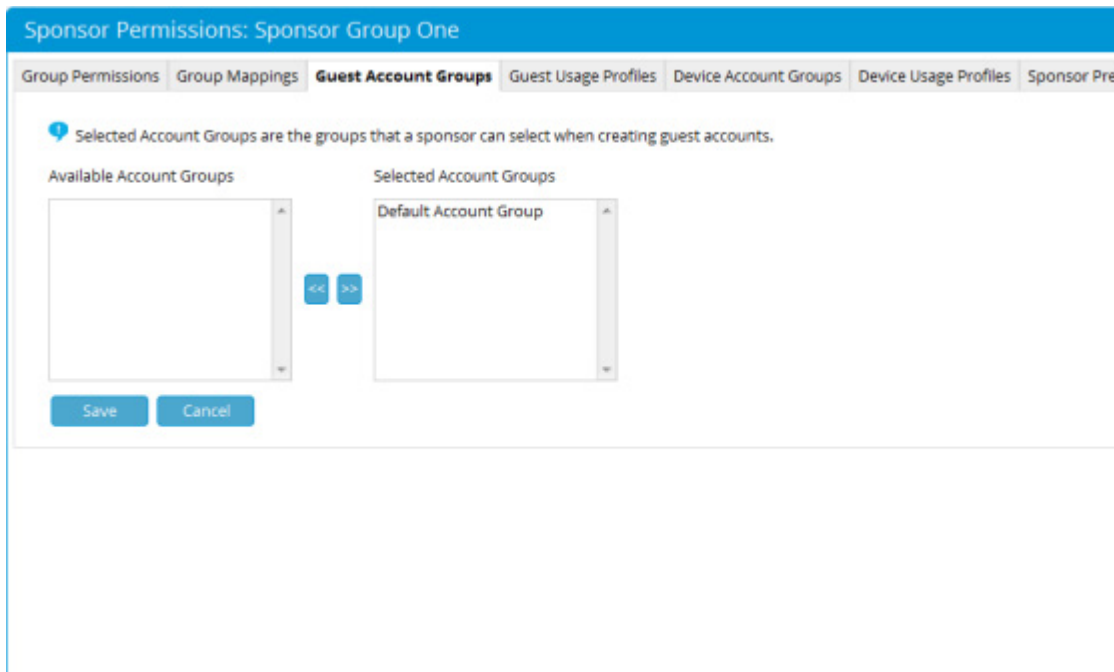
Guest Groups allow a sponsor to assign different levels of access to a User account. You can choose which sponsor user groups are allowed to assign certain profiles to Users.

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.

Each sponsor user group must have the ability to assign Users to at least one role.

If only one role is selected for the user group, the sponsor cannot have the option to select roles. If there is more than one role, sponsors get a dropdown menu to select the role to be assigned to the account during the account creation.

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** from the left hand menu.
2. Select and highlight the group you wish to edit, then click **Edit Sponsor Group** button.
3. Click the **Guest Account Groups** tab to bring up the Available Account groups as shown below.



4. The roles that the sponsor has permission to assign are displayed in the Selected Account Groups list. Move the roles between the Available Account Groups and Selected Account Groups lists using the arrow buttons.
5. Click the **Save** button to assign the permission to create Users in the specified profiles to the sponsor user group.

## Assigning Guest Usage Profiles

Usage Profiles allow a sponsor to assign different levels of access usage to a User account. You can choose 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 choose which additional usage profiles the sponsor can be assigned, or can remove the default usage profile from the user group.

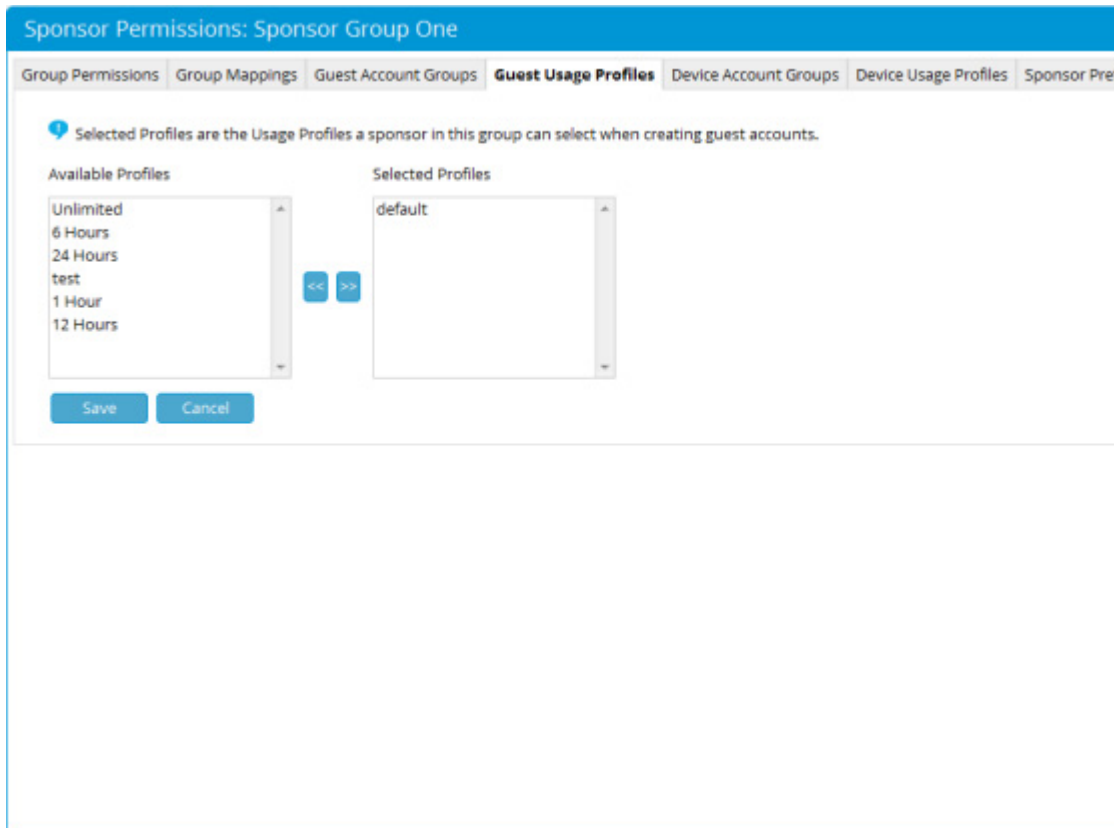
Each user group must have the ability to assign Users in at least one usage profile.

If a user group has only one usage profile selected, the sponsor does not view an option to select the usage profile. If they have the ability to choose more than one usage profile, they can view a dropdown menu from which they can choose the usage profile to be assigned to the account during the account creation.

Refer to [Configuring Usage Profiles](#) for additional details on usage profiles.

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** from the left hand menu.
2. Select and highlight the group you wish to edit, then click **Edit Sponsor Group** button.
3. Click the **Guest Usage Profiles** tab to bring up the Edit Usage Profiles as shown below.





4. The profiles that the sponsor user group has permission to assign are displayed in the Available Profiles list. Move the roles between the Available Profiles and Selected Profiles lists using the arrow buttons.
5. Click the **Save** button to assign the permission to create Users in the usage profiles to the sponsor user group.

## Assigning Device Account Groups

Device Account Groups allow a sponsor to assign different levels of access to a device account. You can choose which sponsor user profiles are allowed to assign certain Account Groups to device accounts.

By default, a sponsor user group has the ability to assign device accounts to the default role. The administrator can choose the additional groups the sponsor can assign, or can remove the default role from the user group.

Each sponsor user group must have the ability to assign Users to at least one role.

If only one group is selected for the user group, the sponsor will not have the option to select groups. If there is more than one group, sponsors get a dropdown menu to select the role to be assigned to the account during the account creation.

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** from the left hand menu.
2. Select and highlight the group you wish to edit, then click **Edit Sponsor Group** button.
3. Click the **Device Account Groups** tab to bring up the Edit Authorization Profiles as shown below.

Sponsor Permissions: Sponsor Group One

Group Permissions | Group Mappings | Guest Account Groups | Guest Usage Profiles | **Device Account Groups** | Device Usage Profiles | Sponsor Preferences

Selected Account Groups are the groups that a sponsor can select when creating device accounts.

Available Account Groups

Selected Account Groups

Default Account Group

Save Cancel

4. The groups that the sponsor user group has permission to assign are displayed in the Selected Account Groups list. Move the groups between the Available Account Groups and Selected Account Groups lists using the arrow buttons.
5. Click the **Save** button to assign the permission to create Users in the specified groups to the sponsor user group.

## Assigning Device Usage Profiles

Device Usage Profiles allow a sponsor to assign different levels of access usage to a device account. You can choose the sponsor user groups that are allowed to assign certain Device Usage Profiles to Users.

By default, a user group has the ability to assign Users to the default device usage profile. The administrator can choose 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.

If a user group has only one usage profile selected, the sponsor does not view an option to select the usage profile. If they have the ability to choose more than one usage profile, they can view a dropdown menu from which they can choose the usage profile to be assigned to the account during the account creation.

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** from the left hand menu.
2. Select and highlight the group you wish to edit, then click **Edit Sponsor Group** button.
3. Click the **Device Usage Profiles** tab to bring up the Edit Usage Profiles as shown below.

Sponsor Permissions: Sponsor Group One

Group Permissions | Group Mappings | Guest Account Groups | Guest Usage Profiles | Device Account Groups | **Device Usage Profiles** | Sponsor Preferences

Selected Profiles are the Usage Profiles a sponsor in this group can select when creating device accounts.

Available Profiles

- Unlimited
- 6 Hours
- 24 Hours
- test
- 1 Hour
- 12 Hours

Selected Profiles

- default

<< >>

Save Cancel

1. The usage profiles that the sponsor user group has permission to assign are displayed in the Available Profiles list. Move the roles between the Available Profiles and Selected Profiles lists using the arrow buttons.
2. Click the **Save** button to assign the permission to create Users in the usage profiles to the sponsor user group.

# Sponsor Preferences

Administrators can restrict/disable or enable controls on a sponsors default preferences page. The section below details the default values for these preferences.

1. From the administration interface, select **Sponsor Portal > Sponsor Permissions** from the left hand menu.
2. Select and highlight the group you wish to edit, then click **Edit Sponsor Group** button.
3. Click the **Sponsor Preferences** tab to bring up the Edit Sponsor Settings as shown below.

The screenshot shows the 'Sponsor Permissions: Sponsor Group One' configuration page. It features a navigation bar with tabs: Group Permissions, Group Mappings, Guest Account Groups, Guest Usage Profiles, Device Account Groups, Device Usage Profiles, and Sponsor Preferences (which is active). Below the navigation bar, a message states: 'These settings assign default values & enable / disable controls on the Sponsor Interface > My Settings > Preferences page'. The main content area is divided into sections: **Language Template**, **Timezone**, **Country Code**, and **Guest Account Groups**. The Language Template section includes a 'Default Language Template' dropdown set to 'English (Default)', an 'Allow sponsor to change' dropdown set to 'Yes', and a template selection interface with 'Available Templates' and 'Currently Selected' lists. The 'Currently Selected' list includes Danish, Hebrew, Ukrainian, Finnish, Spanish, English (Default), Greek, and Czech. The Timezone section has a 'Default Timezone' dropdown set to 'America/Los\_Angeles' and an 'Allow sponsor to change' dropdown set to 'Yes'. The Country Code section has a 'Default Country Code' dropdown set to '+1' and an 'Allow sponsor to change' dropdown set to 'Yes'.

4. Language Template -
  - **Default Template** - Choose a template from the drop down menu provided
  - **Allow Sponsor to change** - Choose **yes** or **no** from the drop down menu.
  - Move any templates you wish to be available to the **currently selected** list by highlighting the template and clicking the correct arrow.
5. Timezone -
  - **Default Timezone** - Select a default timezone from the drop down menu

- provided.
- **Allow Sponsor to change** - Choose **yes** or **no** from the drop down menu.
6. Country Code -
    - **Default Country Code** - Select a default country code from the drop down menu provided.
    - **Allow Sponsor to change** - Choose **yes** or **no** from the drop down menu.
  7. Guest/User Account Group -
    - **Default Group** - Select a default group from the drop down menu provided.
    - **Allow Sponsor to change** - Choose **yes** or **no** from the drop down menu.
  8. Device Account Group -
    - **Default Device Group** - Select a default device group from the drop down menu provided.
    - **Allow Sponsor to change** - Choose **yes** or **no** from the drop down menu.
  9. Email Address -
    - Enter a check in the **Retrieve from LDAP** box if this function is required.
    - **Allow Sponsor to change** - Choose **yes** or **no** from the drop down menu.
  10. Email Confirmation -
    - **Default setting** - Select a default setting from the drop down menu provided
    - **Allow Sponsor to change** - Choose **yes** or **no** from the drop down menu.
  11. Login Page -
    - **Default page** - Select a default page from the drop down menu provided.
    - **Allow Sponsor to change** - Choose **yes** or **no** from the drop down menu.
  12. Click on the **Save** button to save all changes.

## Currency Denomination for Access Codes

In some environments, credit card based purchases are not widely used, and there is a larger interest in using access codes with currency denominations attached to them.

FortiConnect can set a Currency Denomination which will allow a sponsor to create multiple numbers of random User accounts assigned to a time profile, and then export them to a CSV file to print and create an offline coupon or scratch card to distribute to the User.

1. From the FortiConnect Administration Interface go to **Sponsor Portal --> Currency** as shown below.

## Currency Settings

Sponsor Portal Currency:

Save

2. From the dropdown menu, select the **Sponsor Portal Currency** you wish to set.

# Customizing the Application

---

This chapter describes the following

- User Interface Templates
- Adding a User Interface Template
- Editing a User Interface Template
- Deleting a Template
- Setting the Default Interface Mapping
- Setting User Default Redirection
- Session Time outs
- Login Page Message

# Configuring User Interface Templates

FortiConnect allows you to customize the sponsor user interface text and User notification text using User Interface Templates. You can:

- Change the labels for the sponsor interface.
- Provide different instructions for users.
- Change the default Acceptable Use Policy.
- Create a translated template to provide the sponsor interface and User instructions in another language altogether.

FortiConnect provides a several template's (in English) that can be used as is without any further modification. If you want to change the default presentation for sponsors and Users, you can add one or multiple templates that you can store separately on the FortiConnect and modify as desired.

Typically, you create a customized template when you need to modify the account details and instructions that are provided to the User, such as the Acceptable Usage Policy. FortiConnect provides Print, Email, and SMS templates that allow you to customize the information that is printed, emailed, or text messaged to Users.

If you are customizing the interface for another language, create a new template for the language and edit all pages with the translated text.

Once your user interface template is configured, you need to set the default template mapping so

that the FortiConnect starts using the correct template. Once a sponsor has authenticated, the sponsor can choose a different template to use and save it under **My Settings > Preferences > Language Template** in the sponsor interface. This enables each sponsor to have the application displayed in a different template or language.

**Note:** You can set the default user interface template globally for the FortiConnect sponsor and User interfaces under User Interfaces > User Defaults.

**TIP** - When customizing, it is a good idea to open the sponsor interface in a second browser for reference. This allows you to view how the configuration tabs map to the actual sponsor interface pages. You can bring up the sponsor interface by entering the FortiConnect IP address without the “/admin” as the URL, for example, `http://<forticonnect_ip_address>` or `https://<forticonnect_ip_address>`. The sponsor must logout and login again to view the changes.

## Adding a User Interface Template

When you add a new template, it is automatically based on the default template to facilitate editing.

1. From the administration interface, select **Sponsor Portal > Language Templates** from the left hand menu.

2. On the User Interface Templates page as shown below, click the **Add Template** button.



3. In the Add New Template page as shown below, type a Template Name. This can be any descriptive text to identify the template later from the User Interface Templates list as shown above.



## Add Template

Template Name:

Add

Cancel

4. Click the **Add Template** button.

The Edit User Interface Template page for the new template is displayed, initially, with all details copied from the default template. If you only need to make small changes, this allows you not to have to retype all the entries.




























5. Modify these settings as desired, as described in [Editing a User Interface Template](#).
6. FortiConnect also allows you to Import a template, this can be done by clicking on the **Import Template** button.

## Editing a User Interface Template

1. From the administration interface, select **Sponsor Portal > Language Templates** from the left hand menu.

## Language Templates

Showing 31-39 of 39 10 per page Go

Template Name ▲▼	
<a href="#">Slovak</a>	  
<a href="#">Spanish</a>	  
<a href="#">Swedish</a>	  
<a href="#">Thai</a>	  
<a href="#">Turkish</a>	  
<a href="#">Ukrainian</a>	  
<a href="#">Urdu</a>	  
<a href="#">User Template One</a>	  
<a href="#">Vietnamese</a>	  

Page 4 of 4 Go

[Add](#) [Import](#)

2. From the User Interface Templates list as shown above, click the underlined name of the template you wish to edit.
3. The Edit Home Page for the template is displayed as shown below.

Language Templates: User Template One

Home Menu Reporting Notification Sponsor Settings Guest Accounts Device Accounts Event Codes Common Getting Started Timezones Phone

About:	About
Application Title:	Meru Connect
Login:	Login
Logout:	Logout
Username:	Username
Password:	Password
Version:	Version
Serial Number:	Serial Number
Logged Out:	You are logged out
Not Logged In:	Not logged in
Username or Password required:	You must enter a username and password
Username or Password invalid:	Your username or password is invalid

Save Cancel

4. Click the menu tabs at the top of the page to select any of the sponsor page settings that you want to edit.
5. Make any changes to the fields and click the **Save** button. Some example edits are described in the following sections:
  - Editing the Guest Print Template
  - Editing the Guest Email Template
  - Editing the Guest SMS Template

**Note:** The Upload Logo feature allows upload an image with maximum height of 75 pixels and maximum width of 150 pixels. The image can be in .png, .jpg, or .gif format.

## Editing the Guest Print Template

The Guest Print Template page contains the User account details that the sponsor can bring up in a browser to print out for handing to the User after the account is created. The page is configured in HTML and can be fully customized.

TIP - Navigating to Account Management > Manage Accounts on the sponsor interface and clicking the Print button next to the User account entry brings up the output of the Print Template for printing.

1. Go to **Sponsor Portal > Language Templates** and click the underlined name of the template you wish to edit in the Templates list.
2. Under **Edit Home Page**, click the **Notification** tab to bring up the **Edit Notification Page** as shown below.
3. From the **Select Template** for dropdown menu, choose **Guest Print Template** and click the **Show** button.

Language Templates: User Template One

Home Menu Reporting **Notification** Sponsor Settings Guest Accounts Device Accounts Event Codes Common Getting Started Timezones Phone Codes

The following variables should be used to customise the e-mail message:

- %USERNAME%
- %PASSWORD%
- %PAYMENTAMOUNT%
- %STARTTIME%
- %ENDTIME%
- %TIMEZONE%
- %FIRSTNAME%
- %LASTNAME%
- %MOBILENUMBER%
- %MOBILENUMBER\_ONLY%
- %COUNTRYCODE%
- %TIMEPROFILE%
- %OPTION1%
- %OPTION2%
- %OPTION3%
- %OPTION4%
- %OPTION5%
- %DATAUSAGE\_UP%
- %DATAUSAGE\_DOWN%
- %DATAUSAGE\_TOTAL%

Select Template for: Guest Print Template (Start End/From Creation)

Email Subject: Guest User Account Details

You don't have permission to send Email messages: You don't have permission to send Email messages

Email Text Only Body: The following guest user account has been created for you  
Username: %USERNAME%

4. In the Page Body text field, edit the default HTML code for the web page. The Page Body contains all the HTML code that appears between the BODY tags on a HTML page. All HTML code outside these tags is used by the application.
5. In the HTML code you can use the following special variables to replace them with the details from the created User account.
  - %USERNAME% = The Username created for the User.
  - %PASSWORD% = The Password created for the User.
  - %STARTTIME% = The time from which the User account will be valid.
  - %ENDTIME% = The time at which the User account will expire.
  - %FIRSTNAME% = The first name of the User.
  - %LASTNAME% = The last name of the User.
  - %TIMEZONE% = The timezone of the user.
  - %MOBILENUMBER% = The mobile number of the User.
  - %OPTION1% = Optional field 1.

- %OPTION2% = Optional field 2.
- %OPTION3% = Optional field 3.
- %OPTION4% = Optional field 4.
- %OPTION5% = Optional field 5.
- %MOBILENUMBER\_ONLY% = Mobile phone number of User without country code prepended.
- %COUNTRYCODE% = Country code of the mobile phone number.
- %DURATION% = Duration of time for which the account will be valid.
- %ALLOWEDWINDOW% = The time window during which the account can be used after first login.
- %TIMEPROFILE% = The name of the time profile assigned.

6. Click the **Save** button to save your changes.

## Editing the Guest Email Template

The Guest Email Template page contains the User account details that the sponsor can email to the User after creating the account.

TIP - Navigating to Account Management > Manage Accounts on the sponsor interface and clicking the Email button next to the User account entry brings up the output of the Email Template and also emails the User.

1. Go to **Sponsor Portal > Language Templates** and click the underlined name of the template you wish to edit in the Templates list.
2. Under **Edit Home Page**, click the **Notification** tab to bring up the **Edit Notification Page** as shown below.
3. From the **Select Template** for dropdown menu, choose **Guest Email Template** and click the **Show** button.

Language Templates: User Template One

Home Menu Reporting **Notification** Sponsor Settings Guest Accounts Device Accounts Event Codes Common Getting Started Timezones Phone Codes

The following variables should be used to customise the e-mail message:

- %USERNAME%
- %PASSWORD%
- %PAYMENTAMOUNT%
- %DURATION%
- %FIRSTNAME%
- %LASTNAME%
- %MOBILENUMBER%
- %MOBILENUMBER\_ONLY%
- %COUNTRYCODE%
- %TIMEPROFILE%
- %OPTION1%
- %OPTION2%
- %OPTION3%
- %OPTION4%
- %OPTION5%
- %DATAUSAGE\_UP%
- %DATAUSAGE\_DOWN%
- %DATAUSAGE\_TOTAL%

Select Template for:

Email Subject:

You don't have permission to send Email messages:

Email Text Only Body:

4. Change the Email Subject as desired.
5. In the Email Body text field, edit the default email text to be sent to the guest page.
6. In the Email Body you can use the following special variables to replace them with the details from the created User account.
  - %USERNAME% = The Username created for the User.
  - %PASSWORD% = The Password created for the User.
  - %STARTTIME% = The time from which the User account will be valid.
  - %ENDTIME% = The time at which the User account will expire.
  - %FIRSTNAME% = The first name of the User.
  - %LASTNAME% = The last name of the User.
  - %TIMEZONE% = The timezone of the user.
  - %MOBILENUMBER% = The mobile number of the User.
  - %OPTION1% = Optional field 1.
  - %OPTION2% = Optional field 2.
  - %OPTION3% = Optional field 3.
  - %OPTION4% = Optional field 4.
  - %OPTION5% = Optional field 5.

- %MOBILENUMBER\_ONLY% = Mobile phone number of User without country code pre- pended.
- %COUNTRYCODE% = Country code of the mobile phone number.
- %DURATION% = Duration of time for which the account will be valid.
- %ALLOWEDWINDOW% = The time window during which the account can be used after first login.
- %TIMEPROFILE% = The name of the time profile assigned.

7. Click the **Save** button to save your changes

## Editing the Guest SMS Template

The Guest SMS Template page contains the User account details that the sponsor can text message to the User after creating the account. The contents of the text message can be fully customized.

TIP - Navigating to Account Management > Manage Accounts on the sponsor interface and clicking the SMS button next to the User account entry brings up the output of the SMS Template and also text messages the User.

1. Go to **Sponsor Portal > Language Templates** and click the underlined name of the template you wish to edit in the Templates list.
2. Under **Edit Home Page**, click the **Notification** tab to bring up the **Edit Notification Page** as shown below.
3. From the Select Template for dropdown menu, choose **Guest SMS Template** and click the **Show** button.

Language Templates: User Template One

Home Menu Reporting **Notification** Sponsor Settings Guest Accounts Device Accounts Event Codes Common Getting Started Timezones Phone Codes

The following variables should be used to customise the e-mail message:

- %USERNAME%
- %PASSWORD%
- %PAYMENTAMOUNT%
- %STARTTIME%
- %ENDTIME%
- %TIMEZONE%
- %FIRSTNAME%
- %LASTNAME%
- %MOBILENUMBER%
- %MOBILENUMBER\_ONLY%
- %COUNTRYCODE%
- %TIMEPROFILE%
- %OPTION1%
- %OPTION2%
- %OPTION3%
- %OPTION4%
- %OPTION5%
- %DATAUSAGE\_UP%
- %DATAUSAGE\_DOWN%
- %DATAUSAGE\_TOTAL%

Select Template for:

SMS Subject:

SMS Destination:

You don't have permission to send SMS messages:

SMS Body:

4. Change the SMS Subject as desired.
5. Change the SMS Destination to be the email address of the SMS gateway that you use.

To send the text message to the mobile phone number of the User, use the variable %MOBILENUMBER%. The %MOBILENUMBER% variable is replaced by the mobile phone number, including country code of the User as entered by the sponsor. For example, if the country code selected is the UK (+44) and the User's phone number is 055 555-5555, then %MOBILENUMBER% will contain 4455555555.

**Note:** The initial plus symbol (+) is not inserted and the initial 0, any spaces, or hyphens (-) are removed from the phone number. If you need (+) to be inserted, then enter +%MOBILENUMBER%.

6. The SMS Body contains the SMS text to be sent to the User. In the SMS Body you can use the following special variables to replace them with the details from the created User account.
  - %USERNAME% = The Username created for the User.
  - %PASSWORD% = The Password created for the User.
  - %STARTTIME% = The time from which the User account will be valid.
  - %ENDTIME% = The time at which the User account will expire.
  - %FIRSTNAME% = The first name of the User.



- %LASTNAME% = The last name of the User.
- %TIMEZONE% = The timezone of the user.
- %MOBILENUMBER% = The mobile number of the User.
- %OPTION1% = Optional field 1.
- %OPTION2% = Optional field 2.
- %OPTION3% = Optional field 3.
- %OPTION4% = Optional field 4.
- %OPTION5% = Optional field 5.
- %MOBILENUMBER\_ONLY% = Mobile phone number of User without country code pre- pended.
- %COUNTRYCODE% = Country code of the mobile phone number.
- %DURATION% = Duration of time for which the account will be valid.
- %ALLOWEDWINDOW% = The time window during which the account can be used after first login.
- %TIMEPROFILE% = The name of the time profile assigned.

7. Click the **Save** button to save your changes.

## Deleting a Template

1. From the administration interface, select **Sponsor Portal > Language Templates** from the left hand menu.
2. Select the template you want to delete from the User Interface Templates list and click the **dustbin** icon to the right of the template name field.
3. Confirm deletion of the template.

## Setting the Sponsor Interface Defaults

1. From the administration interface, select **Sponsor Portal > Interface Settings** to bring up the Sponsor Defaults page as shown below and click on the **Sponsor Defaults** tab.

Interface Settings

Sponsor Defaults Login Page Message

Default Language Template: English (Default) ▾

Default Theme: Default Meru Connect ▾ 🔍

Default High Contrast Theme: Default Meru Connect High Contrast ▾ 🔍

Save

2. Select the **Default Language Template** from the drop down menu provided. Default will be selected if no Default Language Templates have been created. This is used for the login screen and the template the sponsor uses the first time they login.
3. Select the **Theme** from the drop down menu provided. Default will be selected if no themes have been created. Click on the **preview** link to see what your theme will look like before applying.
4. Select the **High Contrast Theme** from the drop down menu provided. Default will be selected if no High Contrast Themes have been created. Click on the **preview** link to see what your theme will look like before applying.
5. Click the **Save** button.

## Sponsor Themes

---

























Sponsor Themes can be created specifically for your organizations branding needs and are stored on the FortiConnect.

1. From the administration interface go to **Sponsor Portal > Themes** as show below.

## Themes

To set Sponsor Themes go to [Sponsor Defaults](#).

Showing 1-6 of 6 10 per page Go

Theme Name ▲ ▼	Description	
Default		   
Default High Contrast		   
Default Meru		   
Default Meru Connect		   
Default Meru Connect High Contrast		   
Default Meru High Contrast		   

Page 1 of 1 Go

Import Theme

2. A list of Sponsor Themes are shown:
  - Click on the **Disk** icon to Copy the selected theme.
  - Click on the **Edit** icon to Edit the selected theme
  - Click on the **Export** Icon to Export the selected theme.
  - Click on the **Bin** icon to Delete the selected theme.
  - Click on the **Preview** link to Preview the selected theme.
3. To set a Sponsor Theme from the list see the Sponsor Defaults Section.
4. To import a theme that has been created specifically for your requirements, click on the **Import Theme** button and locate and select your theme.

**Note:** Themes can be created and then imported onto the FortiConnect database to suit your organizations specific requirements.

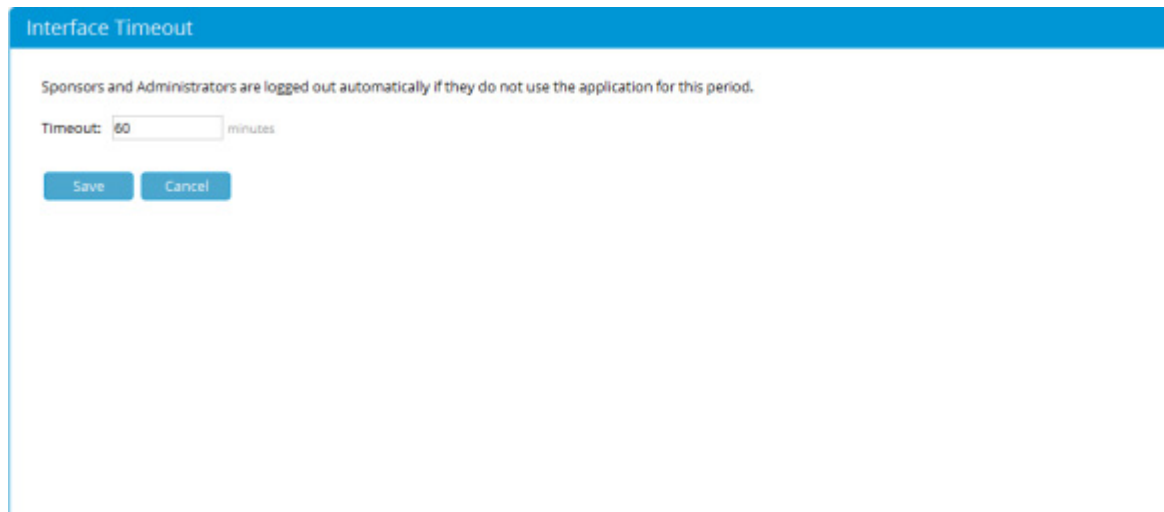
# Session Timeouts

---

A sponsor or administrator that logs in to the FortiConnect is logged out after a period of inactivity. You can set the inactivity period through the Session Timeout Settings page.

**Note:** The Session Timeout defined here applies to both the Sponsor and Administration interfaces.

1. From the administration interface, select **Server > Interface Timeout** from the menu as shown below.



Interface Timeout

Sponsors and Administrators are logged out automatically if they do not use the application for this period.

Timeout:  minutes

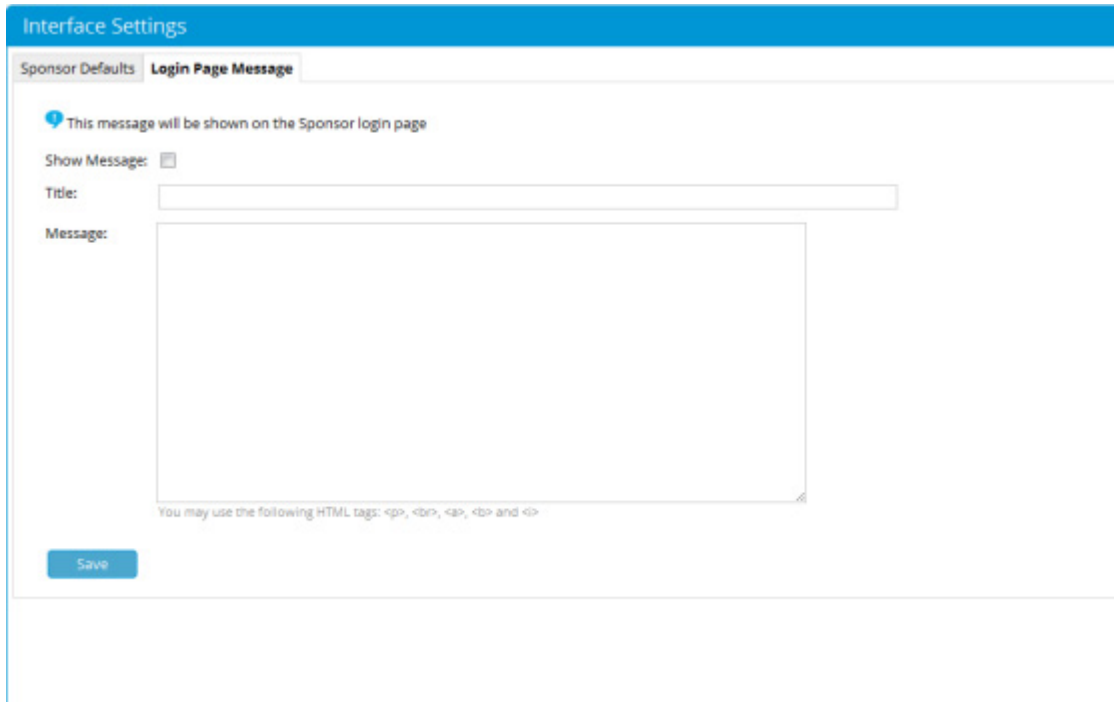
2. Enter the Session Timeout value in minutes (default is 10 minutes). When users are inactive for this amount of time, their sessions expire and the next action they perform takes them to the login page.
3. Click the **Save** button to save the session timeout.

# Login Page Message

---

Administrators can place a message onto the Sponsors login page if they need to be alerted or notified of anything.

1. From the Admin interface, go **Sponsor Portal-->Interface Settings** and click on the **Login Page Message** tab.



The screenshot displays the 'Interface Settings' page with the 'Login Page Message' tab selected. A blue header bar contains the text 'Interface Settings'. Below the header, there are two tabs: 'Sponsor Defaults' and 'Login Page Message'. A blue notification icon with a speech bubble contains the text 'This message will be shown on the Sponsor login page'. Below this, there is a 'Show Message:' label followed by an unchecked checkbox. Underneath, there is a 'Title:' label followed by a text input field. Below that, there is a 'Message:' label followed by a large text area. At the bottom of the text area, there is a small note: 'You may use the following HTML tags: <p>, <br>, <a>, <b> and <i>'. At the bottom left of the form, there is a blue 'Save' button.

2. To display a message on the Sponsor Interface place a check in the **Show Message** check box.
3. Enter a Title of your message in the **Title** field.
4. Enter the content of your message into the **Message** field.
5. Click **Save** when completed.



# Network Access Policy

## Configuring Authentication Policy

---

FortiConnect allows Users to be authenticated via either the internal User database or an external authentication server if required. For an authentication attempt against FortiConnect each server is tried in order against the relevant domain. If an external server rejects the authentication attempt then the user is rejected by FortiConnect. If a server does not respond the next server in the realm is tested.

### Adding Authentication Servers

To add an external authentication server for Authentication go to **Network Access Policy --> Authentication Policy** from the FortiConnect Administration Interface.

Authentication Policy

For every authentication the user credentials are verified in the following order:

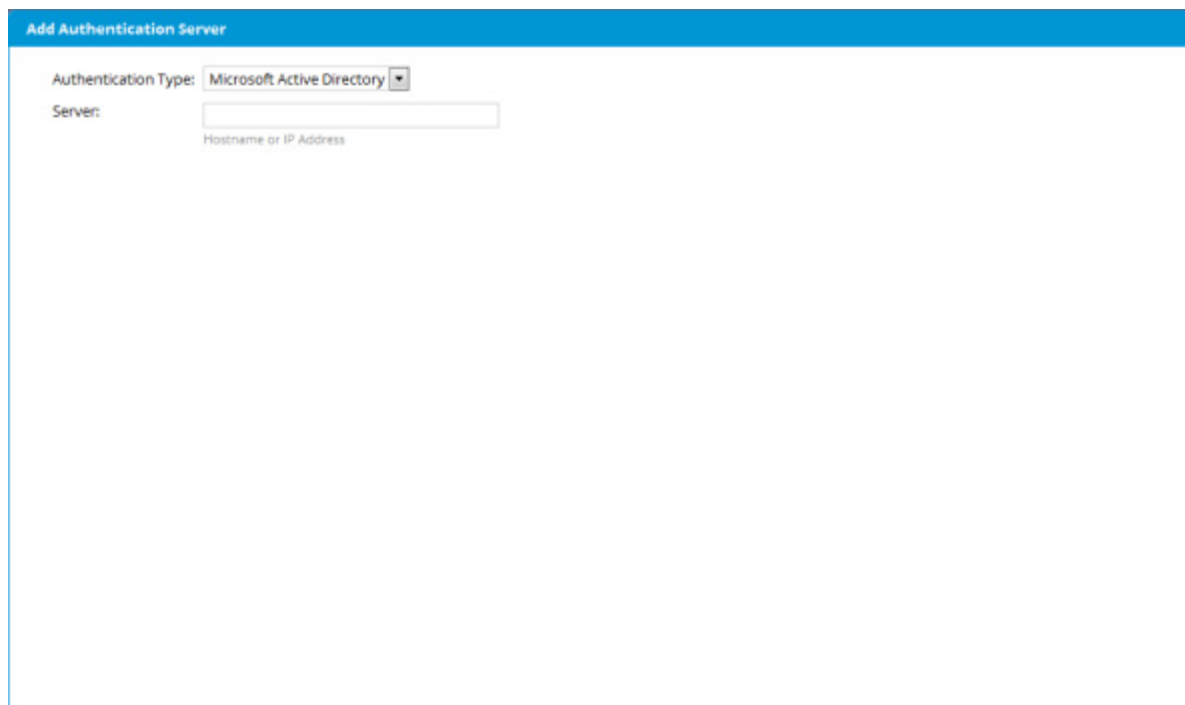
- Servers that match the realm of the user account. For example if the username was user@realm then the account would be verified against each server for that realm until a success or reject is received.
- If a Server does not respond, then the next server for the realm is tried.

Order	Enabled	Name	Type	Server	Realm
No authentication servers defined					

Add Server... Save Order Cancel

1. Click on the **Add Server** button and select what type of server you wish to add from the drop down menu provided

**Note:** For this example we will add a Microsoft Active Directory server, other parameters maybe required when adding other types of Authentication Servers



The screenshot shows a web form titled "Add Authentication Server" with a blue header. Below the header, there are two main input fields. The first is labeled "Authentication Type:" and has a dropdown menu currently showing "Microsoft Active Directory". The second is labeled "Server:" and is an empty text box. Below the "Server:" text box, the text "Hostname or IP Address" is displayed in a smaller font, serving as a placeholder or hint for the user.

2. Enter the **hostname** or **IP address** of the server and click on **next**



## Add Authentication Server

Name:

Server Type: Microsoft Active Directory

Server: 10.10.1.2

Domain: identitynetworks.com

Encryption:

This server supports encryption, but its certificate cannot be validated. You must upload its certificate or its root certificate to continue:

Certificate:  No file chosen

Base DN:

3. Select additional details from the drop down menus provided
  - **Encryption** - From the drop down menu select which encryption method the server will use.
  - **Base DN** - From the drop down menu select the Base DN the server will use from the options provided.
4. Click on **Next** and then enter the **username** and **password** of the server.

## Add Authentication Server

### Connection

Name: 10.10.1.2  
Server Type: Microsoft Active Directory  
Server: 10.10.1.2  
Domain: identitynetworks.com  
Encryption: None  
Base DN: DC=identitynetworks,DC=com

### Search Credentials

Username: @identitynetworks.com

Password:

< Back

Next >

Exit

5. Enter any attribute mappings required for the server and then map them to the **usage profile** you require and also set the **Account Group**.

## Add Authentication Server

### Connection

Name: 10.10.1.2  
Server Type: Microsoft Active Directory  
Server: 10.10.1.2  
Domain: identitynetworks.com

### Attribute Mappings

The response from the external server is tested against each rule below in order. If a rule is matched the specified usage profile and account group are applied and guest authentication succeeds.

- 1 If group name equals  set usage profile to  and account group to
- 2 If no rules match Reject authentication

[add mapping](#)

< Back

Next >

Exit

6. Autocomplete will assist you when entering your rules.
7. Continue to add rules and then click **Next** once complete.

**Add Authentication Server**

**Connection**

Name: 10.10.1.2  
Server Type: Microsoft Active Directory  
Server: 10.10.1.2  
Domain: identitynetworks.com

---

**Secure Authentication**

To enable MSCHAPv2 authentication from Windows clients this server must be joined to the AD domain. This is not required for EAP-TLS authentication.

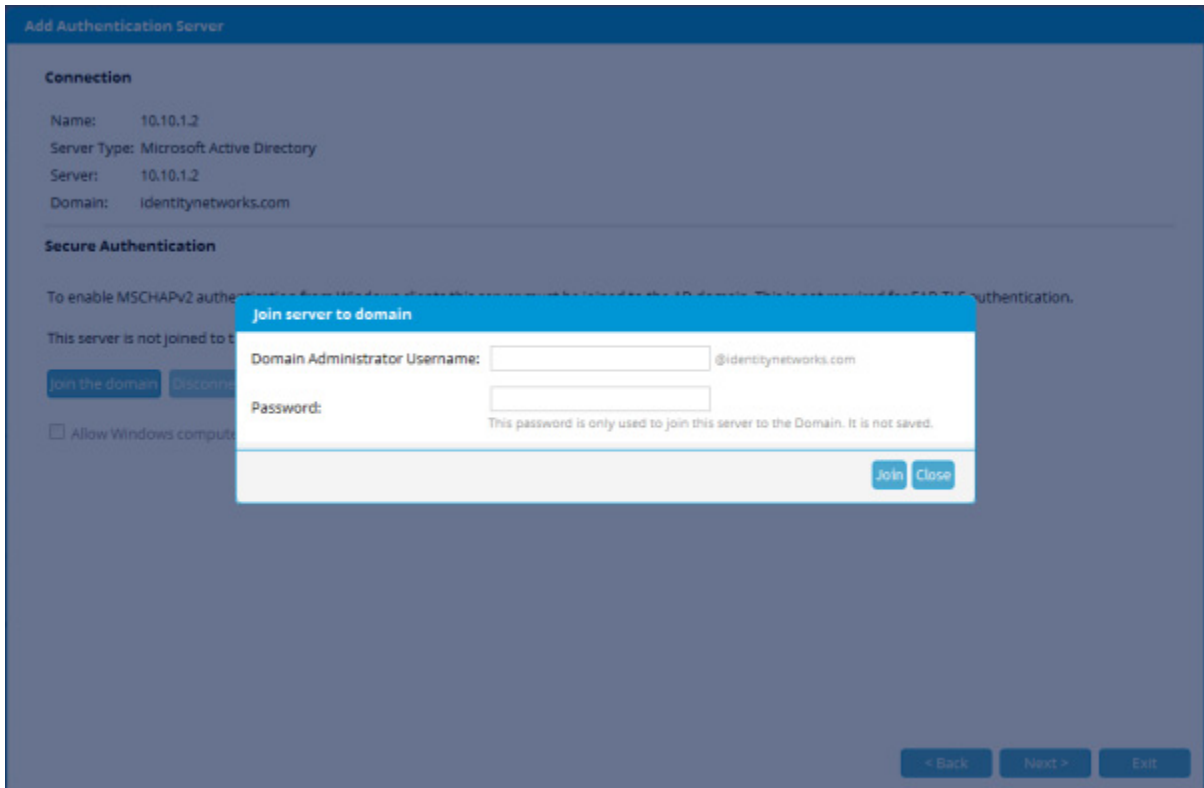
This server is not joined to the domain.

[Join the domain](#) [Disconnect from the domain](#)

Allow Windows computer authentication (machine/host authentication)

[< Back](#) [Next >](#) [Exit](#)

8. Place a check in **Allow Windows computer authentication** to allow the authentication server to allow machine/host authentication.
9. Click on the **Join Domain** to join the server to the domain as shown below.



**10.** Enter the **Domain Administrator Username** and **Password** then click on **Join**.

**11.** You will then be presented with a screen as shown below, this is to allow **EAP-TLS authentication**,

## Add Authentication Server

### Connection

Name: 10.10.1.2  
Server Type: Microsoft Active Directory  
Server: 10.10.1.2  
Domain: identitynetworks.com

### EAP-TLS Authentication

Certificate Authorities: No Certificate Authorities defined

CA Certificates:

<input type="checkbox"/>	Class 3 Public Primary Certification Authority
<input type="checkbox"/>	Class 3 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc. - FC
<input type="checkbox"/>	DigiCert High Assurance CA-3
<input type="checkbox"/>	DigiCert High Assurance EV Root CA
<input type="checkbox"/>	Entrust Certification Authority - L1C
<input type="checkbox"/>	Entrust.net Certification Authority (2048)
<input type="checkbox"/>	Entrust.net Secure Server Certification Authority
<input type="checkbox"/>	Equifax Secure Certificate Authority
<input type="checkbox"/>	GeoTrust Global CA
<input type="checkbox"/>	Thawte DV SSL CA

Upload a CA certificate:  No file chosen

< Back

Next >

Exit

12. You will be required to determine your EAP-TLS Authentication method, if this does not apply to you, then click on next to complete setup.

- **Certificate Authorities** - FortiConnect allows you to define a SCEP server or to define an internal CA authority method. Any that have been setup within FortiConnect will be displayed in this drop down menu. Select your appropriate method.
- **CA Certificates** - Place a check in the check box next to any CA Certificates you wish to install.
- **Upload a CA Certificate** - Click on the choose file button and manually select a CA certificate to install.

13. Click **Next** to continue.

**Note:** If no certificates are installed then installation is now complete.

## Add Authentication Server

To configure client certificates you can upload a sample user certificate. By inspecting this certificate the system will automatically determine how to map the client certificate to a user on an authentication server.

### Parse a sample PKCS#12 file

PKCS#12 File:  No file chosen

Files usually end in a p12 or pkcs12 extension

Password:

The password is only used to extract the certificate from the PKCS#12 file. It is not stored.

### Parse a sample X.509 certificate in PEM or DER format

Certificate:  No file chosen

Files usually end in a pem, cer, der or crt extension

< Back

Next >

Exit

14. To configure client certificates you can upload a sample user certificate. By inspecting this certificate the system will automatically determine how to map the client certificate to a user on an authentication server.
- **Parse a sample PKCS#12 file** - Select and browse to Parse a sample PKCS#12 file. Enter the relevant password and click **next** to continue.
  - **Parse a sample X.509 certificate in PEM or DER format** - Select and browse to Parse sample X.509 certificate in PEM or DER format and click **next** to continue.

#### Sample Client Certificate

Common Name (CN): John Carter  
Subject DN: /C=GB/ST=Greater Manchester/L=Manchester/O=Meru Networks/OU=Identity Manager/CN=John Carter/emailAddress=jcarter@merunetworks.com  
Parsed Subject DN: CN=John Carter,OU=Identity Manager,O=Meru Networks,L=Manchester,ST=Greater Manchester,C=GB  
Email Address: jcarter@merunetworks.com  
User ID: <Not part of certificate>  
User Principal Name: upn@identitynetworks.com

Find user on server by mapping Client Certificate  to user attribute  .

[Advanced >](#)

#### User Search Results

User found  
CN: John Carter  
DN: CN=John Carter,CN=Users,DC=identitynetworks,DC=com  
Email Address: john@identitynetworks.com  
Username: john  
User Principal Name: john@identitynetworks.com

15. This will match the certificate with a user. Click on **Next** to continue.

#### Certificate Matching

Some authentication servers have the client certificate of each user. We can compare that certificate with the one supplied by the browser and the user will only be logged in if the certificates match.

This authentication server does not appear to store the user's certificate.

Verify the user's certificate stored on the server matches the client certificate supplied by the browser.

< Back

Next >

Exit



**16.** Some authentication servers have the client certificate of each user. We can compare that certificate with the one supplied by the browser and the user will only be logged in if the certificate matches. To verify if the users certificate stored on the server matches the client certificate by the browser then place a check in the check box.

**17.** Click on **Next** to continue..

**18.** To allow secure connections from Windows clients the server must be added to the AD domain.

**Note:** FortiConnect supports MSCHAPv2 authentication so that a Windows client can connect to a controller that uses the FortiConnect as a RADIUS server that in turns authenticates against an Active Directory server.

FortiConnect supports authentication from users in domains that are trusted by the domain that FortiConnect is joined to, so if Domain A trusts Domain B, then users from Domain B can also be authenticated to the FortiConnect.

**19.** Once the server has been added click on **Next** and then click on the **Close** button.

## Adding an External Database

FortiConnect allows an External Database to be configured for external authentication.

To add an external database for authentication go to **Network Access Policy --> Authentication Policy** from the FortiConnect Administration Interface.

## Authentication Policy

For every authentication the user credentials are verified in the following order:

- Servers that match the realm of the user account. For example if the username was user@realm then the account would be verified against each server for that realm until a success or reject is received.
- If a Server does not respond, then the next server for the realm is tried.

Order	Enabled	Name	Type	Server	Realm	
No authentication servers defined						

Add Server...

Save Order

Cancel

1. Click on the **Add Server** button and select **External Database**.

Add Authentication Server

Authentication Type: External Database

< Back   Next >   Exit

2. Click on **Next** to continue.

**Add Authentication server**

**Connection**

Name:

Authentication Type: External Database

Type:

Server IP Address:

Port:

Leave blank to use selected type's default port.

Username:

Password:

Database Name:

**Data Queries**

- A user is authenticated if the authentication query returns a row.
- If any of the following columns are set in that row they are applied to the generated account: **first\_name**, **last\_name**, **email**, **phone** and **country\_phone\_code**.
- The optional group query shall return 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.
- Query parameters **username** and **password** are required in the authentication query.
- Query parameter **username** is required in the group query.

Authentication Query:

Group Query:

[Test Settings](#)

[Back](#) [Next](#) [Test](#)

- Enter the required credentials in the fields provided -
  - Name** - Enter the name of your External Database
  - Type** - From the drop down menu select the type of external database
  - Server IP Address** - Enter the server IP Address
  - Port** - Enter the required port number, leave blank to use the selected types default port
  - Username** - Enter the required username
  - Password** - Enter the required password
  - Database Name** - Enter the database name
- Define the **Authentication Query** and **Group Query** required to get user groups from the database.
- Click on the **Test Settings** button to check your settings are correct.
- Click on **Next** to continue.

**Add Authentication Server**

**Connection**

Name: Test Server  
 Authentication Type: External Database  
 Server: 10.10.1.2  
 Type: Microsoft SQL Server

---

**Login Parameters**

Realm:

Authenticates with: *username*

---

**Group Mappings**

The user group(s) returned by external database server is tested against each rule below in order. If a rule is matched the specified usage profile and account group are applied and guest authentication succeeds.

1 If group name equals  set usage profile to  and account group to

2 If no rules match Reject authentication

[add Rule](#)

7. Enter the Login Parameters required -
  - **Realm** - Enter the Realm
8. Enter the relevant **Group Mappings** required, each user group returned will be tested against each rule created in order.
9. Use the drop down menu to select and amend rules.
10. Click on the **add rule** link to add further rules.
11. Click **Next** once complete.
12. Click on **Close** to complete.


## Deleting the External Database

To **delete** an External Authentication server once its has been added go to **Network Access Policy --> Authentication Policy** from the FortiConnect Administration interface

## Authentication Policy

For every authentication the user credentials are verified in the following order:

- Servers that match the realm of the user account. For example if the username was user@realm then the account would be verified against each server for that realm until a success or reject is received.
- If a Server does not respond, then the next server for the realm is tried.

Order	Enabled	Name	Type	Server	Realm	
1	<input checked="" type="checkbox"/>	Test Server	External Database	10.10.1.2	test	

Add Server...

Save Order

Cancel

Click on the **bin** icon to the right of the server you wish to delete and click on **yes** at the prompt.

## 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.

To add a RADIUS or a RadSec authentication server go to **Network Access Policy --> Authentication Policy** from the FortiConnect Interface as shown below.

## Authentication Policy

For every authentication the user credentials are verified in the following order:

- Servers that match the realm of the user account. For example if the username was user@realm then the account would be verified against each server for that realm until a success or reject is received.
- If a Server does not respond, then the next server for the realm is tried.

Order	Enabled	Name	Type	Server	Realm	
1		<a href="#">Test_Server</a>	External Database	10.10.1.2	test	

Add Server...

Save Order

Cancel

### 1. Click on the **Add Server** button

**Note:** Only the first two screen shots differ for RADIUS and RadSec. For documentation purposes we will document the different screenshots, then continue with the setup which is the same for both RADIUS and RadSec from step 10 onwards

# RADIUS Authentication Server

**Add Authentication Server**

Authentication Type:

Server:

Hostname or IP Address

< Back   Next >   Exit

2. Enter the Hostname or IP Address of the RADIUS server.
3. Click on Next



**Add Authentication Server**

Name:

Authentication Type: RADIUS

Support eduroam:  Authentication requests from unknown realms will be proxied to this server

Operation Mode:

---

**Primary RADIUS server**

Server IP Address:

Authentication Port:

Proxy Accounting:

Accounting Port:

Secret:  Confirm:

---

**Secondary RADIUS server (Optional)**

Server IP Address:

Authentication Port:

Proxy Accounting:

Accounting Port:

Secret:  Confirm:

4. Enter the relevant settings in the fields provided -

- **Support Eduroam** - Check the box to enable Eduroam support.
- **Operation Mode** - Use the drop down menu to determine whether the two servers should operate in failover mode or load balance mode.

**Primary RADIUS Server**

- **Server IP Address** - IP address of the server
- **Authentication Port** - Authentication Port number
- **Proxy Accounting** - Check the box to enable Proxy Accounting
- **Accounting Port** - Accounting Port number
- **Secret** - Enter and confirm the shared Secret

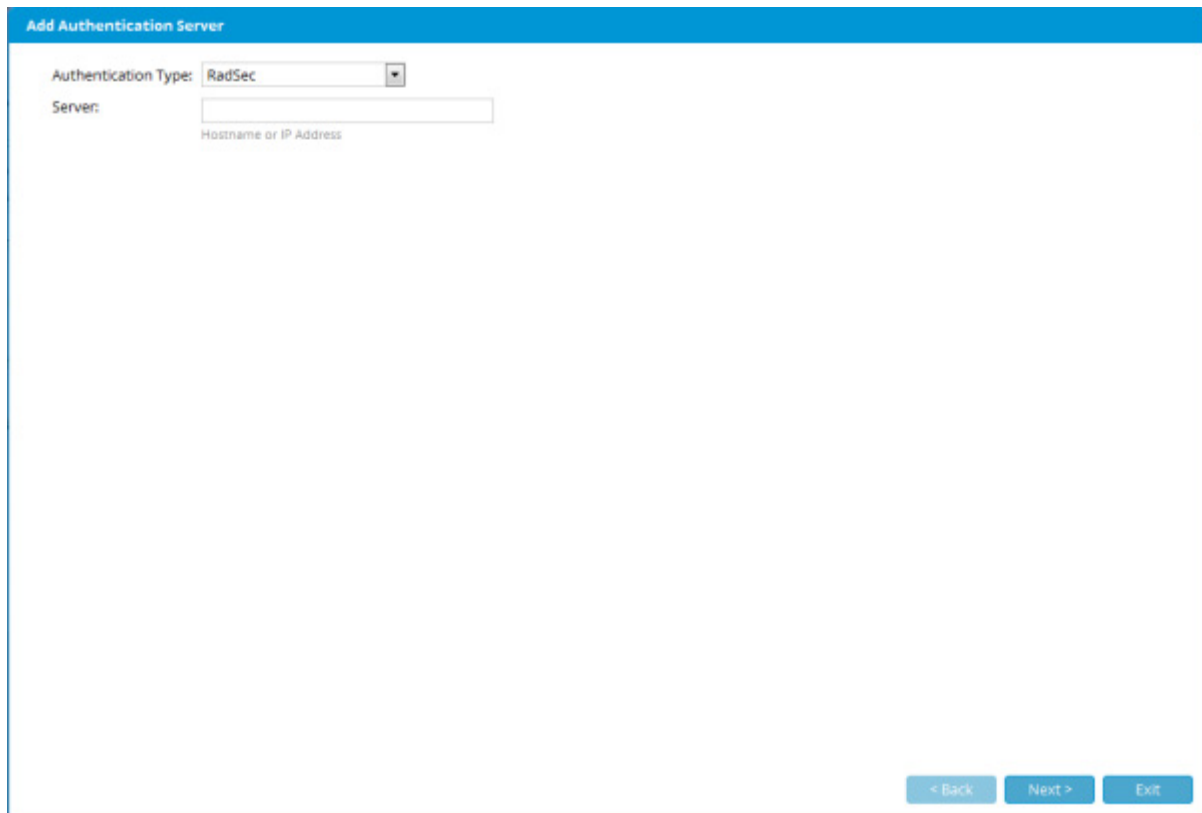
**Secondary RADIUS Server (Optional)**

- **Server IP Address** - IP address of the server
- **Authentication Port** - Authentication Port number
- **Proxy Accounting** - Check the box to enable Proxy Accounting

- **Accounting Port** - Accounting Port number
- **Secret** - Enter and confirm the shared Secret

5. Click on **Next** to continue and go to step 10.

## RadSec Authentication Server



**Add Authentication Server**

Authentication Type: RadSec

Server:

Hostname or IP Address

< Back   Next >   Exit

6. Enter the **Hostname** or **IP Address** of the RadSec server.

7. Click on **Next**

Add Authentication Server

Name:

Authentication Type: RadSec

Support eduroam:  Authentication requests from unknown realms will be proxied to this server

---

**Primary RadSec server**

Server:   
Hostname or IP Address

Verify SSL Certificate CN:

RadSec Type:

Authentication Port:

Secret:  Confirm:

Proxy Accounting:

---

**Fallover RadSec server (Optional)**

Server:   
Hostname or IP Address

Verify SSL Certificate CN:

RadSec Type:

Authentication Port:

Secret:  Confirm:

Proxy Accounting:

8. Enter the relevant settings in the fields provided -

- **Support Eduroam** - Check the box to enable Eduroam support.

### Primary RadSec Server

- **Server** - Enter the hostname or IP address of the server
- **Verify Certificate CN** - Enable this checkbox to enable verification
- **RadSec Type** - From the drop down menu select **TLS** or **DTLS** as RadSec type
- **Authentication Port** - Enter the Authentication port number (If Support Eduroam was selected then this option will not be available)
- **Secret** - Enter then confirm the shared secret (If Support Eduroam was selected then this option will not be available)
- **Proxy Accounting** - Check to enable proxy accounting

### Fallover RadSec Server (Optional)

- **Server** - Enter the hostname or IP address of the server
- **Verify Certificate CN** - Enable this checkbox to enable verification

- **RadSec Type** - From the drop down menu select **TLS** or **DTLS** as RadSec type
- **Authentication Port** - Enter the Authentication port number (If Support Eduroam was selected then this option will not be available)
- **Secret** - Enter then confirm the shared secret (If Support Eduroam was selected then this option will not be available)
- **Proxy Accounting** - Check to enable proxy accounting

9. Click on **Next** to continue and go to step 10.

10. You should now see the screen below, the next steps are applicable to both RADIUS and RadSec setup.

- **Vendor** - Enter the relevant Vendor from the drop down list
- **Authenticate with** - Select the relevant username format

11. Now you can add any attributes you wish to inject into RADIUS requests sent to the RADIUS server

- **Vendor** - From the drop down menu select which vendor is required

- **Attribute** - Select an attribute from the drop down menu
- **Value** - Enter the required value
- **Add AV Pair** - Click to add your pairing to the list.
- Use the Buttons on the right hand side of your list to order your attributes, click on remove to remove an attribute.

12. To add a mapping click on the **add mapping** link and create your rule as shown below.

### Add Authentication Server

**Connection**

Name: 10.10.1.2  
Server Type: RADIUS  
Server: 10.10.1.2

---

**Login Parameters**

Realm:

Authenticate with:

- eduroam\username
- eduroam/username
- username@eduroam
- username

Enable SSID Mapping:

---

**Attribute Mappings**

The response from the external server is tested against each rule below in order. If a rule is matched the specified usage profile and account group are applied and guest authentication succeeds.

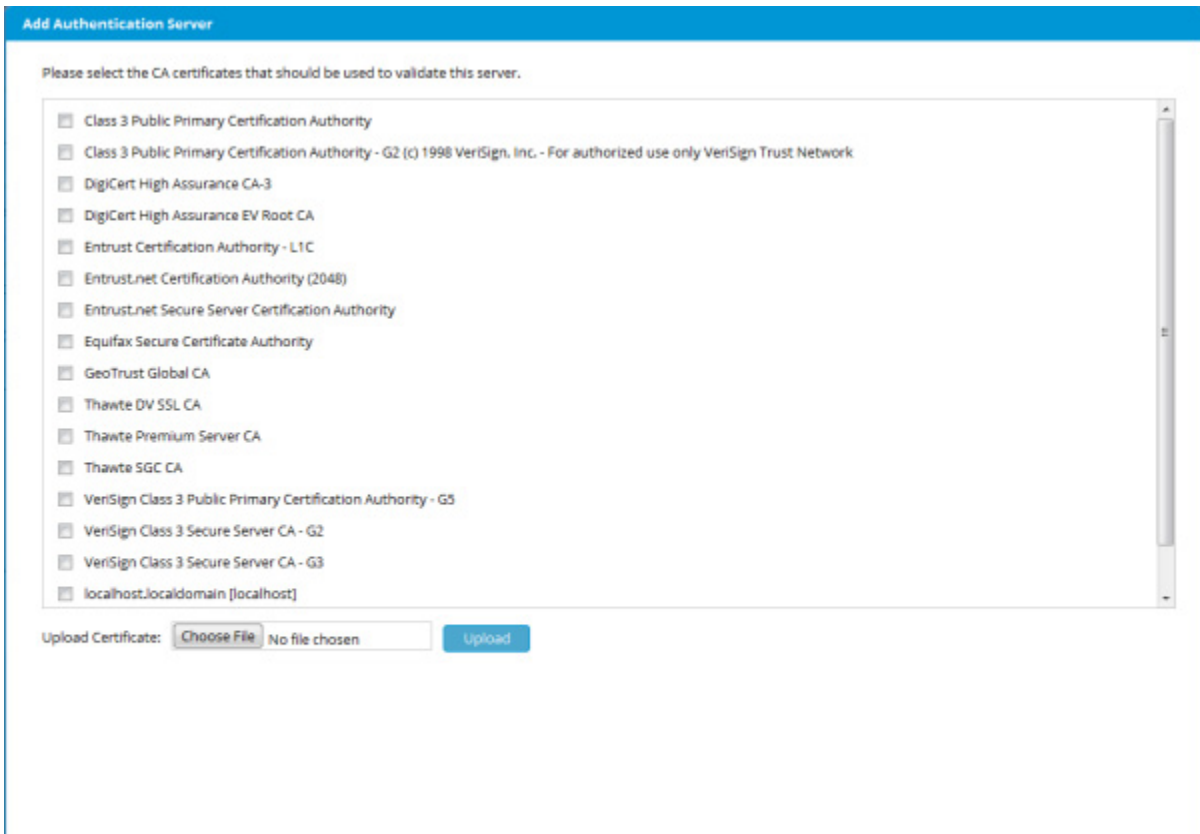
1  If **attribute** equals  set usage profile to  and account group to

2 If no rules match

[add mapping](#)

< Back   Next >   Exit

13. Click **Next** to continue.



14. Now select the CA certificates that should be used to validate your server, choose from the list provided or upload a certificate using the **Choose File** option.
15. Click **Next** once complete.
16. You have now successfully added an authentication server for RADIUS/RadSec Eduroam support.

## Configuring Authorization Policy

---

Authorization Policy enables you to give 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 – maybe allowing access only to the internet.

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.

# Adding an Authorization Policy

1. From the FortiConnect Administration Interface go to **Network Access Policy --> Authorization Policy** as shown below.

Authorization Policy

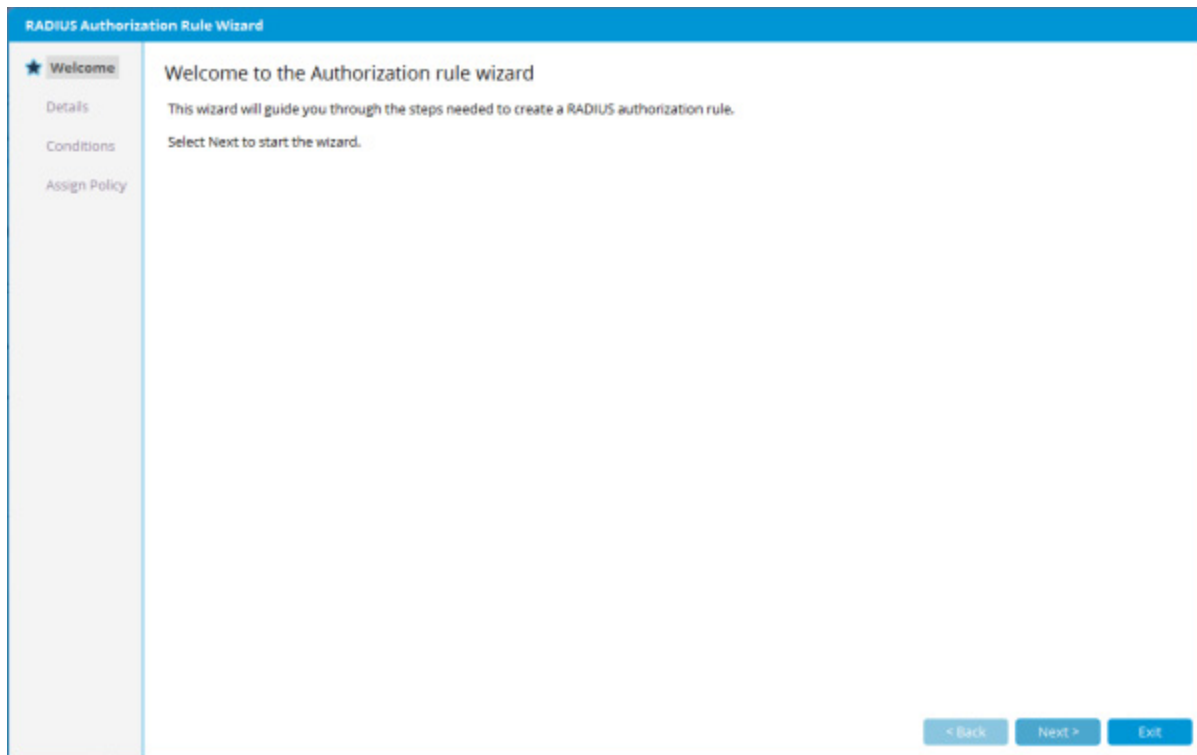
Each Authorization policy is checked in the following order. First matched policy is applied and no other policies are checked.

Order	Name	Rule	Authorization Profile	Enabled	Action
1	<a href="#">Default</a>	Apply profile	Default	<span style="color: green;">●</span>	

[Save Order](#) [Add](#)

2. Each Authorization Policy is checked in the order displayed on the screen, if no policies match then the default policy will be applied
3. To add another Authorization Policy click on the **Add** button which will launch the Authorization Rule Wizard and then click on **Next**.

T



4. Enter a **Name** and **Description** of your Rule as shown below.



RADIUS Authorization Rule Wizard

✓ Welcome

★ **Details**

Conditions

Assign Policy

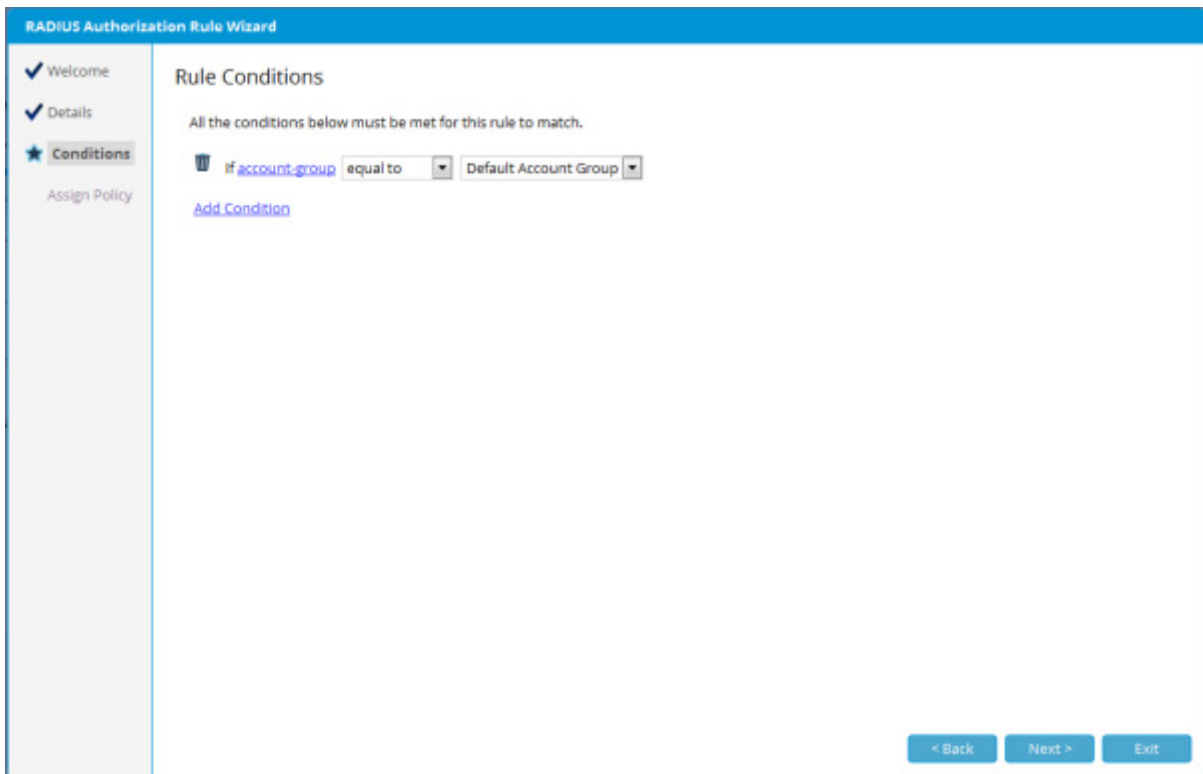
Rule Name

Name:

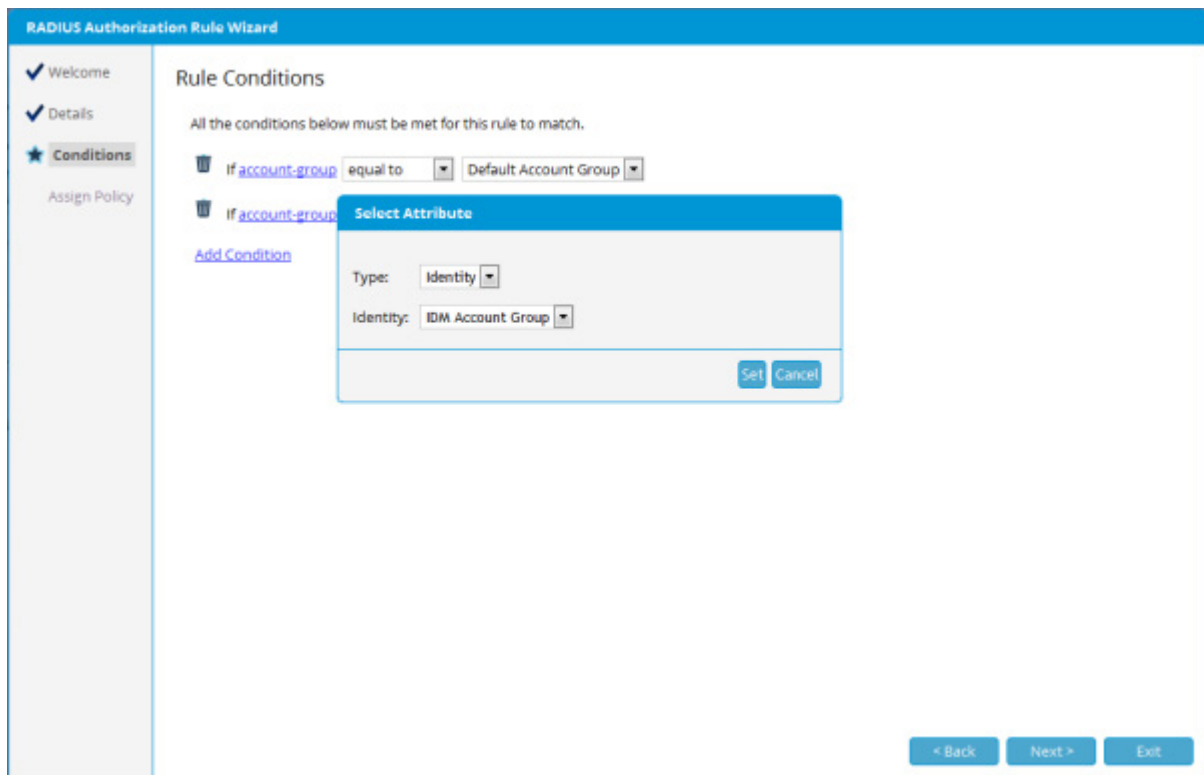
Description:

< Back   Next >   Exit

5. You will then be required to enter all the conditions that need to be met, click on **Next** to do this.



6. The Default Rule Condition will initially be displayed, this can be deleted or amended as necessary.
7. To create a new rule condition, click on the **Add Condition** link.
8. This will then display an **attribute** link, click on that to select the attribute for the rule as shown below.



9. From the drop down menu select the Attribute type and then choose from -
  - **RADIUS** - Selecting RADIUS will then require you to enter Vendor and Attribute Types for your rule condition
  - **Identity** - Selecting Identity will then require you to select from an Account Group or a Group Membership for your rule condition
  - **Time** - Selecting Time will then require you to select Day Of Week or Time Of Day criteria for your rule condition
  - **MDM** - Selecting MDM will then require you to enter Vendor and Attribute Types for your rule condition
10. Click on **Set** once complete.
11. Enter any remaining conditions you require then click on Next when complete.
12. You should now select an authorization profile you want to assign to the users/devices that matches the authorization rule as shown below. Profiles can set up in **Network Access Policy --> Authorization Profiles**.

**RADIUS Authorization Rule Wizard**

✓ Welcome  
✓ Details  
✓ Conditions  
★ **Assign Policy**

### Policy

Select the profile that you want to assign to users/devices that match this authorization rule.

Action:  Assign Profile  ▾

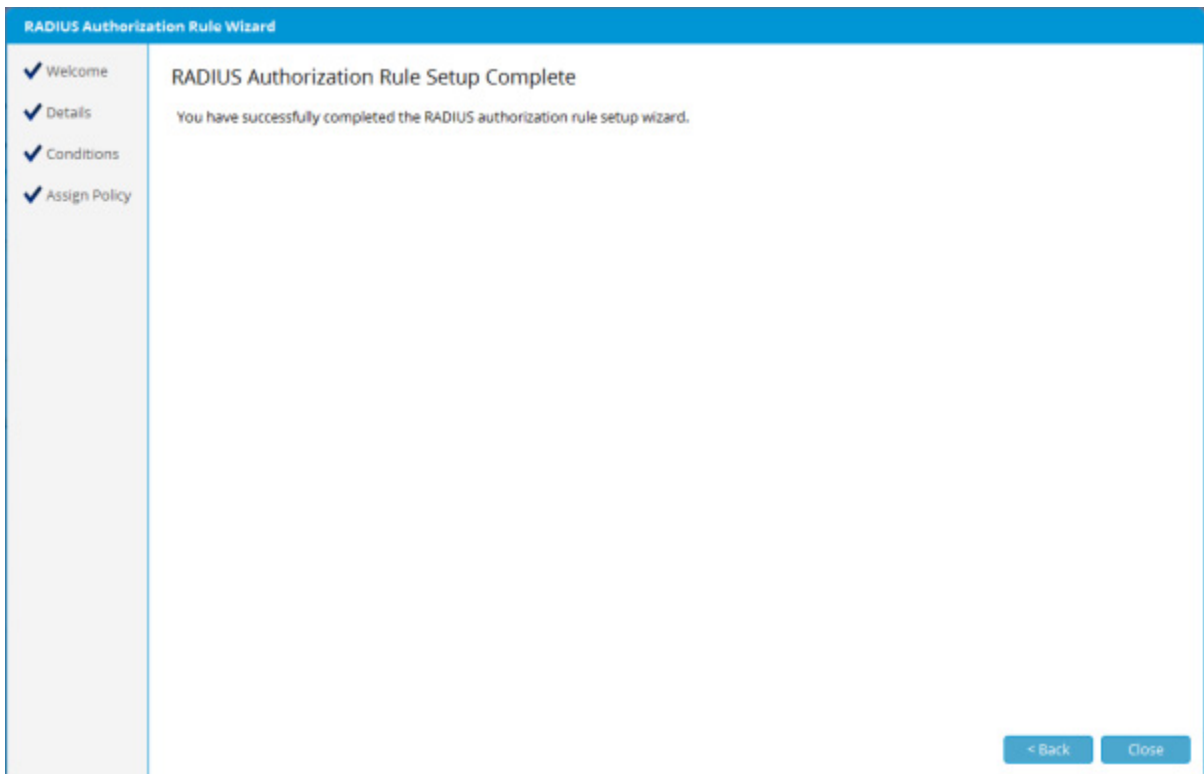
No access (send RADIUS reject)

< Back   Next >   Exit

**13. Select the appropriate Action :-**

- **Assign Profile** - from the drop down menu select the profile that matches the authorization rule.
- **No Access** - select this to prevent users which match this policy from accessing the network

**14. Click on Next to complete the Setup.**






## Editing an Authorization Policy

1. From the FortiConnect Administration Interface go to **Network Access Policy --> Authorization Policy** as shown below.

## Authorization Policy

Each Authorization policy is checked in the following order. First matched policy is applied and no other policies are checked.

Order	Name	Rule	Authorization Profile	Enabled	Action
1	<a href="#">Connect Rule</a>	account-group equals Default Account Group and account-group equals Default Account Group	Default	<span style="color: green;">●</span>	 
2	<a href="#">Default</a>	Apply profile	Default	<span style="color: green;">●</span>	

Save Order

Add

2. Click on the **Edit** icon to the right of the policy you wish to Edit.
3. Repeat steps 6 - 13 in the Add Authorization Policy section above to make your changes.

## Deleting an Authorization Policy

1. From the FortiConnect Administration Interface go to **Network Access Policy --> Authorization Policy** as shown below.

## Authorization Policy

Each Authorization policy is checked in the following order. First matched policy is applied and no other policies are checked.

Order	Name	Rule	Authorization Profile	Enabled	Action
1	<a href="#">Connect Rule</a>	account-group equals Default Account Group and account-group equals Default Account Group	Default		
2	<a href="#">Default</a>	Apply profile	Default		

Save Order

Add

2. Click on the Bin icon to remove the profile you wish to delete.
3. Click on Yes to confirm.

## Configuring Authorization Profiles

---

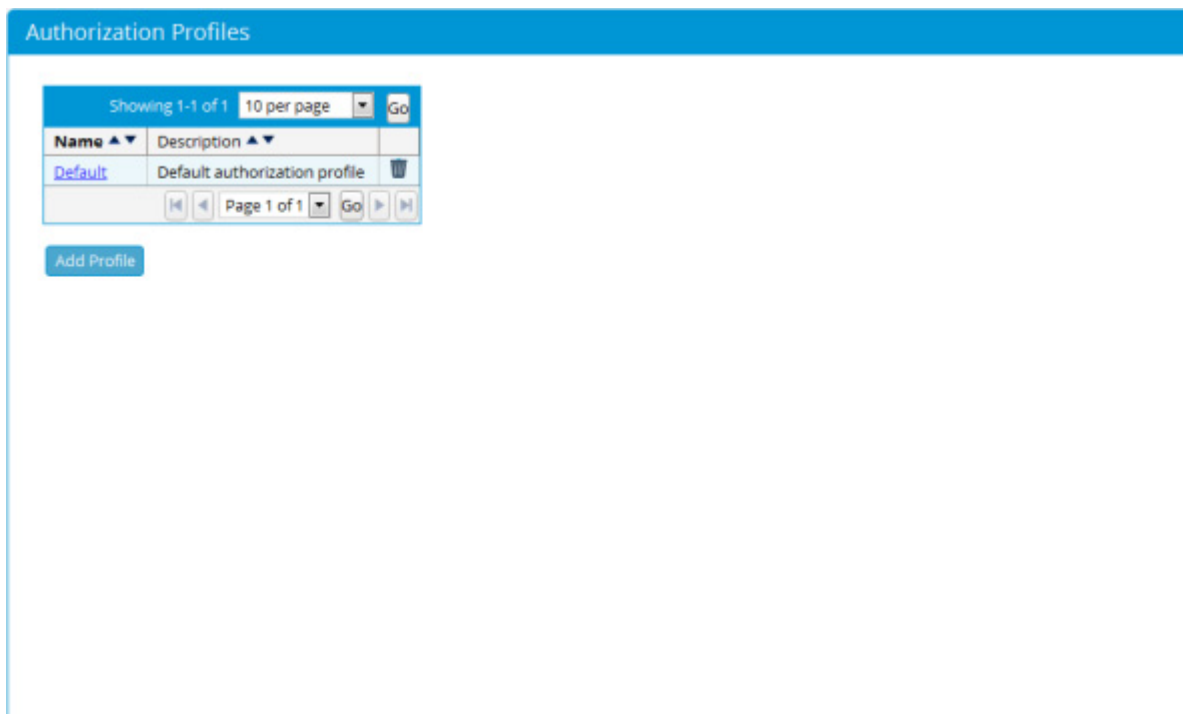
Authorization Profiles provide a way to give different levels of access to different accounts. For example, to assign different RADIUS attributes, or to only allow access to users from certain IP address ranges.

Once Authorization Profiles have been created, you must change the sponsor group to allow sponsors in that group to be able to provision accounts in the appropriate role.

## Adding Authorization Profiles

You can add a new Authorization Profile using the following steps.

1. From the administration interface, select **Network Access Policy > Authorization Profiles** as shown below.



2. Click the **Add Profile** button to add a new Profile.
3. From the Add Profile page as shown below, enter the name for a new Authorization Profile.



- Welcome
- Portal Name
- Portal Theme
- Portal Settings**
- Portal Policy

## Portal Pages

Specify which pages your portal should have enabled and at what stage they should be available.

Page	Displayed in menu	
	Pre-Authentication	Post-Authentication
Login	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Password Change	<input type="checkbox"/>	<input type="checkbox"/>
Self Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Registration	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Billing	<input type="checkbox"/>	<input type="checkbox"/>
Successful Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Welcome Back	<input type="checkbox"/>	<input type="checkbox"/>
Smart Connect	<input type="checkbox"/>	<input type="checkbox"/>
PMS Billing	<input type="checkbox"/>	<input type="checkbox"/>
Access without Login	<input type="checkbox"/>	<input type="checkbox"/>
Password Recovery	<input type="checkbox"/>	<input type="checkbox"/>
My Account	<input type="checkbox"/>	<input type="checkbox"/>
Help	<input type="checkbox"/>	<input type="checkbox"/>
Welcome	<input type="checkbox"/>	<input type="checkbox"/>

### Session Management

Allow user to close existing sessions when the concurrent session limit is exceeded:

### WiFi Marketing Integration

Enable WiFi Marketing Integration:

### Logout Options

Enable Logout Button:

Enable Logout Pop-up window:

4. Enter a Profile Name and its Description in the fields provided.
5. Click the **Add Profile** button to add the guest role. You can now edit the settings for the new guest role as described in Editing Authorization Profiles.

## Editing Authorization Profiles

The following steps describe how to edit the profiles.

1. From the administration interface, select **Network Access Policy > Authorization Profiles** from the left hand menu.

## Authorization Profiles

Showing 1-2 of 2 10 per page Go

Name ▲▼	Description ▲▼	
<a href="#">Auth Profile One</a>	Test	🗑️
<a href="#">Default</a>	Default authorization profile	🗑️

Page 1 of 1 Go

Add Profile

2. Select the profile you wish to edit and click the underlined name of that profile as shown above to bring up the Edit Profiles page. From there you can edit the following attributes:
  - Edit RADIUS Attributes
  - Edit Locations
  - Edit Notification Settings
  - Edit Device Restrictions
  - Edit Auto MAC Registration

## RADIUS Attributes

If a User authenticates using a RADIUS client device such as a Wireless LAN controller, then for each role you can specify additional RADIUS attributes that are sent upon successful authentication.

1. From the administration interface, select **Network Access Policy > Authorization Profiles** and click the underlined name of that role you want to edit.
2. Select **RADIUS Attributes** from the tab at the top of the page as shown below.

The screenshot shows the 'Authorization Profiles: Auth Profile One' configuration interface. The 'RADIUS Attributes' tab is active, with other tabs like 'Locations', 'Notification Settings', 'Device Restrictions', and 'Auto-MAC Registration' visible. The form includes a 'Vendor' dropdown menu set to 'IETF', an 'Attribute' dropdown menu set to 'Access-Loop-Encapsulation', and an empty 'Value' text input field. Below the 'Value' field is an 'Add AV Pair' button. A large empty list box is present, with 'Move up', 'Remove', and 'Move down' buttons to its right. At the bottom of the form are 'Save' and 'Cancel' buttons.

3. From the drop down menu select the appropriate **Vendor** from the list.
4. If the selected Vendor has been successfully highlighted in step 3, then the **Attribute** field will auto-populate with the appropriate Attributes for that Vendor, select the desired **Attribute** from the drop down menu.
5. Enter the **Value** in the field provided.
6. Click on **Add AV Pair**
7. If you need to re-order the attributes that are sent, use the **Move up** and **Move down** buttons.
8. Click the **Save** button to save the RADIUS Attributes.

## Locations

If a User authenticates uses a RADIUS client device such as a Wireless LAN Controller, 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 login from locations that you specify.

1. From the administration interface, select **Network Access Policy > Authorization Profiles** and click the underlined name of that profile you want to edit.
2. Click the **Locations** tab as shown below.

Authorization Profiles: Auth Profile One

RADIUS Attributes **Locations** Notification Settings Device Restrictions Auto MAC Registration

Locations only apply to RADIUS Authentication

IPv4 Network Address:  /

0.0.0.0/0

IPv6 Network Address:  /

::/0

3. Enter each **Network Address** and select the appropriate prefix length from the dropdown menu. Only valid Network Addresses will be accepted—host addresses must be specified using a /32 prefix length.
4. If your network uses IPv6 networking addresses then please use the section provided.
5. Click the **Add Location** button to add the Network Address.

**Note:** When you add a profile, the location 0.0.0.0/0 is automatically added. This means that the profile is valid from any IP address. If you want to restrict to other IP address ranges you must remove this address.

**Note:** Locations only apply to Users authenticating through RADIUS clients such as the Wireless LAN Controller.

**Note:** This only works when the RADIUS Client sends the Users IP address in the RADIUS authentication. The IP address must be contained in the Framed-IP-Address attribute.

## Notification Settings

Admin can configure the User Profile to send an Email and SMS notification after a User first logs on and to also send an expiry notification before a User Account expires.

1. From the FortiConnect administration interface, go to **Network Access Policy --> Authorization Profiles** and click on the **Notification Settings** tab as shown below.

Authorization Profiles: Auth Profile One

RADIUS Attributes Locations **Notification Settings** Device Restrictions Auto MAC Registration

	SMS	Email
At Login:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Minutes since last login:	<input type="text"/>	<input type="text"/>
	<small>Leave blank to send SMS at every login</small>	<small>Leave blank to send email at every login</small>
Expiry:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Minutes before expiry:	<input type="text"/>	<input type="text"/>
Language Template:	English (Default) ▾	

Save Cancel

2. To enable an **SMS Notification At Login**, place a check in the Enable box and then specify how often you wish to send notifications. Leave blank to send an SMS at every login
3. To enable **Email Notification At Login**, place a check in the Enable box and then specify how often you wish to send notifications. Leave blank to send an email at every login
4. To enable an **SMS Notification before Expiry**, place a check in the Enable box and specify how many minutes before a Guest Account expires before an SMS is sent.
5. To enable an **Email Notification before Expiry**, place a check in the Enable box and specify how many minutes before a Guest Account expires before an Email is sent.
6. From the drop down menu select the **Language Template** you wish to use (Only used for login notifications)
7. Click on **Save** to continue.

## Device Restrictions

Admin can configure the User Profile to place Device Restrictions when a User logs in.

1. From the FortiConnect administration interface, go to **Network Access Policy --> Authorization Profiles** and click on the **Device Restrictions** tab as shown below.

Authorization Profiles: Auth Profile One

RADIUS Attributes Locations Notification Settings **Device Restrictions** Auto MAC Registration

Allow Login with:  different devices  
Leave blank for unlimited

Restrict login with device to:  account(s) within  Days   
Leave blank for unlimited

- To allow login with different devices, enter the number of different devices you wish to allow in the **Allow to Login with** field.
- To restrict login with a device to a certain amount of accounts within a specific time period, enter the number of accounts in the **Restrict login with device to** field, then use the field and drop down menu to select the amount of **years, days, hours or minutes**.
- Click **Save** once complete.


## Auto MAC Registration

Admin can enable this setting to register MAC addresses, so that when a device is used to login it is remembered on the network.

- From the FortiConnect administration interface, go to **Network Access Policy --> Authorization Profiles** and click on the **Auto MAC Registration** tab as shown below.

Authorization Profiles: Auth Profile One

RADIUS Attributes Locations Notification Settings Device Restrictions **Auto MAC Registration**

 If enabled, a device account is automatically created for a user's device when they login via a portal. Automatic device registration is subject to the limit set in [Policy Settings > Account Groups](#)

Enable:

Account Group:

Usage Profile:  To define Usage Profiles go to Policy Settings -> Usage Profiles

If this is enabled, a device account is automatically created for a Users device when they login via a portal. Automatic device registration is subject to the limit set in **Policy Settings --> Account Groups**

2. To enable **Auto MAC Registration** place a check in the **Enable** check box.
3. From the **Account Group** drop down menu, select the **Account Group** used to create the device account.
4. From the **Usage Profile** drop down menu, select the **Usage Profile** used to create the device account.
5. Click on **Save** once complete.

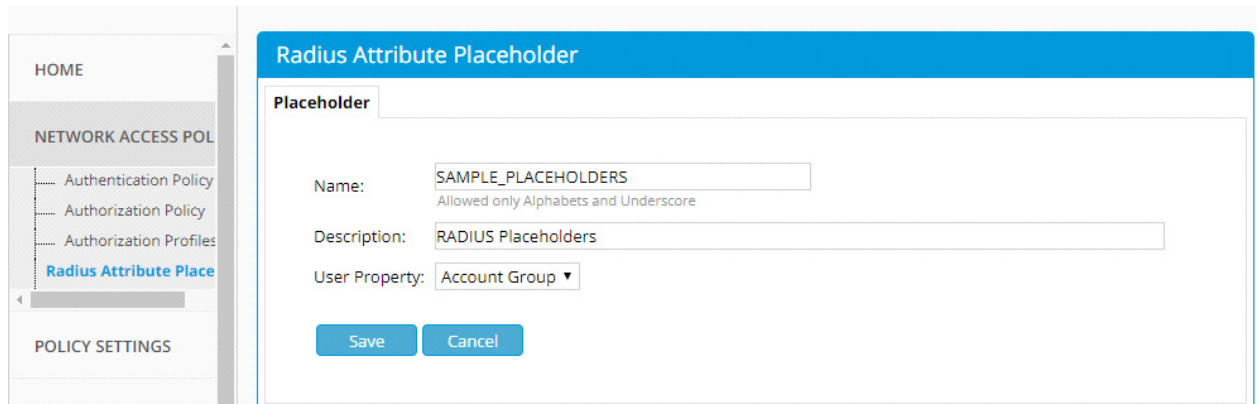
## Configuring RADIUS Attribute Placeholders

---

You can dynamically change the RADIUS attributes returned on authentication. These attributes are set by the authorisation profiles on device configuration.

You can add, edit and delete the RADIUS placeholder attributes under the *Network Access Policy*.

Navigate to *Network Access Policy > Radius Attribute Placeholders > Add Radius Placeholder Attribute* to add new RADIUS placeholders.



The screenshot shows a web interface for configuring a RADIUS Attribute Placeholder. On the left is a navigation menu with sections: HOME, NETWORK ACCESS POL (expanded to show Authentication Policy, Authorization Policy, Authorization Profiles, and RADIUS Attribute Placeholder), and POLICY SETTINGS. The main content area has a blue header 'Radius Attribute Placeholder' and a sub-header 'Placeholder'. Below this are three input fields: 'Name' with the value 'SAMPLE\_PLACEHOLDERS' and a note 'Allowed only Alphabets and Underscore', 'Description' with the value 'RADIUS Placeholders', and 'User Property' with a dropdown menu set to 'Account Group'. At the bottom are 'Save' and 'Cancel' buttons.

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

## Radius Placeholder Mappings

✓ Mappings saved

Placeholder **Mappings**

### Add Radius Placeholder Mapping

Match Value:

Replacement Value:

Add

Match Value ▲▼	Replacement ▲▼	
Match	Match1	
MatchAB	Match3	

Showing 1-2 of 2 10 per page Go

Page 1 of 1 Go

From the list displayed, you can delete or edit any placeholder. Click on the placeholder name to edit the placeholder or the mappings.

HOME

NETWORK ACCESS POL

- Authentication Policy
- Authorization Policy
- Authorization Profiles
- Radius Attribute Place**

POLICY SETTINGS

## Radius Attribute Placeholders

Name ▲▼	Description ▲▼	User Property ▲▼	
<a href="#">SAMPLE_PLACEHOLDERS</a>	RADIUS Placeholders	accountGroup	
<a href="#">TEST</a>	test	realm	

Showing 1-2 of 2 10 per page Go

Page 1 of 1 Go

Add Radius Attribute Placeholder



# User Policy Settings

Organizations commonly have policies in place for creating accounts for their internal users and systems, such as the format or length of the username and/or complexity of password. FortiConnect allows you to configure username and password creation policies to match your organization's policy or to create a policy specific to User's accounts.

Usage Profiles allow you to provide different levels of access to different User accounts (for example, to assign different RADIUS attributes, or to only allow access to guests from certain IP address ranges).

This chapter describes the following:

- Setting Username Policy
- Setting Password Policy
- Setting Guest Details Policy
- Configuring Usage Profiles
- Adding Account Groups
- Currency Denomination for Access Codes

## Configuring Username Policy

---

The Username Policy determines how to create user names for all accounts.

1. From the administration interface, select **Policy Settings > Guest Usernames** as shown below and click in the **Standard Accounts** tab.

## Guest Usernames

**Standard Accounts** Random Accounts

**These settings control username policy for standard account creation**

Username Prefix:   
All generated usernames will be prefixed with this text

---

**Email address as username**

Email address as username

Create Username With Case:

---

**Create username based on first and last names**

Create username based on first and last names

Minimum username length:

Create Username With Case:

Create Username With Separator:

---

**Create random username**

Create random username

Alphabetic characters to include:

Number to include:

Numeric characters to include:

2. **Username Prefix** - All generated usernames will be prefixed with any text/number entered.
3. Choose one of the username policy options for creating the user name for your user accounts:
  - **Username Policy 1 - Email address as username**

Use the users email address as the 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 an overlapping 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 being set by the sponsor.
  - **lowercase**—The username is forced into lowercase after being set by the sponsor.
- 
- **Username Policy 2 - Create username based on first and last names**

Create a username based on combining the first name and last name 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.

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 being set by the sponsor.
- **lowercase**—The username is forced into lowercase after being set by the sponsor.

- **Username Policy 3 - Create random username**

Create a username based upon a random mixture of Alphabetic, Numeric or Other characters. Insert the characters to be included in the randomly generated Username, and select and the number to use from each set of characters.

**Note:** The total length of the username is determined by the total number of characters included.



**Sponsor specified username**

Sponsor specified username

Minimum username length: 5 ▼

Set Policy Cancel

- **Username Policy 4 - Sponsor Specified username**

Sponsors can create a username at account creation, click on the dropdown menu and select the **minimum username length** the sponsor must use.

4. When done, click **Set Policy** to have the username policy take effect.

To set a policy for Random Bulk Account creation click on the **Random Accounts** Tab as shown below.

Determine your random account creation policy using the fields provided.

## Guest Usernames

Standard Accounts **Random Accounts**

These settings control username policy for multiple random account creation

Username Prefix:   
All generated usernames will be prefixed with this text

Alphabetic characters to include:   
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

Number to include:

Numeric characters to include:   
0123456789

Number to include:

Other characters to include:   
\$^\*()\_+=+[]{}:~@#-\_-<>?

Number to include:

Create username based on the above prefix followed by a sequential number:

## Configuring Password Policy

---

The Password Policy determines how to create the password for all User accounts.

1. From the administration interface, select **Policy Settings > Guest Passwords** as shown below.

## Guest Passwords

These settings control password policy for standard account creation

Allow sponsor to change password:

### Auto generated password

Auto generated password

Password case:

Alphabetic characters to include:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

Number to include:

Numeric characters to include:

0123456789

Number to include:

Other characters to include:

!\$^\*( )\_+[]{};:@#~>?

Number to include:

### Sponsor specified password

Sponsor specified password

Minimum password length:

2. Check the **Allow sponsor to change password** box if you wish to allow sponsors to do this.
3. From the **Password case** drop down menu select whether the password that is generated will have a **mixed**, **lowercase** or **uppercase** character base.
4. In the **Alphabetic Characters** section, enter the characters to be used in the password and the number to be included.
5. In the **Numeric Characters** section, enter the numerals to be used in the password and the number to be included.
6. In the **Other Characters** section, enter the special characters to be used in the password and the number to be included.
7. You may also allow the sponsor to specify the password. If you wish to select this option, place a check in the **Sponsor specified password** section and using the drop down menu choose the minimum number of characters a sponsor should use when creating a password for the User.

**Note:** For passwords, use only the following characters for the "Other Characters" field: `!$^*( )_+[]{};:@#~>?`

8. Click the **Set Policy** button to save the settings.

**Note:** The total length of the password is determined by the total number of characters included. You can choose between 0 and 20 characters per type (alphabetic, numeric, or other).

## Configuring Account Details Policy

---

The Guest Details policy determines the data the sponsor needs to enter to create a User account.

1. From the administration interface, select **Policy Settings > Guest Details** as shown below.

The screenshot shows the 'Guest Details' configuration page. It has a blue header with the text 'Guest Details'. Below the header, there are two sections: 'Standard Fields' and 'Additional Fields'. In the 'Standard Fields' section, there are five dropdown menus: 'First Name: Required', 'Last Name: Required', 'Company: Required', 'Email: Required', and 'Mobile: Optional'. A note below the 'Email' dropdown states: 'This cannot be changed as email address is being used as the username in Guest Usernames settings'. The 'Additional Fields' section contains a note: 'The text for additional fields is defined in the [Language Templates](#) section'. Below this note are five dropdown menus labeled 'Option 1: Unused', 'Option 2: Unused', 'Option 3: Unused', 'Option 4: Unused', and 'Option 5: Unused'. At the bottom of the form are two buttons: 'Save' and 'Cancel'.

2. You can specify one of three settings for each requirement:

- **Required**—If a field is set to required it is displayed on the Create Guest Account page and it is mandatory for the sponsor to complete.
- **Optional**—If a field is set to optional it is displayed on the Create Guest Account page. However

the sponsor can choose not to complete the field.

- **Unused**—If a field is set to unused then it is not displayed on the Create Guest Account page and no value is required.

3. Click the **Save Settings** button to save the guest details policy.

**Note:** There are five Additional Fields that you can use to add any additional information that you require sponsors to fill out when creating guest accounts. These are described on the Guest Details page as Option 1 through Option 5. If you want to use these fields, Fortinet recommends customizing the text that is shown to the sponsor by editing the templates as described in User Interface Templates.

## Configuring Usage Profiles

---







Usage Profiles provide a way to give levels of time access to different User accounts, or, also a level of Data Usage. For example, you can assign a usage profile that allows access during a working week day and not on a weekend.

Once 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.

You can add a new usage profile using the following steps.

1. From the administration interface, select **Policy Settings > Usage Profiles** as shown below.

## Usage Profiles

Name	Description	Account Type	Timezone	
<a href="#">12 Hours</a>	12 hours usage from first login	From First Login	America/Los_Angeles	
<a href="#">1 Hour</a>	1 hour usage from first login	From First Login	America/Los_Angeles	
<a href="#">24 Hours</a>	24 hours usage from first login	From First Login	America/Los_Angeles	
<a href="#">6 Hours</a>	6 hours usage from first login	From First Login	America/Los_Angeles	
<a href="#">default</a>	Default time profile	Start End	America/Los_Angeles	
<a href="#">Unlimited</a>	Unlimited time profile	Unlimited	America/Los_Angeles	

Add

2. Click the **Add** button to add a new Usage Profile.
3. From the Usage Profile page as shown below, Click on the **Time Usage** tab and type the **Name** and **Description** of the new time profile.



**Usage Profile:**

**Time Usage** | Time Restrictions | Data Usage

Name:

Description:

Time zone:

Account Type:

Expire if inactive for:

0 = never expire

4. From the **Timezone** dropdown menu, specify the timezone for which any Account Restrictions will apply.
  5. From the **Account Type** dropdown menu, you can choose one of the predefined options.
    - **Start End**—Allows sponsors to define start and end times for account durations.
    - **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 login. For example, account can be valid for 2 hours and usable for any time within 24 hours from first login.
    - **Unlimited** - Unlimited time profiles
  6. **Expire if inactive for** - Allows the admin to specify the time period after which an account with this usage profile should be considered inactive.
- Note:** When creating an account type of Time Used, you may also repeat the time used as many times as you require by entering an amount into the Repeat Field, as shown below

**Usage Profile:**

**Time Usage** | Time Restrictions | Data Usage

Name:

Description:

Time zone:

Account Type:

Duration:  Hours  Within  Hours

Repeat:  more times (ends after 0 hours)

Expire if inactive for:  Days

0 = never expire

7. Once you have selected your account type, click on **Save**.

8. Next, click on the **Time Restrictions** tab as shown below.

**Usage Profile: test**

**Time Usage** | **Time Restrictions** | Data Usage

Guests cannot login or will be logged out during these periods

No current restrictions for this profile

9. Once a Time Profile is created, you can implement Account Restrictions in the **Time Restrictions** section. Use the dropdown menus to select the days and time you wish to restrict guest access to and from. Once a time criteria is complete, click **Add**, then create the next restriction.

10. Depending on the Account Type selected, enter the duration in the following fields:

- **Start End**—Allows sponsors to define start and end times for account durations; therefore, no duration is necessary.

- **From First Login**—Allows sponsors to define a length of time for User access from their first login. Duration in days is required.
- **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 login. For example account can be valid for 2 hours and usable for any time within 24 hours from first login. You need to specify how long the sponsor can allocate a User account for, and the time frame in which it must end.
- **Unlimited** - No action necessary.
- Click the **Save** button to save.

11. Next Click on the **Data Usage** tab as shown below.

**Usage Profile: test**

Time Usage | Time Restrictions | **Data Usage**

Accounts will be expired when the first limit is reached

Data Up:  KB   
0 = unlimited

Data Down:  KB   
0 = unlimited

Total Up & Down:  KB   
0 = unlimited

12. You can also add **Data Usage** restriction to your Usage Profiles.

13. From the drop down menus, determine whether to apply the following -

- **Data Up** - Apply a Data Usage up restriction to your profile, use the drop down menu to determine whether it be in KB, MB or GB.
- **Data Down** - Apply a Data Usage down restriction to your profile, use the drop down menu to determine whether it be in KB, MB or GB.
- **Total Up & Down** - Apply a Total Data Usage restriction to your profile, use the drop down menu to determine whether it be in KB, MB or GB.








14. Click on **Save** once complete.

## Editing Usage Profiles

The following steps describe how to edit Usage Profiles.

1. From the administration interface, select **Policy Settings > Usage Profiles** from the left hand menu.

### Usage Profiles

Name	Description	Account Type	Timezone	
<a href="#">12 Hours</a>	12 hours usage from first login	From First Login	America/Los_Angeles	
<a href="#">1 Hour</a>	1 hour usage from first login	From First Login	America/Los_Angeles	
<a href="#">24 Hours</a>	24 hours usage from first login	From First Login	America/Los_Angeles	
<a href="#">6 Hours</a>	6 hours usage from first login	From First Login	America/Los_Angeles	
<a href="#">default</a>	Default time profile	Start End	America/Los_Angeles	
<a href="#">test</a>	test	Start End	America/Los_Angeles	
<a href="#">Unlimited</a>	Unlimited time profile	Unlimited	America/Los_Angeles	

[Add](#)








2. Select the usage profile you wish to edit and click the underlined name of that profile as shown above.
3. Repeat the steps in the **Adding a Usage Profile** section above to make the necessary amendments.

## Deleting Time Profiles

The following steps describe how to delete Usage Profiles.

1. From the administration interface, select **Policy Settings > Usage Profiles** from the left hand menu.

## Usage Profiles

Name	Description	Account Type	Timezone	
<a href="#">12 Hours</a>	12 hours usage from first login	From First Login	America/Los_Angeles	
<a href="#">1 Hour</a>	1 hour usage from first login	From First Login	America/Los_Angeles	
<a href="#">24 Hours</a>	24 hours usage from first login	From First Login	America/Los_Angeles	
<a href="#">6 Hours</a>	6 hours usage from first login	From First Login	America/Los_Angeles	
<a href="#">default</a>	Default time profile	Start End	America/Los_Angeles	
<a href="#">test</a>	test	Start End	America/Los_Angeles	
<a href="#">Unlimited</a>	Unlimited time profile	Unlimited	America/Los_Angeles	

Add

2. From the **Usage Profiles** page as shown above, choose the profile you wish to delete and click the **dustbin** icon.
3. Confirm the deletion when prompted.

## Configuring Account Groups

---


Account Groups are used to group User & device accounts and are assigned at the point of account creation. If no additional account groups are created, User & device accounts will be assigned to the default account group.


In previous versions of FortiConnect, User and device accounts could be assigned an authorization profile at creation. This is no longer the case and instead we assign an account group to the User or device account.

An Authorization Profile will be assigned via the Authorization Policy which may reference an Account Group as part of its mapping criteria.

From the FortiConnect Administration Interface go to **Policy Settings --> Account Groups** as shown below.

## Account Groups

 Guest (user) & device accounts will be assigned to an account group on creation.

Group Name ▲▼	Description ▲▼	
<a href="#">Default Account Group</a>	Default Account Group	

Showing 1-1 of 1    10 per page   

1. By default User and device accounts will be assigned to the **Default Account Group**, to add another group click on the **Add** button.

### Add Account Group

**Details**

Name:

Description:

---

**Authentication Settings**

Maximum Concurrent Connections:   
0 = unlimited

Maximum Failed Authentications:   
0 = unlimited

Allow Password Change:

Require Password Change:

---

**Guest Portal Device Registration Limit**

Maximum Number Of Different Devices:   
0 = unlimited

2. Edit the fields as required -

- **Name** - Enter the name of your group
- **Description** - Enter the group description
- **Maximum Concurrent Connections** - Enter the maximum amount of concurrent connections allowed
- **Maximum Failed Authentications** - Enter the maximum amount of failed authentications allowed
- **Allow Password Change** - Check box to allow passwords to be changed
- **Require Password Change** - Check box to require passwords be changed (applies to accounts create on FortiConnect only)
- **Maximum Number Of Different Devices** - Specify the maximum number of different devices a user can register

3. Click on **Save** once complete


### Editing Account Groups

From the FortiConnect Administration Interface go to **Policy Settings --> Account Groups** as shown below.

## Account Groups

! Guest (user) & device accounts will be assigned to an account group on creation.

Showing 1-1 of 1 10 per page Go

Group Name ▲▼	Description ▲▼	
<a href="#">Default Account Group</a>	Default Account Group	

Page 1 of 1 Go

Add


1. Click on the Group Name of the group you wish to edit.
2. Edit the fields as required -
  - **Name** - Enter the name of your group
  - **Description** - Enter the group description
  - **Maximum Concurrent Connections** - Enter the maximum amount of concurrent connections allowed
  - **Maximum Failed Authentications** - Enter the maximum amount of failed authentications allowed
  - **Allow Password Change** - Check box to allow passwords to be changed
  - **Require Password Change** - Check box to require passwords be changed
  - **Maximum Number Of Different Devices** - Specify the maximum number of different devices allowed to be registered.
3. Click on **Save** once complete.

## Deleting Account Groups




From the FortiConnect Administration Interface go to **Policy Settings** --> **Account Groups** as shown below.

## Account Groups

 Guest (user) & device accounts will be assigned to an account group on creation.

Showing 1-1 of 1    10 per page   

Group Name ▲▼	Description ▲▼	
<a href="#">Default Account Group</a>	Default Account Group	

Page 1 of 1

1. Click on the **Bin Icon** of the group you wish to delete.
2. Click on **Ok** to delete.



This chapter describes the following:

- Overview
- Adding RADIUS Clients
- Editing RADIUS Clients
- Deleting RADIUS Clients
- Support Syslog for RADIUS accounting

## Configuring RADIUS Clients

---

Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization and accounting) protocol. FortiConnect uses the RADIUS protocol to authenticate and audit Users who login through RADIUS-capable network enforcement devices, such as Wireless LAN Controllers.

When a User authenticates against a RADIUS client, such as a Wireless LAN Controller, the RADIUS client performs a RADIUS authentication check with FortiConnect to validate whether the credentials supplied by the user/device are valid. If the User authentication is successful, FortiConnect 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).

**Note:** The Wireless LAN Controller needs to be specifically configured to Allow AAA Override. This enables it to honour the session-timeout attribute returned to it by FortiConnect.

In addition to authentication, the RADIUS client device reports details to FortiConnect, 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.

**TIP** - If there is a Firewall between FortiConnect and the RADIUS client, you need to allow traffic from UDP Port 1812 or 1645(RADIUS authentication) and UDP Port 1813 or 1646 (RADIUS accounting) to pass.

**Note:** The Debug button under Devices > RADIUS Clients turns the RADIUS server on in debugging mode. This enables detailed debug information to be viewed under Server > System Logs > Support Logs. See Support Logs for additional details.

# Adding RADIUS Clients

1. From the administration interface, select **Devices > RADIUS Clients** from the left hand menu.
2. Before adding a RADIUS client you can determine whether you wish RADIUS authentication to be performed in a case sensitive or insensitive manner as show in the screen shot below. From the drop down menu in the **RADIUS Authentication** section, select the option you wish authenticate the RADIUS username in.
3. In the RADIUS Clients page as shown below, click the **Add RADIUS Client** button to add a RADIUS client.

**RADIUS Clients**

**RADIUS Clients**

Name	Device	Type	Description
No RADIUS Clients defined			

[Add RADIUS Client](#)

**RADIUS Debug**

RADIUS Support logs can be found in [Reports & Logs > System Logs > Support Logs](#)

RADIUS is running normally.

[Restart RADIUS in Debug](#)

**RADIUS Authentication**

This setting controls whether RADIUS authentication is performed in a case sensitive or insensitive manner.

RADIUS username is

[Save](#)

4. In the Add RADIUS page, click on the **Client** tab as shown below, type a descriptive **Name** for the RADIUS client.

5. In **Name** - Type the name of the RADIUS Client
6. In **Device IP Address / Prefix Length**- Type the **IP Address / Prefix Length** of the RADIUS client, if you do not know the Prefix Length, the FortiConnect will automatically enter this for you. This needs to match the IP address from which the RADIUS request is originated.
7. Type a shared **Secret** for the RADIUS client. This must match the shared secret specified in the configuration of the RADIUS client.
8. Retype the shared secret in the **Confirm** field.
9. From the **Type** drop down menu select the type or vendor of the RADIUS client, if you select **Fortinet**, an extra tab will appear at the end of the set of tabs on the screen called **Automatic Setup**, for details on this screen goto **step 22** for details on how to configure the options within.

**Note:** If selecting Generic Radius Device an Guest Portal along the top will appear, see step 18 for details on this.

**Note:** Depending on the **Type** of Radius Device you select, the options on this screen may differ slightly.

10. Type a **Description** of the client and any other information needed.
11. To turn on the use of **Change-of-Authorization** then place a check in the **Use COA** box.
12. Click the **Save** Button and the system will automatically restart and save the settings. Please wait whilst this occurs.
13. If you want the RADIUS client to send any additional attributes upon successful authentication, click on the **Attributes** tab as shown in the figure below.

The screenshot shows the 'RADIUS Clients' configuration page. The 'Attributes' tab is selected, displaying a form to add or edit attribute-value pairs. The 'Vendor' dropdown is set to 'IETF', and the 'Attribute' dropdown is set to 'Access-Loop-Encapsulation'. The 'Value' field is empty. An 'Add AV Pair' button is located below the value field. A table area is currently empty, with 'Move up', 'Remove', and 'Move down' buttons to its right. At the bottom are 'Save' and 'Cancel' buttons.

14. You can use the drop down menus to select :

- **Vendor** - A list of predefined Vendors are available using the drop down menu.
- **Attribute** - A list of predefined Attributes will appear depending on what Vendor you selected, use the drop down menu to select the appropriate one.
- **Value** - Enter the appropriate value in the field provided.

15. Click on the **Add AV Pair** button to add attribute and value pair to the table below.

- If you want to remove an attribute, select the attribute from the table and click the **Remove** button.
- Use the **Move up** and **Move down** buttons to change the order of the RADIUS attributes as they are sent in the RADIUS Accept Message.

16. Click the **Save** Button and the system will automatically restart and save the settings. Please wait whilst this occurs.

**Note:** FortiConnect supports TLS, PAP, CHAP, PEAP-MSCHAPv2 and PEAP-GTC in RADIUS Authentication

**Note:** SNMP is used for recording the Framed-IP-Address of the guest when the RADIUS client does not set this in RADIUS accounting messages. You do not need to set this if the device sets it correctly.

17. To set this click on the **SNMP** tab as shown in the figure below

**RADIUS Clients**

Client | Attributes | **SNMP** | MAC Authentication | RadSec Authentication | Automatic Setup

SNMP is used for recording the Framed-IP-Address of the guest when the RADIUS client does not set this in RADIUS accounting messages. You do not need to enable this if the device sets it correctly.

Enable:

Alternative SNMP device IP Address:  If the RADIUS Client doesn't support SNMP access to the ARP table, query this device instead

Version: **V3** V2c & V3 perform better than V1

Read Community:

Authentication Protocol: **MD5**

Authentication Username:

Authentication Passphrase:  Confirm:

Privacy Protocol: **DES**

Privacy Passphrase:  Confirm:

Security Type: **Authentication**

**Save** **Cancel**

18. Place a check in the **enable** check box.

- **Version** - Select the correct version number from the drop down box.
- **Read Community** - Enter the read community string.
- **Authentication Protocol** - Select the correct authentication protocol from the drop down box.
- **Authentication Username** - Enter the authentication username.
- **Authentication Passphrase** - Enter the authentication passphrase and confirm it in the field provided.
- **Privacy Protocol** - Select the correct privacy protocol from the drop down menu provided.
- **Privacy Passphrase** - Enter the privacy passphrase and confirm it in the field provided.
- **Security Type** - Select the correct security type from the drop down menu provided.

Click the **Save** button and the system will automatically restart and save the settings. Please wait whilst this occurs.

To set up and enable **MAC Authentication**, click on the **MAC Authentication** tab as shown below.

## RADIUS Clients

Client | Attributes | SNMP | **MAC Authentication** | RadSec Authentication | Automatic Setup

Enable MAC authentication:

User-Name attribute contains: Client MAC Address ▾

User-Password attribute contains: Shared Secret ▾

Service-Type attribute contains: Login-User ▾

Save Cancel

**Note:** MAC Auth settings depend on what the controller sends when it does a MAC Auth request

19. Place a check in the **Enable MAC authentication** check box :-

- **User-Name attribute contains** - From the drop down menu select whether the User Name attribute contains **Client MAC Address**, **Shared Secret**, whether its **Not Present**, or **Don't Check**.
- **User-Password attribute contains** - From the drop down menu select whether the User Password attribute contains **Client MAC Address**, **Shared Secret**, whether its **Not Present**, or **Don't Check**.
- **Service-Type attribute contains** - From the drop down menu select whether the Service Type attribute should contain the **Login User**, **Call Check**, or **Don't Check**.

20. Click on **Save** once complete.

21. When creating certain client of 'Type' the tab below is shown



**RADIUS Clients**

Client Attributes SNMP MAC Authentication RadSec Authentication **Guest Portal**

These settings allow the RADIUS client to interface with a guest portal.

Method:

Login URL:  e.g. https://1.1.1.1/login.html

Username request key:  e.g. userid

Password request key:  e.g. passwd

Redirection request key:  e.g. redirect

Custom Login Parameters:  e.g. buttonClicked=go&activity=123

Logout URL:  e.g. https://1.1.1.1/logout.html

Custom Logout Parameters:  e.g. buttonClicked=stop&activity=456

The setting on the tab can allow a generic RADIUS client to interface with a Portal by providing login/logout parameters and request keys


Enter the relevant settings to allow the RADIUS client to interface with a Portal :

- Method - Choose 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 logout users on the device.
- Custom Logout Parameters - Enter any custom logout parameters the device may require.

Click on the **Save** button once completed.

**22.** If you are adding RADIUS for authentication with a Fortinet Controller you will see the tab as shown below.

## RADIUS Clients

 The Meru Connect is using a self-signed SSL certificate, you may get certificate warnings on your clients when they attempt to authenticate

Client Attributes SNMP MAC Authentication RadSec Authentication **Automatic Setup**

Meru Connect Address:   
This hostname is used to redirect guests to the Meru Connect, it should match the SSL certificate on Meru Connect.

Device IP Address:

Admin user name:

Admin Password:

Configure RADIUS profiles:

Set Captive Portal RADIUS profiles:

Set Captive Portal External URL:

Configure QoS Rules:

Write changes to startup-config:  This will overwrite your startup-config with the current running-config

Setup Controller

23. Within this tab you can automate several configuration steps between FortiConnect and the Fortinet Controller. Steps you previously took when setting up the client and SNMP will also be automated once you click on the **Setup Controller** button :-

- **FortiConnect Address** - Enter the IP Address of FortiConnect (should match the SSL cert common name)
- **Device IP Address** - Enter the IP Address of the controller, this can be IP address or FQDN
- **Admin User Name** - Enter the admin user name for the controller
- **Admin Password** - Enter the admin password for the controller
- **Configure RADIUS Profiles** - Check the box to Configure RADIUS profiles for authentication and account
- **Set Captive portal RADIUS profiles** - Check the box to set captive portal RADIUS profiles
- **Set Captive portal mode** - Check the box to set the captive portal mode to customized
- **Configure QoS Rules** - Check the box to configure Pre Authentication QoS Rules
- **Transfer Pages to Controller** - Check the box to transfer portal redirection pages to controller
- **Write changes to startup-config** - Check the box to write changes to startup config.

24. Click on the **Setup Controller** button to apply the selection confirmation to the controller.

25. Click on the **Download portal pages** link for manual upload to the RADIUS client

**Note:** **System Director 6.0 & Later** - for versions of System Director 6.0 and later we configure the Captive Portal External URL with a redirection URL pointing to FortiConnect. Also, Automatic Setup no longer requires you to Transfer Custom Portal Pages from FortiConnect to the controller, Set the Captive Portal Mode to Customized and Set the Captive Portal Authentication Method to Internal as shown in the screenshot below.

Identity Manager Address:   
This hostname is used to redirect guests to the Identity Manager, it should match the SSL certificate on Identity Manager.

Device IP Address:

Admin user name:

Admin Password:

Configure RADIUS profiles:

Set Captive Portal RADIUS profiles:

Set Captive Portal External URL:

Configure QoS Rules:

Write changes to startup-config:  This will overwrite your startup-config with the current running-config

## RadSec Authentication

The main focus of RadSec is to provide a means to secure the communication between RADIUS/TCP peers on the transport layer. The most important use of RadSec lies in roaming environments where RADIUS packets need to be transferred through different administrative domains and untrusted, potentially hostile networks. An example for a world-wide roaming environment that uses RadSec to secure communication is Eduroam of which FortiConnect supports (see Network Access Policy section for Eduroam)

To enable RadSec Authentication on your RADIUS client go to **Devices --> RADIUS Clients** and click on the RadSec Authentication tab as shown below.

RADIUS Clients

Client Attributes SNMP MAC Authentication **RadSec Authentication** Automatic Setup

Enable RadSec:

RadSec Type: TLS

Verify SSL Certificate Common Name:

Hostname:

Save Cancel


1. Click the **Enable RadSec** checkbox to enable RadSec
2. From the **RadSec Type** dropdown menu, select TLS or DTLS as your RadSec type.
3. Click the **Verify SSL Certificate Common Name** checkbox to enable verification.
4. Enter the RADIUS Client **Hostname** in the field provided.
5. Click **Save** to continue.

## Editing RADIUS Clients

1. From the administration interface, select **Devices > RADIUS Clients** from the left hand menu.
2. In the RADIUS Clients page as shown below, select the RADIUS client from the list you wish to edit and click the underlined name of that client.

## RADIUS Clients

### RADIUS Clients

Name	Device	Type	Description	
<a href="#">RADIUS 1</a>	10.10.1.2/32	Meru SD 6.0 & Later	RADIUS 1	

[Add RADIUS Client](#)

### RADIUS Debug

RADIUS Support logs can be found in [Reports & Logs > System Logs > Support Logs](#)

RADIUS is running normally.

[Restart RADIUS in Debug](#)

### RADIUS Authentication

This setting controls whether RADIUS authentication is performed in a case sensitive or insensitive manner.

RADIUS username is

[Save](#)

3. In the Edit RADIUS Client page as shown below, click on the tabs you wish to Edit and follow the instructions as shown in **Adding RADIUS Clients**.


Click on **Save** once complete.

## Deleting RADIUS Clients

1. From the administration interface, select **Devices > RADIUS Clients** from the left hand menu.

## RADIUS Clients

**RADIUS Clients**

Name	Device	Type	Description	
<u>RADIUS 1</u>	10.10.1.2/32	Meru SD 6.0 & Later	RADIUS 1	

[Add RADIUS Client](#)

---

**RADIUS Debug**

RADIUS Support logs can be found in [Reports & Logs > System Logs > Support Logs](#)

RADIUS is running normally.

[Restart RADIUS in Debug](#)

---

**RADIUS Authentication**

This setting controls whether RADIUS authentication is performed in a case sensitive or insensitive manner.

RADIUS username is

[Save](#)

2. In the RADIUS Clients page as shown above, click the underlined name of the RADIUS client in the list to edit it.
3. Click the **dustbin** icon to the right of the entry to delete it, and confirm the action.

## RADIUS Accounting Servers

---

To add a RADIUS Accounting Server go to **Devices --> RADIUS Accounting Servers** and click on the **Add RADIUS Accounting Server** button as shown below. FortiConnect can replicate and forward any accounting packets to an admin defined server.

## RADIUS Accounting Servers

**RADIUS Accounting Servers**

Name	Device	Action
No RADIUS Accounting servers defined		

[Add RADIUS Accounting Server](#)

---

**User-Name Format**

Modify User-Name value:

Realm:   
Leave empty to use the realm the user authenticated with

Authenticate with:

- realm/username
- realm/username
- username@realm
- username

[Save](#)

1. On the Add RADIUS Accounting Server, enter the server details you wish to forward accounting packets to.

## RADIUS Accounting Server

Name:

Server IP Address:

Secret:  Confirm:

Accounting Port:

[Save](#) [Cancel](#)

2. In the fields provided, enter :-
  - **Name** - The name 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
3. Click on **Save** once complete
  4. If you wish to Modify the User-Name value of your server, then place a check in the **Modify User-Name value** check box as shown below.

**RADIUS Accounting Servers**

**RADIUS Accounting Servers**

Name	Device	Action
<a href="#">RAD_ACC</a>	10.10.1.2	

[Add RADIUS Accounting Server](#)

---

**User-Name Format**

Modify User-Name value:

Realm:   
Leave empty to use the realm the user authenticated with

Authenticate with:

- realm/username
- realm/username
- username@realm
- username

[Save](#)

5. **Realm** - Enter the Realm details
6. **Authenticate with** - Place a check next to the format you wish to authenticate with
7. Click on **Save** to complete your changes


## Editing a RADIUS Accounting Server

1. To Edit a RADIUS Accounting Server go to **Devices --> RADIUS Accounting Servers** and click on the link of the RADIUS Accounting Server you wish to edit as shown below



**RADIUS Accounting Servers**

**RADIUS Accounting Servers**

Name	Device	Action
<a href="#">RAD.ACC</a>	10.10.1.2	

[Add RADIUS Accounting Server](#)

---

**User-Name Format**

Modify User-Name value:

Realm:   
Leave empty to use the realm the user authenticated with

Authenticate with:

- realm/username
- realm/username
- username@realm
- username

[Save](#)

2. Follow steps 2 and 3 in the Add RADIUS Accounting Server section to Edit the server.

## Deleting a RADIUS Accounting Server

1. To Delete a RADIUS Accounting Server go to **Devices --> RADIUS Accounting Servers** and click on the Bin Icon of the RADIUS Accounting Server you wish to delete as shown below

**RADIUS Accounting Servers**

**RADIUS Accounting Servers**

Name	Device	Action
<a href="#">RAD ACC</a>	10.10.1.2	

[Add RADIUS Accounting Server](#)

---

**User-Name Format**

Modify User-Name value:

Realm:   
Leave empty to use the realm the user authenticated with

Authenticate with:

- realm/username
- realm/username
- username@realm
- username

[Save](#)

2. Click on **OK** to delete the server details or click on **Cancel** to abort.

## Syslog for RADIUS Accounting

---

FortiConnect can send RADIUS accounting information as Syslog messages to a firewall's and other devices to allow access to the client once they have logged onto the network via FortiConnect.

1. From the FortiConnect Administration interface go to **Devices --> Syslog Servers**.

## Syslog Servers

When RADIUS accounting is received a syslog message is sent to these servers.

Message Format: Smoothwall Firewall ▾

IP Address	Port	
There is no syslog server configured to send messages to		
<input type="text"/>	514	<input type="button" value="Add"/>

2. Select how the Syslog message should be formatted by selecting the **Message Format** from the drop down menu -
3. **Smoothwall Firewall** - this option will apply predefined format as under:
  - Start = "name=%{User-Name} mac=%{Calling-Station-Id} ip=%{Framed-IP-Address} \$"
  - Stop = "name=%{User-Name} mac=%{Calling-Station-Id} ip=%{Framed-IP-Address} \$"
  - Interim = "name=%{User-Name} mac=%{Calling-Station-Id} ip=%{Framed-IP-Address} \$"
4. **Custom** - this option lets admin define format against each point e.g Start, Stop and Interim as shown below.

When RADIUS accounting is received a syslog message is sent to these servers.

Message Format: Custom

Start: name=%{User-Name} mac=%{Calling-Station-Id} ip=%{Framed-IP-Address} \$

Stop: name=%{User-Name} mac=%{Calling-Station-Id} ip=%{Framed-IP-Address} \$

Interim: name=%{User-Name} mac=%{Calling-Station-Id} ip=%{Framed-IP-Address} \$

IP Address	Port
There is no syslog server configured to send messages to	
<input type="text"/>	514 <input type="button" value="Add"/>

5. Once completed click on **Save** to continue, this will send a message to all configured servers in this format.
6. Now add a **syslog server** to send messages to -
7. Enter the server **IP Address** and the **Port** number, click on the **Add** button once complete.
8. Click on **Save**.

## User Account Notification

---

When a User account is created, the details of the account need to be passed from the sponsor to the User. The FortiConnect provides a number of ways to do this:

- Manually reading the details to the User from the screen.
- Printing the details out on paper.
- Sending the details in an email.
- Sending the details as an SMS text message.

Sponsors always have the option of reading and printing out User account details to Users. Email and SMS text message notification require email servers to be configured, but can be configured based upon policy.

**Note:** Email and SMS User account notification policies need to be configured globally, then enabled per user group for individual sponsor permissions.

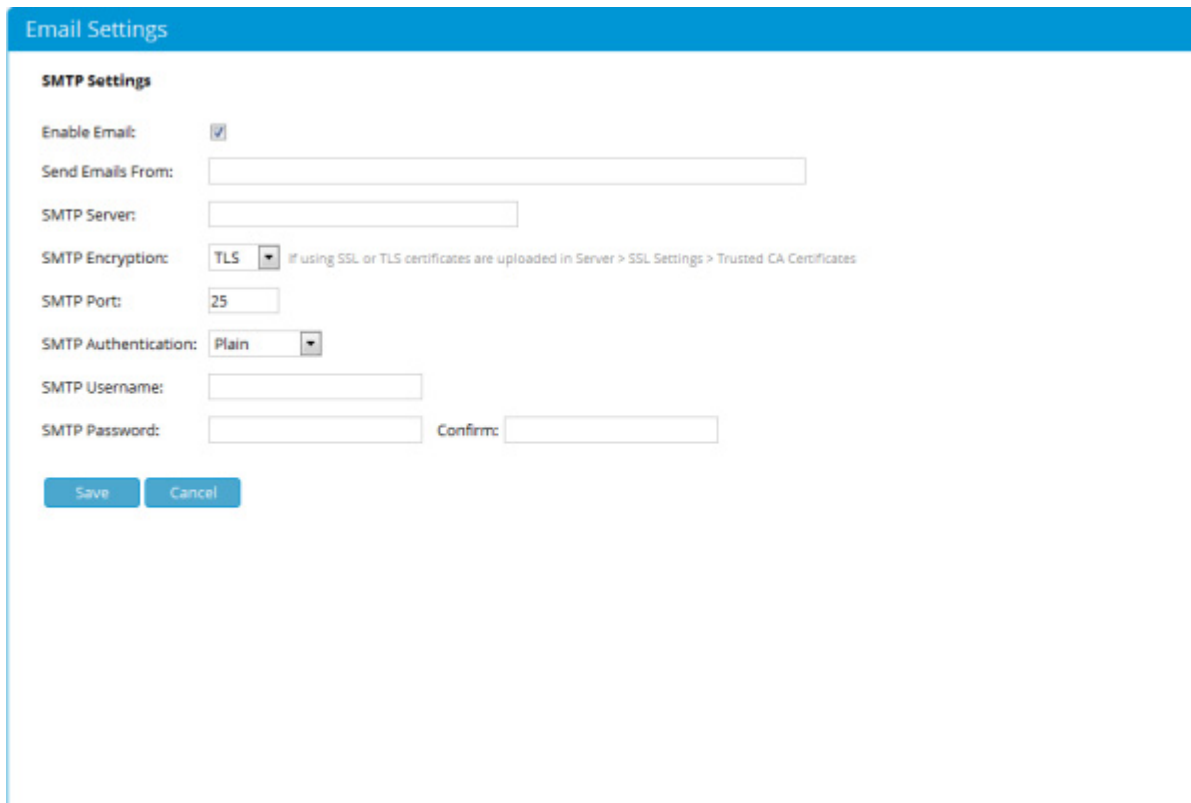
This chapter describes the following:

- Configuring Email Notification
- Configuring SMS Notification
- Print Notification

## Configuring Email Notification

The following steps describe how to configure email settings for the FortiConnect to correctly deliver User account details via email.

1. From the administration interface, select **Devices > Email Settings** from the left hand menu



The screenshot shows the 'Email Settings' configuration page in the FortiConnect administration interface. The page has a blue header with the title 'Email Settings'. Below the header, there is a section titled 'SMTP Settings'. The configuration options are as follows:

- Enable Email:** A checkbox that is checked.
- Send Emails From:** An empty text input field.
- SMTP Server:** An empty text input field.
- SMTP Encryption:** A dropdown menu set to 'TLS'. A note next to it reads: 'if using SSL or TLS certificates are uploaded in Server > SSL Settings > Trusted CA Certificates'.
- SMTP Port:** A text input field containing the number '25'.
- SMTP Authentication:** A dropdown menu set to 'Plain'.
- SMTP Username:** An empty text input field.
- SMTP Password:** Two text input fields, one for the password and one labeled 'Confirm'.

At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

2. In the Email Settings page as shown above, check the **Enable Email** option to enable email functionality globally for the FortiConnect.
3. For SMTP Server, type the IP address of the outbound SMTP server to which you need to deliver email. If you enter localhost, or leave this field empty, the FortiConnect attempts to deliver the email directly to the User's SMTP server.
4. In the Sent From field, type the email address from which you want User notification emails to be sent (for example, host@company.com).

5. From the **SMTP Encryption** drop down box, select whether SSL or TLS encryption is required. Certificates can be uploaded in the Server -->SSL Settings section.
6. From the **SMTP Authentication** drop down box you can select from three different types of authentication modes, select from **Plain**, **Login** or **CRAM-MDS** and enter the SMTP username and password details where required.
7. Click the **Save Settings** button.
8. Once this has been set up, you can perform an SMTP test by entering an email address in the **Send test email to** field.

**Note:** Refer to Editing the Email Template for additional details.

## Configuring SMS Notification

Short Message Service (SMS) is delivered through an SMS gateway service that supports SMTP (Simple Mail Transport Protocol) 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.

1. From the administration interface, select **Devices > SMS Settings** from the left hand menu.

### SMS Settings

Enable SMS:

SMS Service:  SMTP to SMS gateway

Twilio

SMPP

ThunderSMS

HTTP API

#### ThunderSMS Account

Sender ID:

API Key:

Confirm:

Verify

Server SSL

Certificate:

Save

Cancel

#### SMS Test

2. In the SMS Settings page as shown above, check the **Enable SMS** checkbox to globally enable SMS on the FortiConnect.
  - **SMTP to SMS Gateway** - Check this for SMTP to SMS gateway. SMS requires an SMTP server to deliver the

email to the SMS gateway. Click on the Email Settings link to configure the SMTP Server as described in the Configuring Email Notification section.

- **Twilio** - Check this to send SMS using Twilio.
  - **SMPP** - Check this to send using SMPP.
  - **ThunderSMS** - Check this to send SMS via ThunderSMS provider.
  - **HTTP API** - Check this to send an SMS via an HTTP(S) API.
3. In the Sent From field, type the sending email address for the email to be sent to the SMS gateway.
  4. Click **Save Settings**.
  5. Once this has been set up, you can perform an SMS test by entering a destination in the **Destination** field.

**Note:** FortiConnect supports Twilio and SMPP, see below on how to set this up.

6. **Twilio** - A Twilio API account along with a Twilio enabled phone number would be required to configure with the FortiConnect, enter the relevant details.
7. **SMPP** - (Short Message Peer to Peer) An SMPP API account would be required from the SMSC (Short Message Service Centre) to configure with FortiConnect.
8. **ThunderSMS** - Enter the Thunder SMS account details. The sender ID, API key, and a ThunderSMS enabled phone number are required.
9. **HTTP API** - This option integrates SMS providers that offer a HTTP(S) API for sending SMS. Enter the API URL and HTTP message details as shown below.

### SMS Settings

Enable SMS:

SMS Service:  SMTP to SMS gateway  
 Twilio  
 SMPP  
 ThunderSMS  
 HTTP API

---

#### HTTP API

The following variables should be used to customise the e-mail message.

- %DESTINATION% - The mobile number the message is addressed to.
- %MESSAGE% - The SMS message text.

API URL:

HTTP Method:

HTTP Headers:

HTTP POST body:

10. Click on **Save** once you have completed entering all the required details.

**Note:** Depending on how details are routed to the SMS provider, you need to customize the SMS portion of the User Interface template to include the User's mobile phone number in the correct format for your SMS gateway. See [Editing the SMS Template](#) for details.

## Print Notification

See “Editing the Guest Print Template” on page 175.

# User Activity Logging

---

User Activity Logging provides the ability for the FortiConnect to receive syslog information from network devices such as Firewalls, Proxy Servers and Routers. This information can provide details on all the connections that a User has made and Layer 7 information such as URLs accessed, depending on the network device.

User Activity Logging relies on knowing the IP address for each User as they authenticate to the network. The FortiConnect receives this information from RADIUS accounting, so you need to configure the network device that the user authenticates through to send this information. Commonly, this is the Wireless LAN Controller or NAC Appliance. Refer to the information in, “Configuring RADIUS Clients” for details on adding these devices as a RADIUS client.

**Note:** User Activity Logging relies on correlating the syslog information with the IP Address received from RADIUS accounting. This means that it will not work if you use a deployment method where the User's IP address changes after authentication and no additional RADIUS accounting messages are sent.

Once the FortiConnect has the IP Address of each of the Users, then it needs to receive syslog information from the network devices. You should configure each of your network devices to send syslog to UDP port 514 on the FortiConnect. The FortiConnect then processes the syslog information and correlates it against each User. This correlation enables you to view the User's activity on the User activity log details page for each User as described in [Reporting on Users](#).

User Activity is correlated into individual files that are stored on the disk of the appliance. The appliance can store log files until less than 30% disk space remains; it then either deletes the oldest log files or archives the log files to an external FTP server as described in [Configuring](#)

[Syslog Monitoring Settings](#). In addition if archiving is configured, logs are archived every hour to the external FTP server.

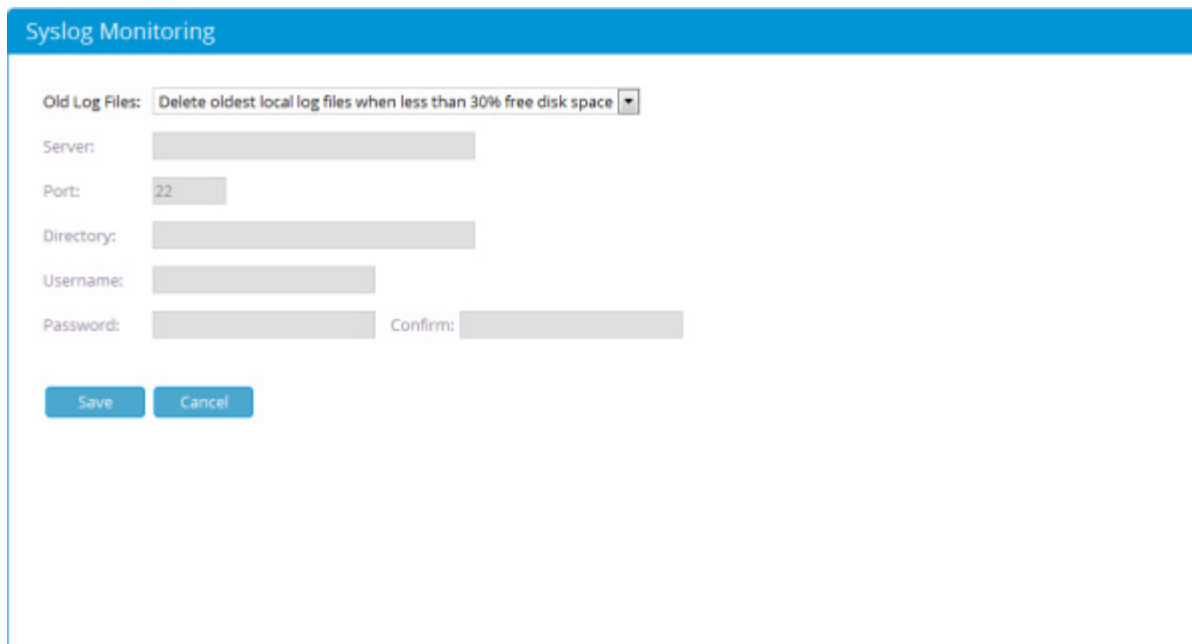
## Configuring Syslog Monitoring Settings

Archiving of logs to an FTP server provides the ability to store logs for long periods of time, and also provides the ability to back them up.



When viewing the logs through the sponsor interface, the FortiConnect automatically searches for logs on the archive server and displays them in the report for you.

1. From the administration interface, select **Devices > Syslog Monitoring** from the left hand menu as shown below.



The screenshot shows the 'Syslog Monitoring' configuration page. At the top, there is a blue header with the text 'Syslog Monitoring'. Below the header, there are several configuration fields:

- Old Log Files:** A dropdown menu with the selected option 'Delete oldest local log files when less than 30% free disk space'.
- Server:** A text input field.
- Port:** A text input field containing the value '22'.
- Directory:** A text input field.
- Username:** A text input field.
- Password:** A text input field.
- Confirm:** A text input field for password confirmation.

At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

2. To delete local log files when disk space is low, select **Delete oldest local log files when disk space is low** and click on **save**.

## Syslog Monitoring

Old Log Files:

Server:

Port:

Directory:

Username:

Password:  Confirm:

Passive Mode:

- To archive logs to an FTP Server select the **Archive to FTP Server** from the drop down menu and enter the relevant details
  - Server - Server name or IP address
  - Port - Port of the FTP Server
  - Directory - Directory of the FTP server you wish files to be stored in.
  - Username - Username of the account that has the ability to log onto the FTP server
  - Password - Password of the account that has the ability to log onto the FTP server
  - Passive Mode - check box if you wish to use passive mode

Click the Save Button when complete

## Syslog Monitoring

Old Log Files:

Server:

Port:

Directory:

Username:

Password:  Confirm:

- To archive logs to an SFTP Server select the **Archive to SFTP Server** from the drop down menu and enter the relevant details.

- Server - Server name or IP address
- Port - Port of the SFTP Server
- Directory - Directory of the SFTP server you wish files to be stored in.
- Username - Username of the account that has the ability to log onto the SFTP server
- Password - Password of the account that has the ability to log onto the SFTP server
- Passive Mode - check box if you wish to use passive mode.

Click on the Save Button when complete

## User Activity Logging with Replication Enabled

If you have a Cluster of FortiConnects replicating database information for resilience, then the User activity logs are not replicated between each box.

However, if you view the report in the Sponsor interface, the FortiConnect contacts the replication box and retrieves the logs from there. It then displays all logs in a consolidated view. This enables you to have some network devices send syslog to one FortiConnect and some to another, but then view all the results through a single interface.

Each FortiConnect retrieves the logs from the other FortiConnect in the replication pair securely over HTTPS. Each FortiConnect must trust the certificate of the other FortiConnect so that the retrieval can occur properly. To enable this, ensure that the root CA certificate for the other FortiConnect is uploaded as described in Uploading Certificate Files.

## Configuring the LDAP Server

---

FortiConnect has a built-in LDAP server that exposes User and Device accounts to applications that use the LDAP for User authentication and Device validation.

It is also possible to use the LDAP server to browse the current active User and Device accounts. This is unrelated to using an external LDAP server for Sponsor authentication.

Administer the FortiConnect LDAP Server by following the steps below.

1. From the administration interface select **Devices --> LDAP Server** and place a tick inside the **Enable LDAP Server** check box as shown below.

LDAP Server

Enable LDAP Server:

Admin Bind Username:

Admin Bind Password:  Confirm:

Protocol:

- LDAP
- LDAP, LDAPS and Start TLS
- LDAPS and Start TLS

2. Create an **Admin Bind Username** in the field provided.
3. Create an **Admin Bind Password** and **Confirm** in the fields provided.
4. Select the required protocol by placing a check in the relevant check box.
  - LDAP - Allow Unencrypted only.
  - LDAP, LDAPS and Start TLS - Allow Unencrypted and encrypted.
  - LDAPS and Start TLS - Allow encrypted only.
5. Click on **Save** once you have finished.

## Authenticating a User Account via LDAP

To authenticate a user account the client must bind to the LDAP server using the bind DN and password of the User account. The bind DN is always of the form:

```
cn=username,ou=users,dc=FortiConnect
```

where username is that of the user account. For example if we have a user account with username “test” the bind DN would be:

```
cn=test,ou=users,dc=FortiConnect
```

The base DN for searching is always:

```
ou=users,dc=FortiConnect
```

Users can only be authenticated if they are active and are not currently under any time restrictions.

## Troubleshooting User Authentication

We can use command-line tools and graphical tools to test the behaviour of the LDAP server. For example if the `ldapsearch` command is available on a client machine we can test authentication using the following (where `testpassword` and `testusername` are the users credentials and `x.x.x.x` is the IP address of the FortiConnect server):

```
ldapsearch -h x.x.x.x -x -D "cn=testusername,ou=users,dc=FortiConnect" -w testpassword
```

This will return all the detail of the account, including the DN:

```
dn: cn=test,ou=users,dc=FortiConnect
```

If the username or password is incorrect it will return:

```
ldap_bind: Invalid credentials (49)
```

## Validating a Device Account via LDAP

Device accounts may be validated in a similar way to User accounts, however device accounts do not have passwords so we must use the admin bind credentials to search for the existence of a device account.

The device DN is always of the form:

```
cn=aa:bb:cc:dd:ee:ff,ou=Devices,dc=FortiConnect
```

Where the CN is the MAC address of the device in a canonical format.

We may search for a device using `ou=Devices,dc=FortiConnect` as the base DN and `cn=aa:bb:cc:dd:ee:ff` as the filter.

Many other MAC address formats are supported for searching, the `altMacAddressFormat` attribute should be used e.g. using a filter of `altMacAddressFormat=aabb-ccdd-eeff`.

## Testing Device Validation

We can use command-line tools and graphical tools to test the behaviour of the LDAP server. For example if the `ldapsearch` command is available on a client machine we can test validation of device accounts with the following (where `x.x.x.x` is the IP address of the FortiConnect server and `adminuser` and `adminpassword` are the admin bind username and password respectively and we assume we have a device with a MAC address of `aa:bb:cc:dd:ee:ff`):

```
ldapsearch -h x.x.x.x -LLL -x -D "cn=adminuser,dc=FortiConnect" -w adminpassword  
(cn=aa:bb:cc:dd:ee:ff)
```

This will return all the details of the device, including:

dn: cn=aa:bb:cc:dd:ee:ff,ou=Devices,dc=FortiConnect

If the username or password is incorrect it will return:

ldap\_bind: Invalid credentials (49)

It will not display any results if the device is not found.

## Browsing Guest and Device Accounts

While configuring clients that access the LDAP server it may be useful to view the LDAP

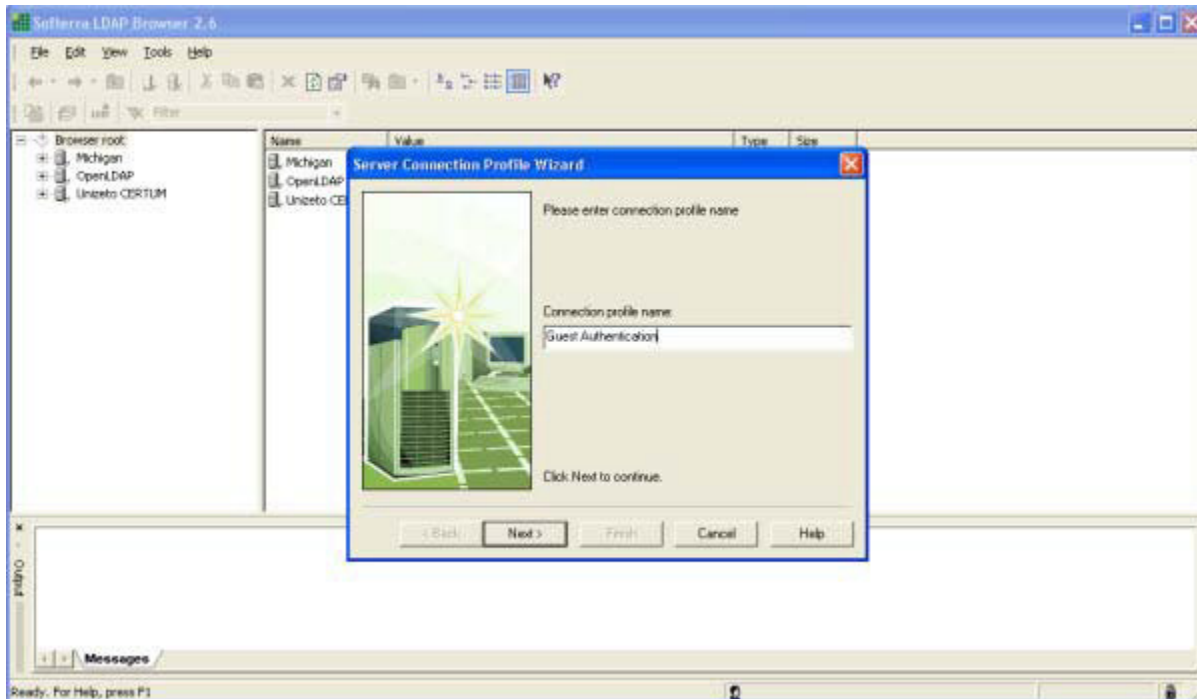
database using a LDAP browsing application. The following screenshots are taken of the free LDAP Browser application from Softera (<http://www.ldapadministrator.com>).

In the examples that follow the FortiConnect is running on 192.168.137.20 and the LDAP server has been configured with the username “admin” and password “password”:

- Guest Authentication
- Device Validation
- Browsing

## User Authentication

1. Click on **File** then **New Profile** from the drop down menus and select **Create New File** and name it Guest Authentication



2. Click Next
3. Host - IP Address of the FortiConnect
4. Leave the Port and Protocol version as they appear.
5. Base DN = ou=Guests,dc=GuestManager

Host Information

Please enter server host information

Host: 192.168.137.20

Port: 389 Protocol version: 3

Base DN: ou=Guests,dc=GuestManager

Fetch DNs (only LDAP v.3)

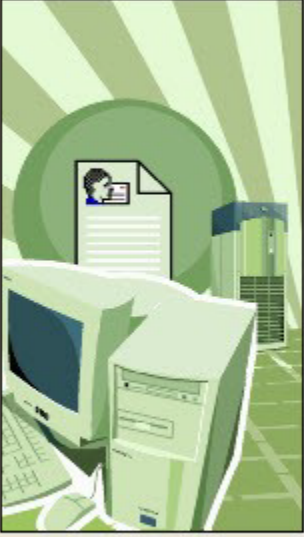
Anonymous bind

Click Next to continue.

< Back Next > Finish Cancel Help

6. Click Next
7. User DN = Guest User DN
8. Password = Guest User Password
9. Click on the check box to Save Password.

### Credentials



Please enter user information

User DN:

Password:

Save password

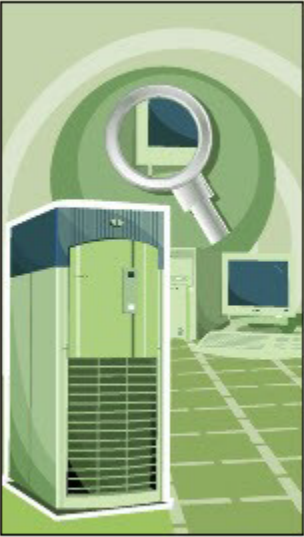
Click Next to continue.

< Back   Next >   Finish   Cancel   Help

10. Click Next

11. Click Finish as shown below.

### LDAP Settings



Connection Options

Filter:

Timeout:    Entry count limit:

Try to use secure connection (only LDAP v.3)

Dereference Aliases

Never    Searching  
 Finding    Always

Enable Referrals  
 Connect now

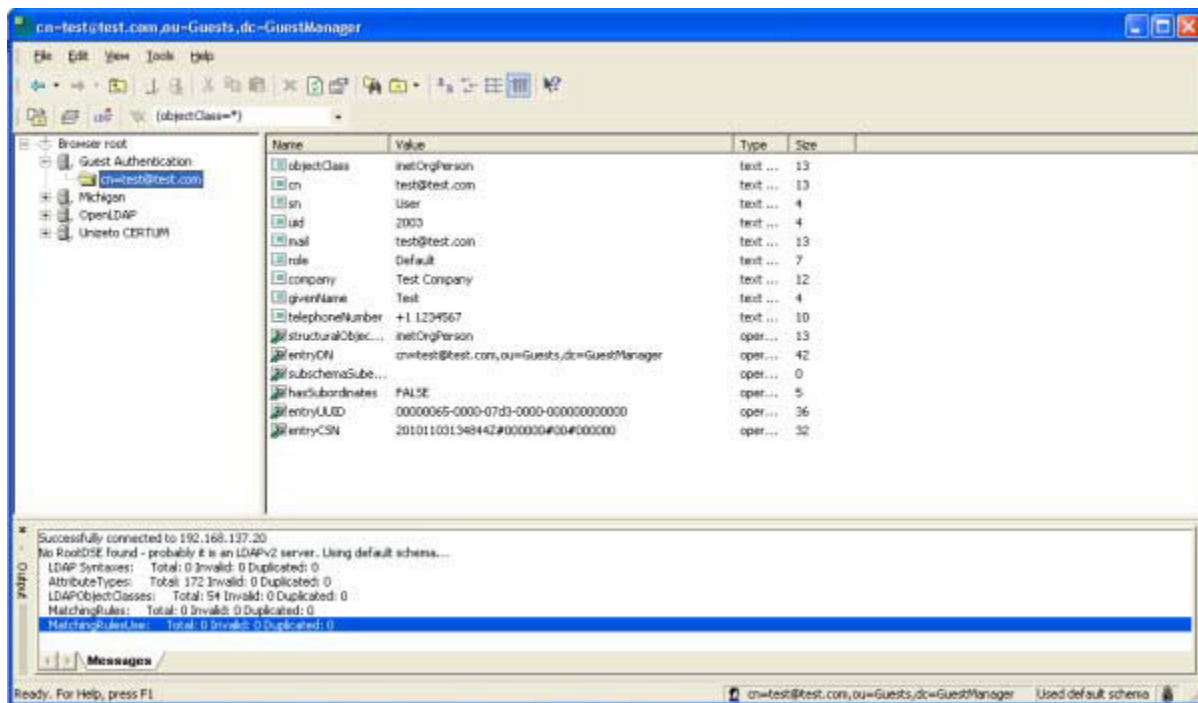
Advanced...

< Back   Next >   Finish   Cancel   Help



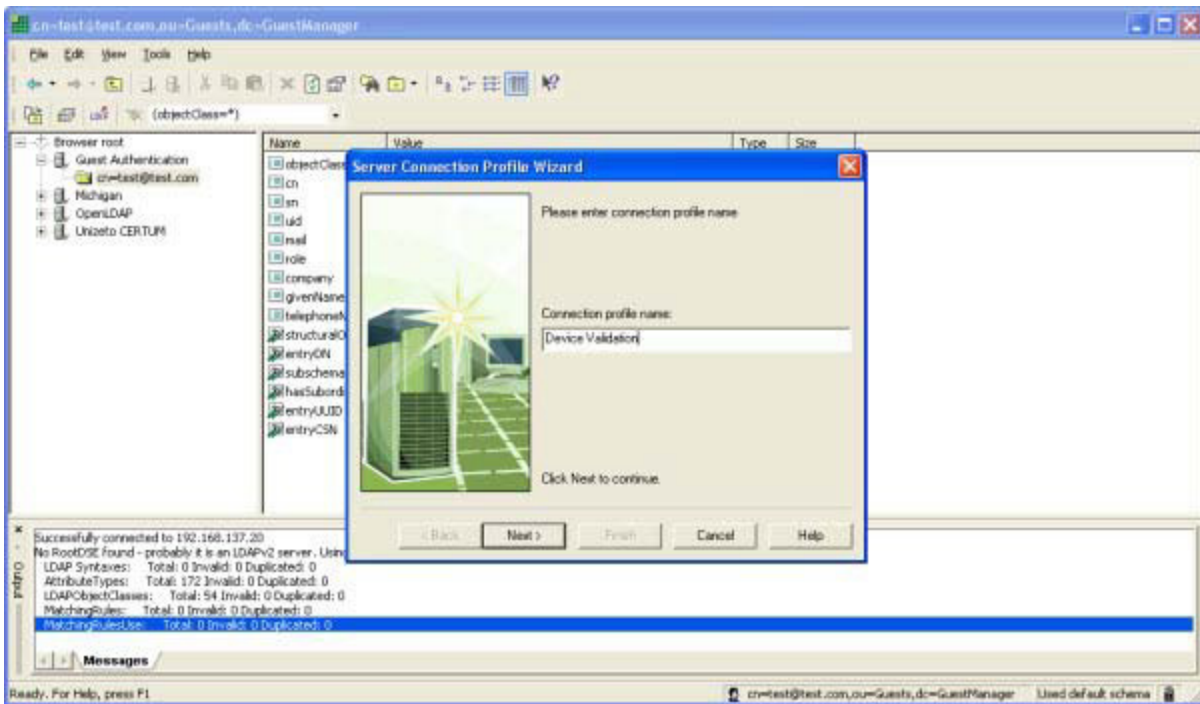
The results should be shown in the Guest Authentication folder.

Click on the folder to see the results and prove the Guest has authenticated.

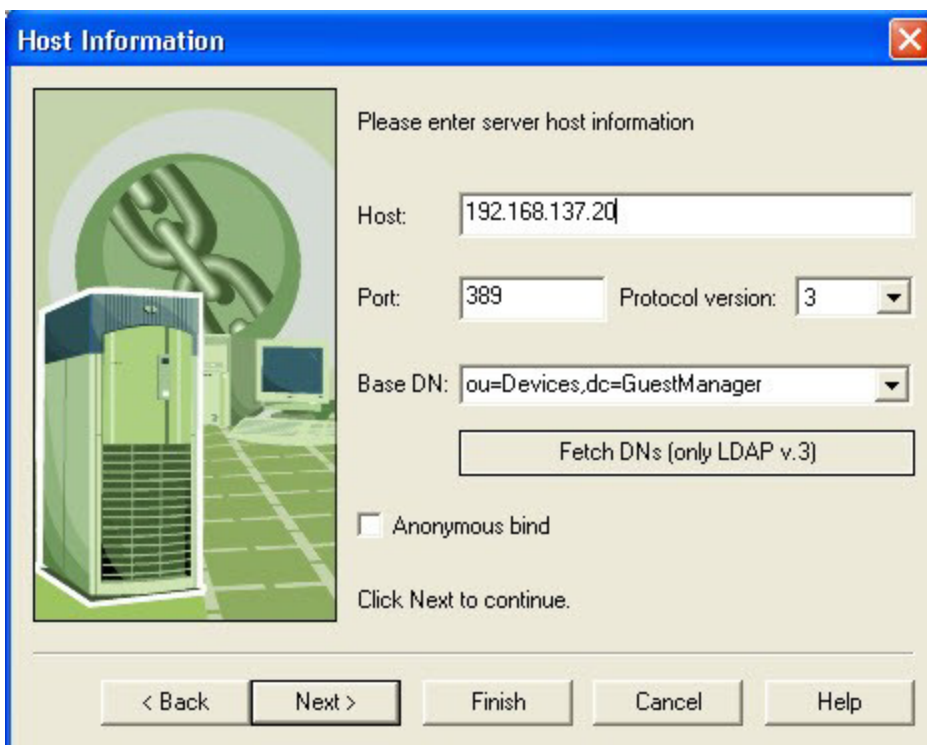


## Device Validation

1. From the drop down menu select **File-->New Profile** and create a new profile called **DeviceValidation**.



2. Click Next
3. Host - FortiConnect IP Address
4. Base DN - ou=Devices,dc=GuestManager
5. Port and Protocol remain how they are.



The image shows a Windows-style dialog box titled "Host Information". On the left is a 3D illustration of a server rack. The main area contains the text "Please enter server host information". There are four input fields: "Host" with the value "192.168.137.20", "Port" with "389", "Protocol version" with a dropdown menu showing "3", and "Base DN" with a dropdown menu showing "ou=Devices,dc=GuestManager". Below these is a button labeled "Fetch DN's (only LDAP v.3)". There is an unchecked checkbox for "Anonymous bind" and the text "Click Next to continue." at the bottom. At the very bottom are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

Host Information

Please enter server host information

Host: 192.168.137.20

Port: 389 Protocol version: 3

Base DN: ou=Devices,dc=GuestManager

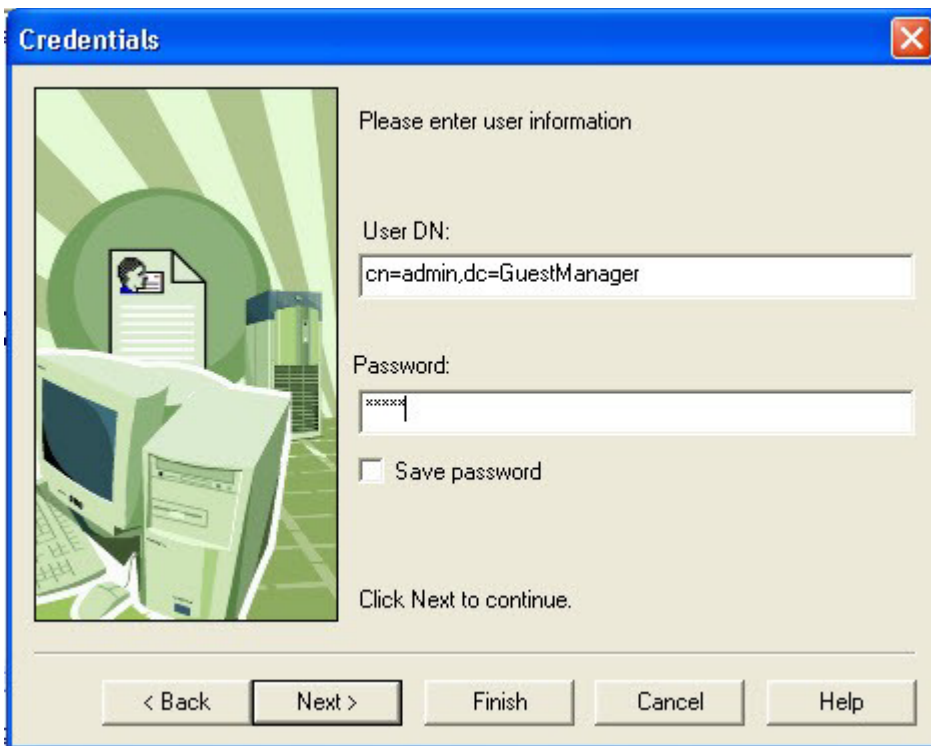
Fetch DN's (only LDAP v.3)

Anonymous bind

Click Next to continue.

< Back Next > Finish Cancel Help

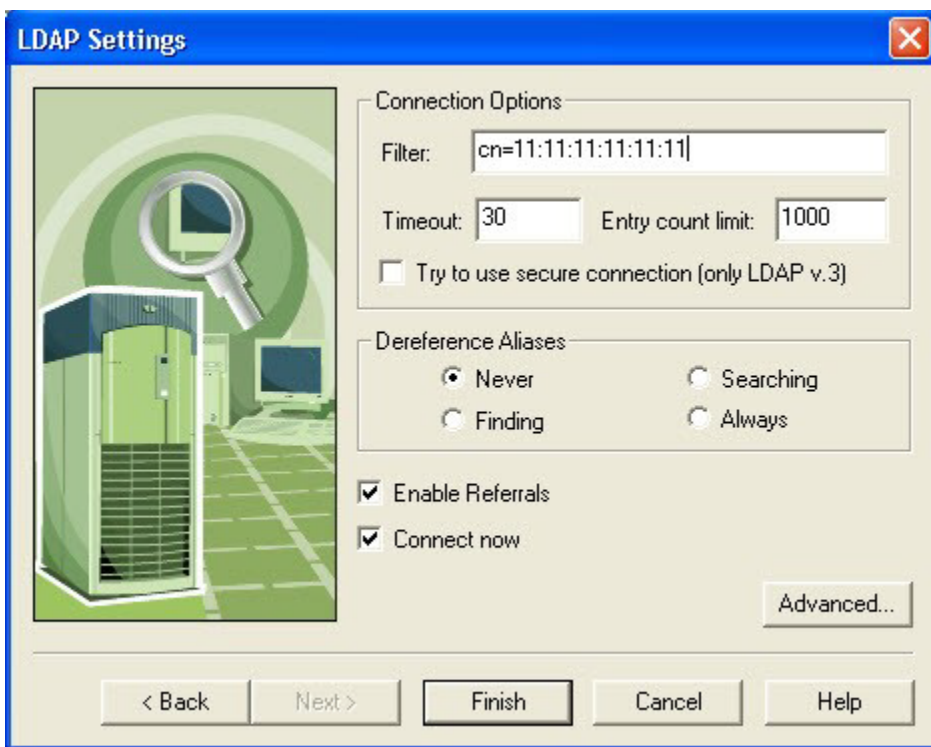
6. Click **Next**
7. User DN, this is the username created when setting up LDAP FortiConnect - cn=Admin,dc=GuestManager
8. Password, this is the password created when setting up LDAP FortiConnect.



9. Click Next

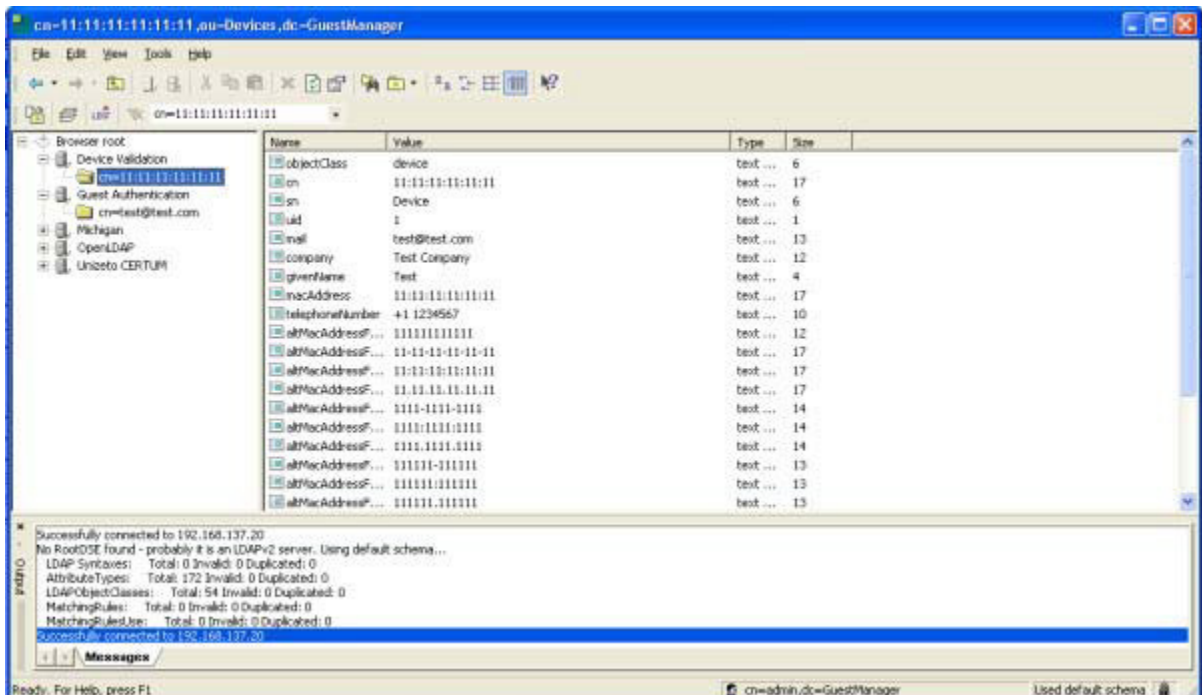
10. You must then setup a filter to find whether the Device exists. Filter - MAC Address of the Device.

11. Leave all other options as they are.



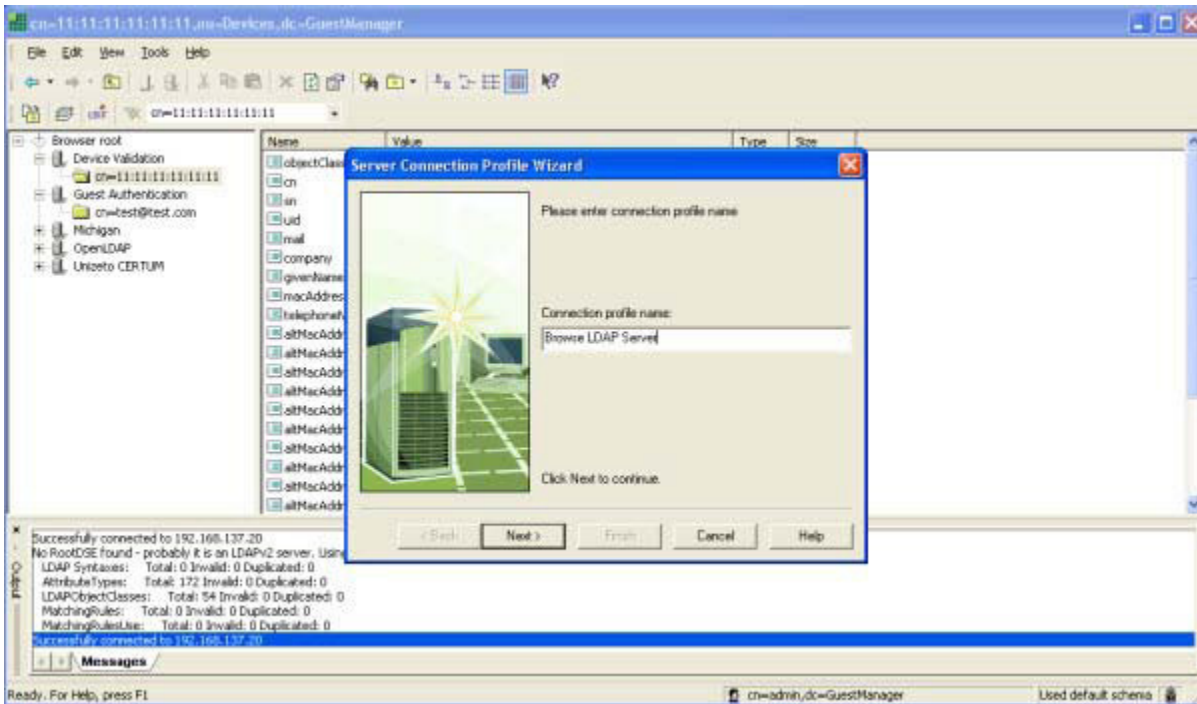
## 12. Click Finish

Under the Device Validation option on the menu, click on the Device Validation to prove the Device has validated as shown below.

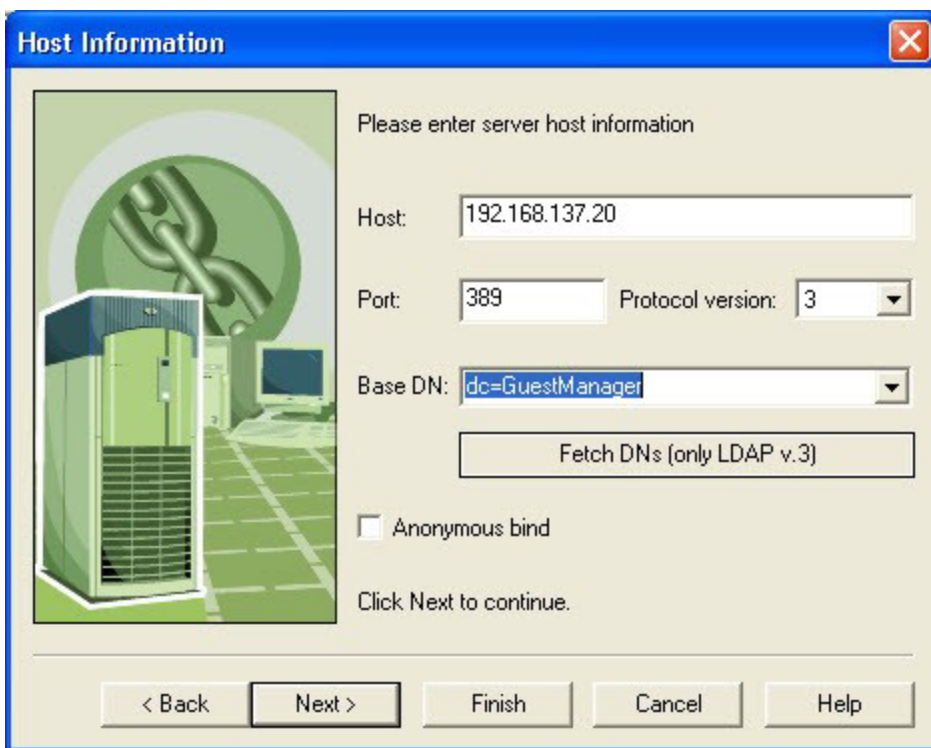


# Browsing the LDAP Database

1. From the drop down menu select **File-->New Profile** and create a new profile called **Browse LDAP Server**.



2. Click **Next**
3. Host is the IP Address of your FortiConnect
4. Base DN is - dc=GuestManager
5. Leave the Port and Protocol settings as they appear.



The image shows a Windows-style dialog box titled "Host Information". On the left is a 3D illustration of a server rack in a data center. The main area contains the text "Please enter server host information". There are four input fields: "Host" with the value "192.168.137.20", "Port" with the value "389", "Protocol version" with a dropdown menu showing "3", and "Base DN" with a dropdown menu showing "dc=GuestManager". Below these is a button labeled "Fetch DN's (only LDAP v.3)". There is an unchecked checkbox for "Anonymous bind" and the text "Click Next to continue." at the bottom. At the very bottom are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

Host Information

Please enter server host information

Host: 192.168.137.20

Port: 389 Protocol version: 3

Base DN: dc=GuestManager

Fetch DN's (only LDAP v.3)

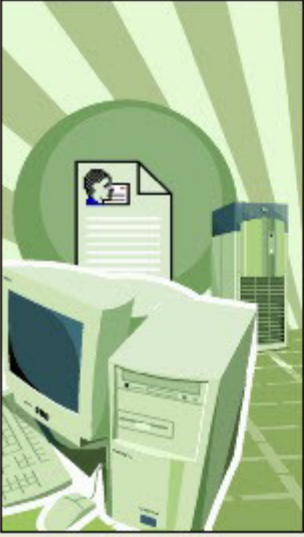
Anonymous bind

Click Next to continue.

< Back Next > Finish Cancel Help

6. Click **Next**
7. User DN is - cn=admin,dc=GuestManager
8. Password is the password you created when setting up the LDAP FortiConnect.

**Credentials** ✕



Please enter user information

User DN:

Password:

Save password


Click Next to continue.

< Back   **Next >**   Finish   Cancel   Help

9. Click Next

10. Leave the filter as it appears, this will search for all entries.

**LDAP Settings** ✕



Connection Options

Filter:

Timeout:    Entry count limit:

Try to use secure connection (only LDAP v.3)

Dereference Aliases

Never    Searching  
 Finding    Always

Enable Referrals  
 Connect now

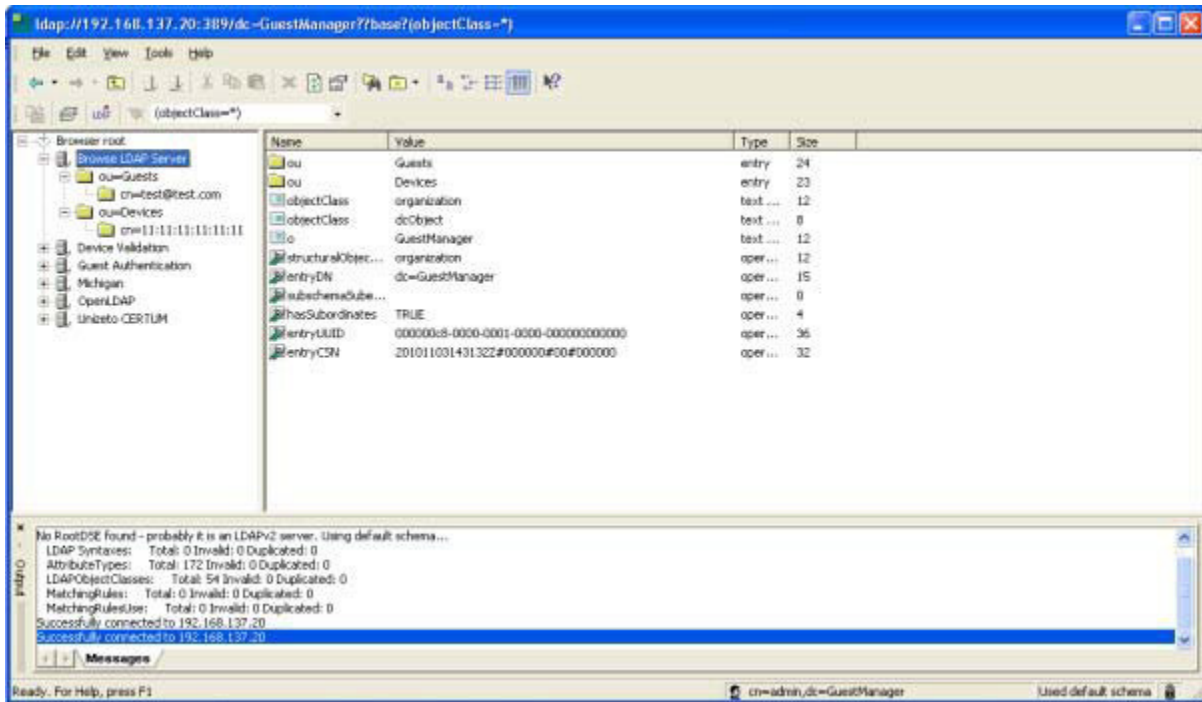
Advanced...

< Back   **Next >**   Finish   Cancel   Help



## 11. Click Finish

Search results will display everything in the Database under the **Browse LDAP Server** folder as shown below.



## MDM Servers

FortiConnect can now integrate with MDM Vendors, current supported vendors are -

- Xenmobile
- Airwatch
- Mobile Iron

An MDM server can be added, then Authorization Policies created with rules based on the MDM integration by going to **Network Access Policy --> Authorization Policy** from the FortiConnect Admin interface.

To add an MDM server, go to **Devices --> MDM Servers** as shown on the screen below.

## MDM Servers

Name	Description	Vendor	Enabled	Action
No MDM servers defined				

[Add MDM Server](#)

1. Click on the **Add MDM Server** button to enter the MDM Server details as shown below

## Add New MDM Server

Server Name:

Server Description:

Vendor:  ▾

Server:

Validate Certificate:

Username:

Password:  Confirm:

API Key:

[Save](#) [Cancel](#)

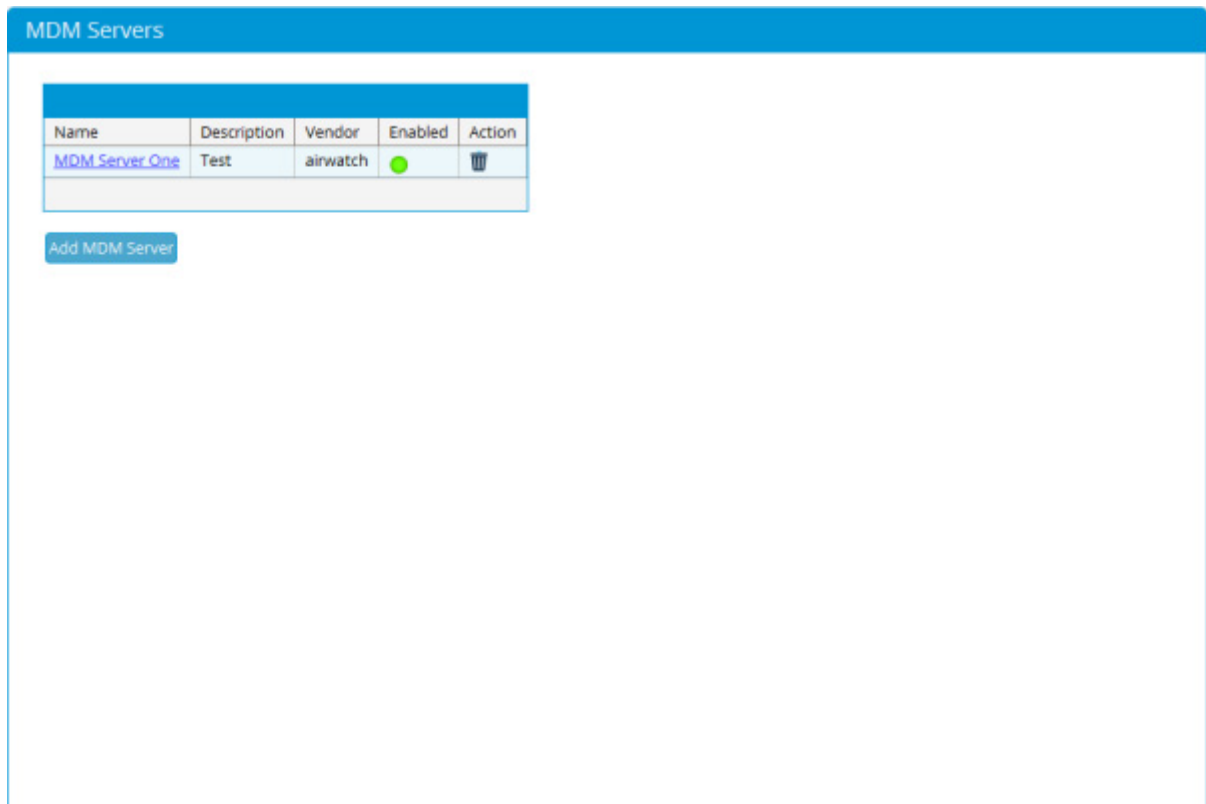
2. Now enter your Server details -

- **Server Name** - Enter the MDM server name
- **Server Description** - Enter the description of the MDM server
- **Vendor** - From the drop down menu select which Vendor of MDM server you wish to integrate with
- **Server** - Enter the IP address or the hostname of the server
- **Validate Certificate** - Check this box to validate the SSL cert on the server (CA certs must be installed on the FortiConnect for this to work)
- **Username** - Enter the username of the MDM server
- **Password** - Enter the password of the MDM server and confirm it
- **Tenant Code** - Enter the Tenant Code of the MDM server

3. Click on **Save** once complete

## Editing an MDM Server

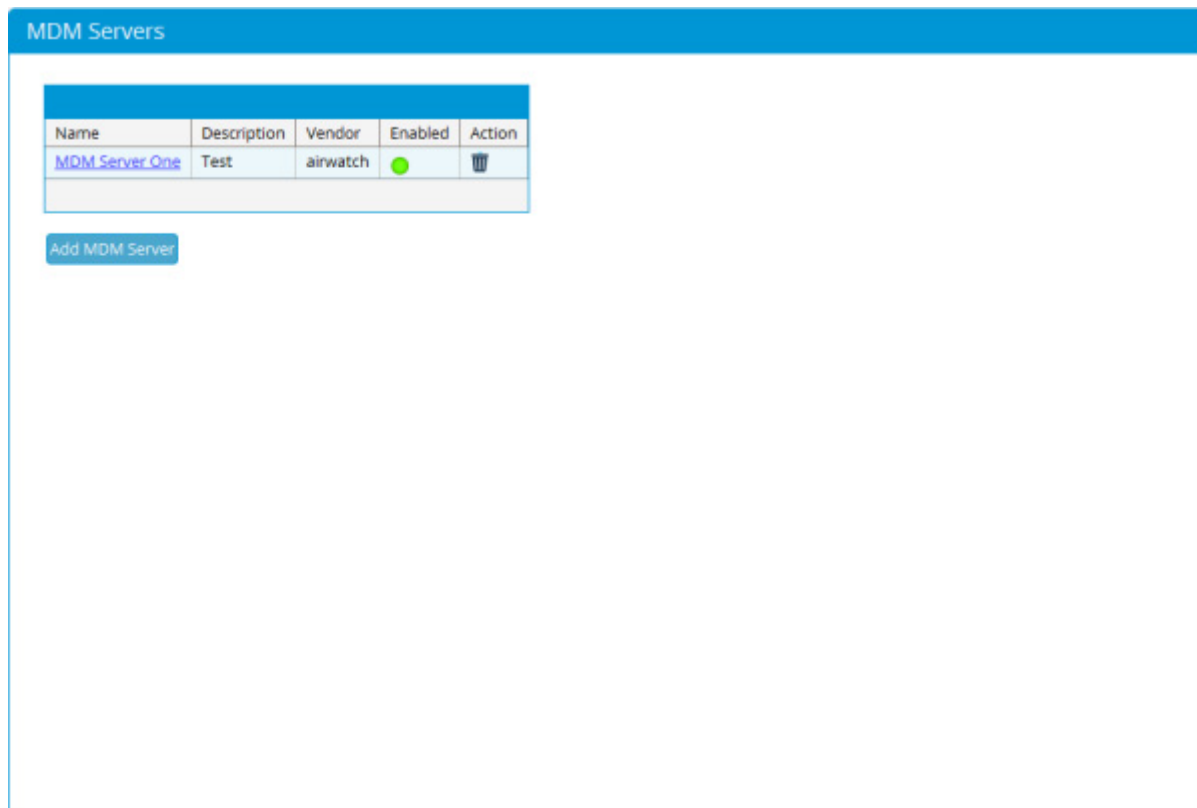
To Edit an MDM Server go to **Devices --> MDM Servers** as shown on the screen below.



1. Click on the **Name** of the MDM Server you wish to Edit and perform any necessary changes.
2. Click on **Save** once complete.

## Deleting an MDM Server

To Delete an MDM Server go to **Devices --> MDM Servers** as shown on the screen below.



1. Click on the **Bin Icon** next to the MDM Server you wish to delete.
2. Click on **Ok** to confirm deletion.

## Wi-Fi Based Marketing Notification Services

---

FortiConnect introduces support for 3rd party Wi-Fi based marketing notification services. Wi-Fi Based marketing notification services enables merchants to push promotions and other related notifications to customers in their close proximity.

# How This Works

In FortiConnect, add the server / services details of the notification service provide. After adding this service, enable it in the Guest Portal settings. Any user authenticating via the FortiConnect guest portal login will start seeing the notifications pushed from the server enabled in Guest Portal Settings.

**Note:** Only one server can be enabled per portal. Guest users will receive promotions from the server that is enabled in the guest portal and used by the guests to login

## Adding and Configuring the Service

1. Login to FortiConnect Administration UI and go to Devices > WiFi Marketing Providers.



2. Click Add New Server to add a new service provider and enter the following details:

Field Name	Description
Server Name	Specify a name to identify the service provide. For ease of use, use the actual name of the service provider
Server Description	Specify additional information about the service provider

Field Name	Description
Vendor	Select the vendor from the list. <b>NOTE:</b> This release supports only WiForia
Host	Enter the IP address or domain name provided by the service provider
Service ID	This is provided by the service provider and is used to authenticate FortiConnect in their server
Username	This is provided by the service provider
Password	This is provided by the service provider

Server Name:

Server Description:

Vendor:

Host:

Service ID:

Username:

Password:  Confirm:

Leave blank to keep existing password

3. After adding server details, click the **SAVE** button to continue.

In the Portal settings page, enable Wi-Fi marketing service. Go to **Portals**. You can select an existing portal or create a new one. If you already have portal to which you plan to enable the Wi-Fi marketing service, do the following:

Click an existing portal to open the **Portal Settings Wizard**. Click the **Next** button to navigate to the Portal Settings section. In this section, select **WiFi Marketing Integration** option to enable notification services.

★ Portal Settings

Portal Policy

Page	Displayed in menu	
	Pre-Authentication	Post-Authentication
Login	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Password Change	<input type="checkbox"/>	<input type="checkbox"/>
Self Service	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Registration	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Billing	<input type="checkbox"/>	<input type="checkbox"/>
Successful Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Welcome Back	<input type="checkbox"/>	<input type="checkbox"/>
Smart Connect	<input type="checkbox"/>	<input type="checkbox"/>
PMS Billing	<input type="checkbox"/>	<input type="checkbox"/>
Access without Login	<input type="checkbox"/>	<input type="checkbox"/>
Password Recovery	<input type="checkbox"/>	<input type="checkbox"/>
My Account	<input type="checkbox"/>	<input type="checkbox"/>
Help	<input type="checkbox"/>	<input type="checkbox"/>
Welcome	<input type="checkbox"/>	<input type="checkbox"/>

**Session Management**

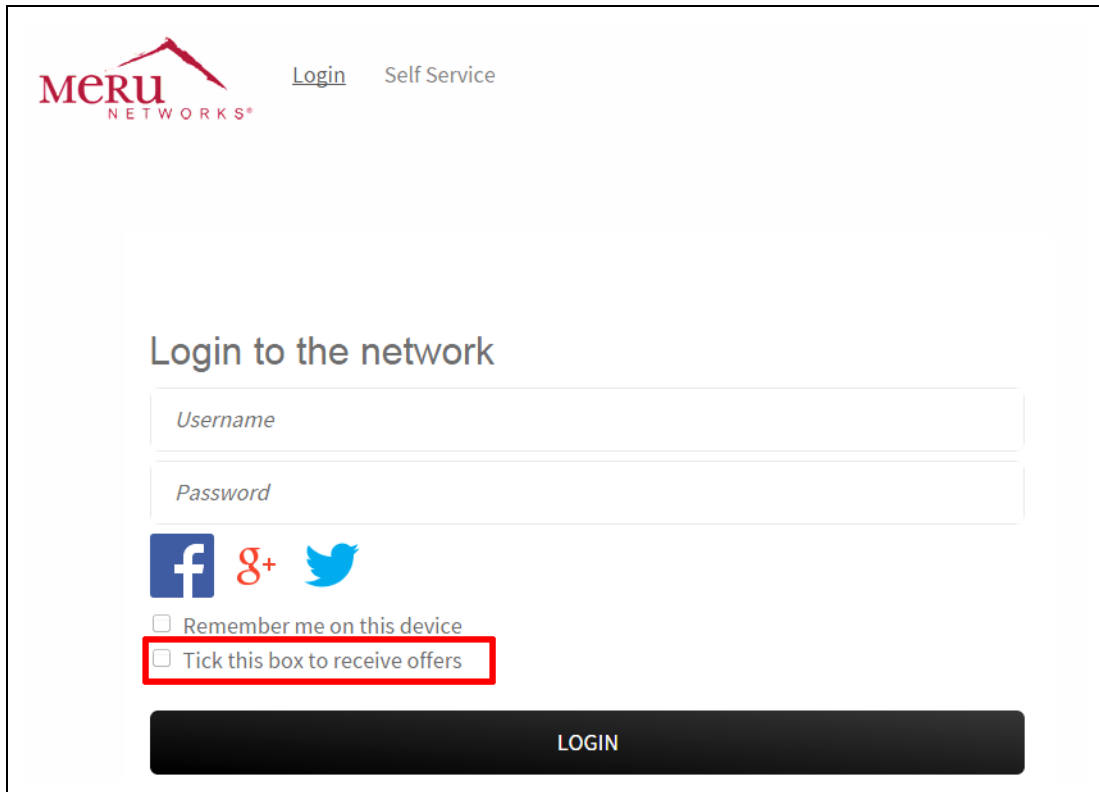
Allow user to close existing sessions when the concurrent session limit is exceeded:

**WiFi Marketing Integration**

Enable WiFi Marketing Integration:

# For the Users

To receive notifications from the service providers, users login in using the captive portal page, must opt-in to receive notifications.






Meru NETWORKS®

[Login](#) [Self Service](#)

### Login to the network

Username

Password

Remember me on this device

Tick this box to receive offers

LOGIN

## Limitations

1. When a guest moves from one AP to another (change in location), FortiConnect can notify WiForia of this change only after 10 minutes, as the Controller will do the radius update only after 10 minutes (this can be changed based on the configuration in the controller, minimum value is 10 minutes).
2. The feature will work only for users who would do Self Service. i.e feature will not work for Guest accounts created by Sponsor.
3. Feature will not work for guests who authenticate with their Twitter accounts as Twitter will not send us the email address of the guest user.
4. This feature will not work for Mac authentication as Controller does not send Radius Accounting for this.







# Managing Guest Portals

Portals on the FortiConnect are used to allow administrators to create their own portal pages and host them on the FortiConnect.

Portals created by administrators can be fully customized and used as the portal to provide the following:

- Customized authentication pages—Allow portal pages to be located on the FortiConnect 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.
- PMS Integration - Property Management System Integration
- Smart Connect - Secure Smart Connect provisioning for devices.

This chapter explains the following:

- Configuring Portals Sites
- Configuring Payment Providers
- Creating Portal Web Pages
- Event Codes

## Creating a Guest Portal









---

When adding a Portal Site, the FortiConnect will take you through the Portal Wizard to enable easy setup.

1. From the FortiConnect Admin interface, select **Guest Portals-->Portals** as shown below.

## Portals

Showing 1-2 of 2 10 per page Go

Name	Description	
<a href="#">access-denied</a>	Default portal that denies access	   
<a href="#">login</a>	Default login portal	   

Page 1 of 1 Go

Add Portal

2. Click on the **Add Portal** button to bring up the Portal Wizard as shown below.

Portal Setup Wizard

★ Welcome

Portal Name

Portal Theme

Portal Settings

Portal Policy

### Welcome to the Guest Portal setup wizard

This wizard will guide you through the steps needed to edit a Guest Portal. Please finish the wizard completely to avoid any errors which may arise if left incomplete.

Select Next to start the wizard.

< Back   Next >   Exit

3. Now click on **Next** to start the wizard and bring up the **Basic Settings** page.

The screenshot shows the 'Portal Setup Wizard' interface. On the left, a sidebar contains a list of steps: 'Welcome' (checked), 'Portal Name' (selected with a star), 'Portal Theme', 'Portal Settings', and 'Portal Policy'. The main content area is titled 'Name' and includes the instruction: 'Please provide a name and description for the portal. Guests will see the name in the portal URL.' Below this are two input fields: 'Name:' and 'Description:'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

4. Enter a **Site Name** and a **Site Description**, note that the name you enter will be visible by Portal users as it will be part of the site url.
5. Click on **Next** to continue.

## Configuring Portal Theme


1. Select a predefined **Portal Theme** as shown above (contact Fortinet to create a customized theme for your company), you can also upload new themes via **Guest Portals --> Themes**.
2. You will be asked to confirm your selection and be made aware that changing the theme will result in the new theme definition being used throughout the rest of the portal. Click **Yes** to acknowledge.

**Portal Setup Wizard**


- ✓ Welcome
- ✓ Portal Name
- ★ **Portal Theme**
- Portal Settings
- Portal Policy

### Theme


The theme is the look and feel of your portal. You can upload new themes from Guest Portals -> Themes.




Name: **Meru Networks (Responsive Theme)**  
Author: *Meru Networks*  
Description: Responsive theme based on the Meru Networks color scheme and logo



Name: **Meru Networks (white)**  
Author: *Meru Networks*  
Description: Theme based on the Meru Networks color scheme and logo



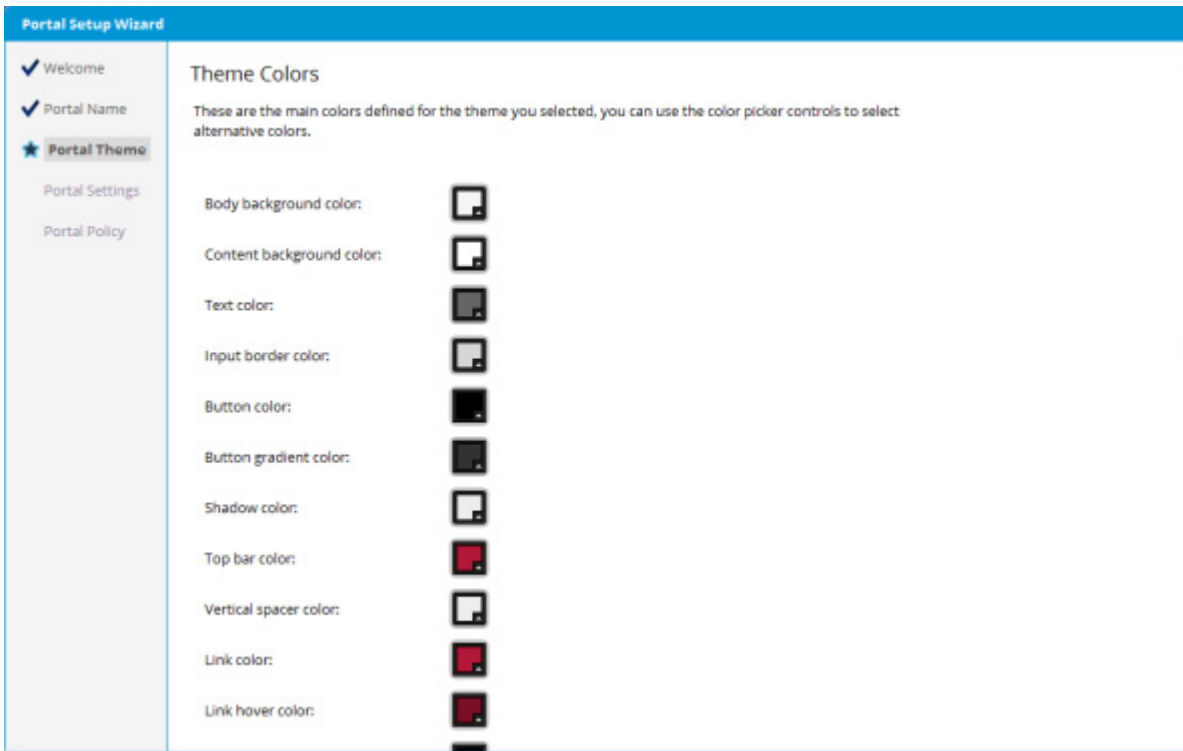
Name: **White Mobile Theme (All Devices)**  
Author: *Meru Networks*  
Description: This theme is for mobile devices.



Name: **Access Denied**

**Note:**

3. Click on Next.



4. Select a color scheme for your **Portal Theme**, click on the relevant boxes next to the text to change their color.
5. Click on **Next** to continue.



Portal Setup Wizard


- ✓ Welcome
- ✓ Portal Name
- ★ **Portal Theme**
- Portal Settings
- Portal Policy

### Theme Images

The images will be used on the Portal.


Supported file formats are JPG, GIF and PNG. Using larger images may result in the portal not looking as the theme intended.

Company logo large:




No file chosen  
It is recommended you use an image with 300x40 pixels.

Company logo medium:



No file chosen  
It is recommended you use an image with 170x70 pixels.

Company logo small:



No file chosen  
It is recommended you use an image with 170x70 pixels.

6. Select a corporate image to use with your **Portal**.
7. Click **Next** to continue.

# Configuring Portal Settings

### Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ★ **Portal Settings**

Portal Policy

#### Portal Pages

Specify which pages your portal should have enabled and at what stage they should be available.

Page	Displayed in menu	
	Pre-Authentication	Post-Authentication
Login	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Password Change	<input type="checkbox"/>	<input type="checkbox"/>
Self Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Registration	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Billing	<input type="checkbox"/>	<input type="checkbox"/>
Successful Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Welcome Back	<input type="checkbox"/>	<input type="checkbox"/>
Smart Connect	<input type="checkbox"/>	<input type="checkbox"/>
PMS Billing	<input type="checkbox"/>	<input type="checkbox"/>
Access without Login	<input type="checkbox"/>	<input type="checkbox"/>
Password Recovery	<input type="checkbox"/>	<input type="checkbox"/>
My Account	<input type="checkbox"/>	<input type="checkbox"/>
Help	<input type="checkbox"/>	<input type="checkbox"/>
Welcome	<input type="checkbox"/>	<input type="checkbox"/>

#### Session Management

Allow user to close existing sessions when the concurrent session limit is exceeded:

#### WiFi Marketing Integration

Enable WiFi Marketing Integration:

#### Logout Options

Enable Logout Button:

Enable Logout Pop-up window:

1. You can add or remove features to the Portal by modifying the selection of pages that should be available to users as shown above. In each case, select **Pre-Authentication** to make the feature available before authentication, select **Post-Authentication** to make the feature available after authentication, or leave both check boxes blank to disable that feature.

Select :

- **Login** - Display a screen that will allow a user to Login in.
- **Password Change** - Display a screen allowing the user to change their password.
- **Self Service** - Display a screen that allows a user to create their own account using Self Service.
- **Device Registration** - Display a screen that enables a user to register their own device.
- **Credit Card Billing**- Display a screen that enables Credit Card Billing.
- **Successful Authentication** - Display a screen that shows Successful Authentication.
- **Welcome Back** - Display a welcome back page if the user has authenticated previously.
- **Smart Connect** - Check to enable Smart Connect on the portal.

- **PMS Billing** - Display a screen that enables PMS Billing.
- **Access Without Login** - Allow access without having to authenticate.
- **Password Recovery** - Display a page allowing password recovery options.
- **My Account** - Display 'My Account' details for the user to manage their account once logged in.

My Account page offers following features after log in for the user.

- View account details
  - Change password provided when change password feature is enabled
  - Detail If it is a purchased account
  - List all the payments a User made to purchase access plans
  - Printing purchased receipts
  - If logged in as an active account
  - Top-up a Users usage by extending account time and data allowance by purchasing an Access Plan
  - If logged in as expired account
  - Reactivate their account to get connect to the network
    - **Help** - Display a Help page screen. (optional page)
    - **Welcome** - Display a Welcome page screen. (optional page)
2. **Session Management** -
    - **Allow users to close existing sessions when the concurrent session limit is exceeded** - Check to allow users to close existing sessions when the concurrent session limit is exceeded.
  3. **WiFi Marketing Integration** -
    - Support for 3rd party Wi-Fi based marketing notification services. Wi-Fi Based marketing notification services enables merchants to push promotions and other related notifications to customers in their close proximity
  4. Now enter your **Logout Options** for the user :-
    - **Enable Logout Button** - Check to enable a logout button.
    - **Enable Logout Pop-up Window** - Check to enable a pop-up window to logout.

All text on these screens and all Portals can be amended if necessary in **Guest Portals --> Portals** and by clicking on the Edit icon.

5. Click on **Next** to continue.
6. Depending on what options you selected in the **Portal Pages** section above, you will be presented with some or all of the following screens.

**Portal Setup Wizard**

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ★ **Portal Settings**
- Portal Policy

### Remember User on Device

When configured the user login will be remembered for this device. If the user reconnects to the open network they will be automatically logged in.

MAC detection requires that the controller sends the MAC address as part of initial redirection to Meru Connect. This is supported on Meru System Director 6.0 or later, other controllers may not provide this.

If a user obtains access via "Access without Login" page the user will only be remembered if "Remember credentials" is set to "Always".

Remember credentials:  ▾

Remember for:  Days ▾

Remember a user by:

- Storing encrypted credentials on a cookie in the user's browser
- Remembering the device they previously logged in with (detected via the MAC address)
- Initially attempt to use a cookie, if that fails try the MAC address

7. If configured, the users credentials will be remembered for this device. If the user reconnects to the open network they will automatically be logged in using these credentials. MAC detection requires that the controller sends the MAC address as part of initial redirection to FortiConnect. This is supported on Fortinet System Director 6.0 or later, other controllers may not provide this. If a user obtains access via "Access without Login" page the user will only be remembered if "Remember credentials" is set to "Always".
8. **Remember Credentials** - From the drop down menu select if and how the credentials are stored
9. **Remember for** - Select how long you wish the credentials to stored for.
10. **Remember a user by** - How you wish a user to remembered
11. Click on **Next** once you have selected all your options.

**Portal Setup Wizard**

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ★ **Portal Settings**
- Portal Policy

### Account Options

The following options define what should happen after an account either guest or device is created.

- Auto login — If this option is selected the user will be presented with a login button that will allow them to authenticate without having to type in the new account credentials.
- Display account details - If this option is selected the new account credentials will be displayed on the screen.
- Send account details via SMS - If this options is selected the new account credentials will be sent to the user's mobile phone.
- Send account details via e-mail - If this options is selected the new account credentials will be sent to the user's e-mail address.
- Send purchase receipt by e-mail - If this options is selected a receipt for purchased account will be sent to the user's e-mail address.

Auto Login:

Display account details:

Send account details by SMS:

Send account details by e-mail:

Send purchase receipt by e-mail:

---

#### Self Service Account Verification Options

No verification required:

Use event codes:

Use sponsor approval:

---

#### Device Registration Verification Options

Use sponsor approval:

---

#### Smart Connect Options

Smart Connect language template:

12. Define what should happen after the account has been created :-

- **Auto Login** - Select so the user will be presented with a login button that will allow them to authenticate without having to type in the new account credentials.
- **Display Account Details** - Select to display the new account details on screen.
- **Send Account Details by SMS** - Select to send the new account details to the users mobile phone.
- **Send Account Details by e-mail** - Select to send the new account details to the users e-mail address.
- **Send Purchase Receipt by e-mail** - If this option is selected a receipt for a purchased account will be sent to the users e-mail address.

13. Under the **Self Service Account Verification Options**, select :-

- **Use Event Codes** - If enabled the user will be required to provide a valid event code for an account to be generated.
- **Use Sponsor Approval** - Select so that a sponsor must approve the account before it is activated.

14. Under the **Device Registration Verification Options**, select :-

- **Use Sponsor Approval** - Select so that a sponsor must approve the account before it is

activated.

15. Under the **Smart Connect Options**, select :-

- **Smart Connect Language Template** - From the drop down menu select the language to be used by the Smart Connect Apps.

16. Click on **Next** once you have selected all your options.

The screenshot shows the 'Portal Setup Wizard' interface. On the left is a navigation pane with 'Portal Settings' selected. The main area is titled 'Sponsor Approval Options' and contains a list of seven options with checkboxes and a text input field. The 'E-mail sponsor on approval time out' option is checked. At the bottom right are three buttons: '< Back', 'Next >', and 'Exit'.

**Portal Setup Wizard**

✓ Welcome  
✓ Portal Name  
✓ Portal Theme  
★ **Portal Settings**  
Portal Policy

### Sponsor Approval Options

The following options define what should happen when a guest account needs approval by a sponsor .

- Send notification to guest when account is rejected — When enabled guests will receive an e-mail and/or SMS message letting them know their account requests have been rejected.
- Verify sponsor e-mail - If this option is enabled the e-mail address entered by the guest will be validated against the internal sponsor database and authentication servers.
- E-mail sponsor on approval time out - If this is enabled, an e-mail message will be sent to a designated e-mail address after the defined time out period.
- Sponsor e-mail - The e-mail address of the sponsor in charge of dealing with guest accounts waiting for approval.
- Approval times out in - The time window sponsors have to approve or reject the account before a notification e-mail is sent to the designated sponsor.
- Send notifications until account is dealt with - If this option is enabled notification e-mails will be sent out recurrently until the account is approved, rejected or expires.

Send notification to guest when account is rejected:

Verify sponsor e-mail:

E-mail sponsor on approval time out:

Sponsor e-mail:

Approval times out in:  Hours

Send notifications until account is dealt with:

< Back   Next >   Exit

17. Define the Sponsor Approval Options, what should happen when a User account needs approval by a sponsor :-

- **Send notification to Guest when account is rejected** - When enabled Users will receive an e-mail and/or SMS message letting them know their account requests have been rejected.
- **Verify sponsor e-mail** - If this option is enabled the e-mail address entered by the User will be validated against the internal sponsor database and authentication servers.
- **E-mail sponsor on approval time out** - If this is enabled, an e-mail message will be sent to a designated e-mail address after the defined time out period.
- **Sponsor e-mail** - The e-mail address of the sponsor in charge of dealing with User accounts waiting for approval.
- **Approval times out in** - The time window sponsors have to approve or reject the account before a notification e-mail is sent to the designated sponsor.

- **Send notifications until account is dealt with** - If this option is enabled notification e-mails will be sent out recurrently until the account is approved, rejected or expires.

18. Click on **Next** once this has been complete.

The screenshot shows the 'Portal Setup Wizard' interface. On the left is a navigation sidebar with 'Portal Settings' selected. The main area is titled 'Notification Options' and contains instructions, variable definitions, and input fields for email and SMS settings. A 'Password Recovery Options' section is also visible at the bottom.

**Portal Setup Wizard**

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ★ **Portal Settings**
- Portal Policy

### Notification Options

This step allows you to set e-mail and SMS header fields.  
You should use the following variables to build the SMS destination field so it complies with your SMS gateway requirements

- %MOBILENUMBER% - The mobile number of the guest.
- %MOBILENUMBER\_ONLY% - Mobile phone number of guest without country code pre-pended.
- %COUNTRYCODE% - Country code of the mobile phone number.

E-Mail from field:

SMS from field:

SMS to field:

---

#### Password Recovery Options

Send Via:

< Back   Next >   Exit

19. Define your Notification Options, this allows you to set up e-mail and SMS header fields.

- **E-Mail from field** - Enter the E-Mail from address in this field.
- **SMS from field** - Enter the SMS from address in this field.
- **SMS to field** - Enter the SMS to address string in this field.

20. Define how FortiConnect will send out a password when **Password Recovery** has been selected, from the drop down menu, choose from -

- **Email Only**
- **SMS Only**
- **Both Email and SMS**
- **Email then if not successful via SMS**
- **SMS then if not successful via Email**

21. Click on **Next** when you have finished.

**Portal Setup Wizard**

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ★ **Portal Settings**
- Portal Policy

### Select Payment Provider

The payment provider details are needed to allow your payment provider to perform credit card billing into your account.

Select an existing payment provider or enter the details for a new account.

Payment Provider:

Account Name:

Account Description:

Payment Provider:

Operation Mode:  [<https://secure.authorize.net/gateway/transact.dll>]

API Login:

Transaction Key:

**Available Cards**

- Visa
- MasterCard
- American Express
- Diners Club
- Discover Card
- En Route
- JCB
- Carte Blanche

**Supported Cards**

**Payment Page Settings**

Show/Hide input fields on the payment page of the Guest Portal using this account.

22. Select your Payment Provider details, these are needed to allow your payment provider to perform credit card billing into your account :-

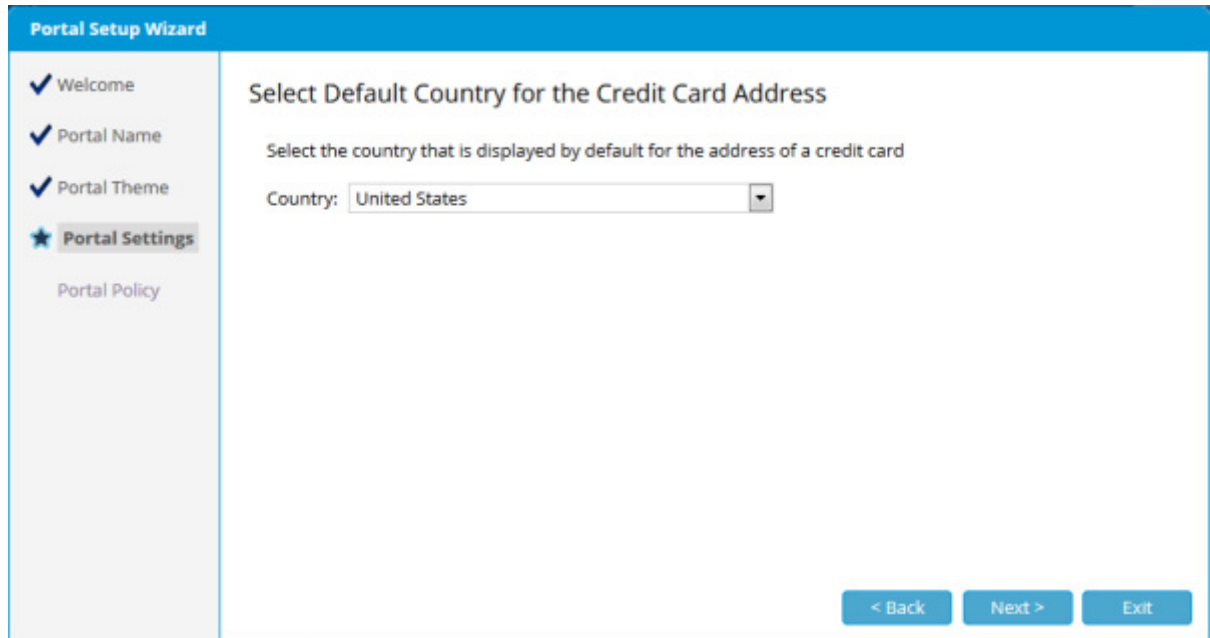
- **Payment Provider** - From the drop down menu, Configure a new payment provider, or select a pre-configured payment provider. You can click on the **Test connection** button to test a transaction by sending gateway specific details to the payment provider.
- **Account Name** - Enter a name for your account.
- **Account Description** - Enter a description for your account.
- **Payment Provider** - From the drop down menu, select a payment provider.
- **Operation Mode** - From the drop down menu choose between it being a Production or Test interface.
- **API Login** - Enter the API login details.
- **Transaction Key** - Enter the transaction key details.
- **Available Cards** - Move any supported cards from the Available Cards section to the Supported Cards section using the arrows provided.



23. 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** - Field requires input
- **Optional** - Field can be left blank
- **Unused** - Field will not appear

24. Click on **Next** once you have finished.



The screenshot displays the 'Portal Setup Wizard' interface. On the left, a sidebar lists the steps: 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings' (highlighted with a star), and 'Portal Policy'. The main content area is titled 'Select Default Country for the Credit Card Address' and includes the instruction: 'Select the country that is displayed by default for the address of a credit card'. Below this, there is a 'Country:' label followed by a dropdown menu currently set to 'United States'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

25. Select a Default Country that is displayed for the Credit Card Address :-

- **Country** - From the drop down menu select your country.

26. Click on **Next** to continue.

Portal Setup Wizard

✓ Welcome  
✓ Portal Name  
✓ Portal Theme  
★ Portal Settings  
Portal Policy

### Select PMS Provider

The Property Management System details are needed to enable room billing.  
Select an existing Property Management System or enter the details for a new account.

Property Management System:

Name:

Description:

Type:

IP Address:

Port:

< Back   Next >   End

27. Select your PMS Provider details, these are needed to enable room billing.

- **Property Management System** - From the drop down menu choose an existing Property Management System or Configure new Property Management System.

**Note:** Existing Property Management Systems can be added at Guest Portals --> Hotel PMS

- **Name** - Enter a name for the Property Management System.
- **Description** - Enter a description for the Property Management System.
- **Type** - From the drop down menu, select the type of Property Management System you will be using.
- **IP Address** - Enter the IP address of the Property Management System.
- **Port** - Enter the port number.

28. Click on **Next** to continue.

**Portal Setup Wizard**

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ★ **Portal Settings**
- Portal Policy

### Select Currency

Select which currencies this portal should use for billing credit cards and Hotel PMS systems.

Payment Gateway Currency:

PMS Currency:

< Back   Next >   Exit

29. Select which currencies the portal should use for billing credit cards and for Hotel PMS systems.
- **Payment Gateway Currency** - Select the currency for your payment gateway.
  - **PMS Currency** - Select the currency for your Property Management System.
30. Click on **Next** to continue.

**Portal Setup Wizard**

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ★ **Portal Settings**
- Portal Policy

## Access Plans

Manage the access plans users accessing this portal will be able to select.

Access plans allows you to define when and where the user will be allowed to access the network by selecting a Usage Profile and Account Group. You can also specify the cost of purchasing an account if your portal allows this through Credit Card or PMS billing.

Name	Description	Total Price	Currency	Usage Profile	Account Group	Used for
No access plans defined						

Use Access Plan for:

Name:

Description:

Usage Profile:  To define Usage Profiles go to Policy Settings -> Usage Profiles

Account Group:  To define Account Groups go to Policy Settings -> Account Groups

Pre-tax Price:

Tax:  %  
Leave blank/zero if no tax applies

Total Price:

### 31. Manage the access plans users accessing the portal will be able to select :-

- **Use Access Plan for** - From the drop down menu select whether the access plan is for Self Service users, Credit Card Billing, PMS Billing, Device Registration, Access without Login or the My Account option where users can provision their own account after login.
- **Name** - Enter the name of your plan.
- **Description** - Enter a description for your plan.
- **Usage Profile** - From the drop down menu choose from a pre-defined Usage profile. Usage profiles can be defined in Policy Settings --> Usage Profiles.
- **Account Group** - From the drop down menu choose from a pre-defined Account Group. Account Groups can be defined in Policy Settings --> Account Groups.
- **Pre-tax Price** - If your time profile is assigned to a billing plan, then enter the price of your plan, pre-tax.
- **Tax** - Enter the percentage of tax you wish to charge. Leave blank of no tax applied.
- **Total Price** - The total price of the plan will appear automatically in this field.

32. Click on **Add** to add your plan.

33. Click on **Next** to continue.

## Configuring Portal Policy

The screenshot shows the 'Portal Setup Wizard' interface. On the left, a navigation pane lists steps: Welcome, Portal Name, Portal Theme, Portal Settings, and Portal Policy (which is selected with a star). The main content area is titled 'Portal Redirect Policy' and contains the following information:

- **Acceptable Usage Policy** — Use this option to specify when should guests be shown the Acceptable usage policy.
- **Show Acceptable Usage Policy to the user** — Use this option to specify when Acceptable usage policy needs accepting by a user after authentication.
- **Initial Page** — This is the portal page guests will be taken to once they first get on the network.
- **After Authentication Redirect To** — Use this option to specify where the user should be taken to after a successful authentication.
- **First login portal success page** — Use this option to specify which portal page first time users should be taken to after authentication.
- **Subsequent login portal success page** — Use this option to specify which portal page returning users should be taken to after authentication.

Configuration fields shown in the screenshot:

- Acceptable Usage Policy: Disabled
- Show Acceptable Usage Policy to the user: Every login
- Initial Page: Login
- After Authentication Redirect To: Predefined URL
- Redirect to: http://dev.dcf.com/?id=%ID%&uname=

It's possible to use the following variables to build the redirect URL.

- %ID% - The account id number.
- %USERNAME% - The account username.
- %FIRSTNAME% - The user's first name.
- %LASTNAME% - The user's last name.
- %MACADDRESS% - The MAC address of the device from which the user is authenticating.

1. You are now presented with the Portal Redirect Policy screen, choose from the following :
  - **Acceptable Usage Policy** - From the drop down menu select whether an acceptable usage policy should be displayed **Pre-Authentication**, **Post-Authentication**, or whether it should be **Disabled**.
  - **Show Acceptable Usage Policy** - From the drop down menu select how often you wish to show the Acceptable Usage Policy, whether it be **Every Login**, **On First Login**, and **on First Login and any Subsequent Acceptable Usage Policy Changes**.
  - **Initial Page** - From the drop down menu select which portal page the Users will be taken to once they first get on the network. Your options will differ depending on the choices you made on the **Portal Pages** screen previous.
  - **After Authentication Redirect To** - From the drop down menu select as to where the Users should be directed to after a successful authentication.
    - **Portal Success Page** - Redirect to a Portal Success Page, from the drop down menu select which page you wish to use as a Portal Success Page.
    - **Predefined URL** - Redirect users to a predefined URL once they authenticate successfully. You can pass certain properties of the User as GET requests of the redirect. To do this, construct the URL using the following placeholders:
      - %ID% - placeholder for the MCT internal id of the authenticated account
      - %USERNAME% - placeholder for the username of the authenticated account

- %FIRSTNAME% - placeholder for the first name of the authenticated account
- "%LASTNAME% - placeholder for the last name for the authenticated account
- %MACADDRESS% - placeholder for the MAC address of the device of the authenticated account

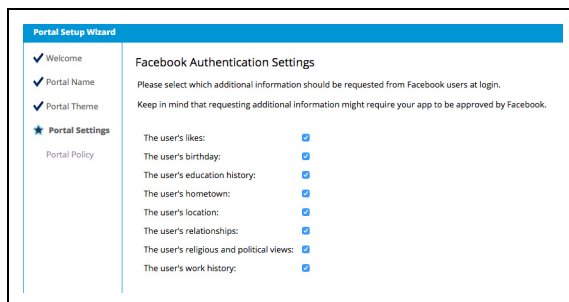
For example if the customer website is at <http://example.com> and you need info the username of the authenticated user, you configure redirect URL like <http://mywebsite.com?username=%USERNAME%> it would then be up to the customer website to parse and use that information as required.

2. If on the **Portal Pages setup** screen you chose to display a **Welcome Back** page after authentication you will see a set of different options to define landing pages as shown below.
3. The option to land at a subsequent portal page if the user is recognized can now be defined -
  - **First login portal success page** - From the drop down menu select what portal success page a user should land on after first login.
  - **Subsequent login portal success page** - From the drop down menu select which portal success page a user should land on upon their return.
4. Click on **Next** to continue.

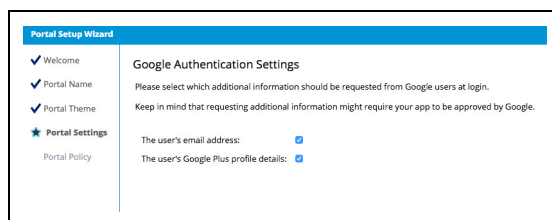
5. Now you can select which realms should be displayed to the User on the login page, the realms are defined on the external Users page **Policy Settings --> Account Groups** and are used to authenticate Users against different external servers for a realm.

6. **Portal External Authentication Policy** - If you use OAuth using any of the social login (Facebook, Twitter, and Google), you can specify what social profile information you wish to capture on the MCT database when a user authenticates. This is done through the Guest Portal wizard, new portal stages are displayed when Facebook or Google authentication is enabled for the portal, Twitter does not allow extra user information to be gathered and as such this feature does not apply to it.

On the wizard stage for the different services its possible to select different categories of information, these depend on the service used, you will notice there are more options for Facebook when compared to Google.



The screenshot shows the 'Portal Setup Wizard' interface for Facebook authentication. The left sidebar contains a navigation menu with 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings' (selected), and 'Portal Policy'. The main content area is titled 'Facebook Authentication Settings' and includes a sub-header 'Please select which additional information should be requested from Facebook users at login.' Below this, a note states: 'Keep in mind that requesting additional information might require your app to be approved by Facebook.' A list of information categories follows, each with a checked checkbox: 'The user's likes', 'The user's birthday', 'The user's education history', 'The user's hometown', 'The user's location', 'The user's relationships', 'The user's religious and political views', and 'The user's work history'.



The screenshot shows the 'Portal Setup Wizard' interface for Google authentication. The left sidebar contains a navigation menu with 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings' (selected), and 'Portal Policy'. The main content area is titled 'Google Authentication Settings' and includes a sub-header 'Please select which additional information should be requested from Google users at login.' Below this, a note states: 'Keep in mind that requesting additional information might require your app to be approved by Google.' A list of information categories follows, each with a checked checkbox: 'The user's email address' and 'The user's Google Plus profile details'.

When available the user information will be recorded on the MCT database, it will not be visible through any Sponsor/Admin portal reports. The only way to access this information is through the MCT Sponsor API, Any API call that returns account objects will include a <socialProfile> XML element containing the available information for that account.

**Note:** Only the information authorized by the social app can be collected. In some cases, depending on the type of information this will require the OAuth app to be approved by the OAuth provider, this is outside the scope of the MCT documentation. Also the user has ultimate control over what he/she shares with MCT, if the user refuses to share information MCT will not get access to it.

To enable OAuth in FortiConnect with Fortigate, ensure that you whitelist the following OAuth service provider URLs in the Fortigate Server:

### Facebook

```
config firewall address
edit "FB0"
set subnet 5.178.32.0 255.255.240.0
next
edit "FB1"
```

```
set subnet 195.27.154.0 255.255.255.0
next
edit "FB2"
set subnet 80.150.154.0 255.255.255.0
next
edit "FB3"
set subnet 77.67.96.0 255.255.252.0
next
edit "FB4"
set subnet 212.119.27.0 255.255.255.128
next
edit "FB5"
set subnet 2.16.0.0 255.248.0.0
next
edit "FB6"
set subnet 66.171.231.0 255.255.255.0
next
edit "FB7"
set subnet 31.13.24.0 255.255.248.0
next
edit "FB8"
set subnet 31.13.64.0 255.255.192.0
next
edit "FB9"
set subnet 23.67.246.0 255.255.255.0
next
edit "akamai-subnet-23.74.8"
set subnet 23.74.8.0 255.255.255.0
next
edit "akamai-subnet-23.74.9"
set subnet 23.74.9.0 255.255.255.0
```



```
next
edit
"akamaihd.net"
set type fqdn
set fqdn "akamaihd.net"
next
edit "channel-proxy-06-frcl.facebook.com"
set type fqdn
set fqdn "channel-proxy-06-frcl.facebook.com"
next
edit "code.jquery.com"
set type fqdn
set fqdn "code.jquery.com"
next
edit "connect.facebook.com"
set type fqdn
set fqdn "connect.facebook.com"
next
edit "fbcdn-photos-c-a.akamaihd.net"
set type fqdn
set fqdn "fbcdn-photos-c-a.akamaihd.net"
next
edit "fbcdn-profile-a.akamaihd.net"
set type fqdn
set fqdn "fbcdn-profile-a.akamaihd.net"
next
edit "fbexternal-a.akamaihd.net"
set type fqdn
set fqdn "fbexternal-a.akamaihd.net"
next
edit "fbstatic-a.akamaihd.net"
```

```
set type fqdn
set fqdn "fbstatic-a.akamaihd.net"
next
edit "m.facebook.com"
set type fqdn
set fqdn "m.facebook.com"
next
edit "ogp.me"
set type fqdn
set fqdn "ogp.me"
next
edit "s-static.ak.facebook.com"
set type fqdn
set fqdn "s-static.ak.facebook.com"
next
edit "static.ak.facebook.com"
set type fqdn
set fqdn "static.ak.facebook.com"
next
edit "static.ak.fbcdn.com"
set type fqdn
set fqdn "static.ak.fbcdn.com"
next
edit "web_ext_addr_SocialWiFi"
set type fqdn
set fqdn "web_ext_addr_SocialWiFi"
next
edit "www.facebook.com"
set type fqdn
set fqdn "www.facebook.com"
next
```

end

## Google+

config firewall address

edit "www.googleapis.com"

set type fqdn

set fqdn "www.googleapis.com"

next

edit "accounts.google.com"

set type fqdn

set fqdn "accounts.google.com"

next

edit "ssl.gstatic.com"

set type fqdn

set fqdn "ssl.gstatic.com"

next

edit "fonts.gstatic.com"

set type fqdn

set fqdn "fonts.gstatic.com"

next

edit "www.gstatic.com"

set type fqdn

set fqdn "www.gstatic.com"

next

edit "Google\_13"

set subnet 216.58.192.0 255.255.224.0

Accounts.google.com is too dynamic for an FQDN policy to function.

This IP policy covers the whole range of possible subnets.

next

end

## Twitter

```
config firewall address
edit "api.twitter.com"
set type fqdn
set fqdn "api.twitter.com"
next
edit "abs.twimg.com"
set type fqdn
set fqdn "abs.twimg.com"
next
edit "abs-0.twimg.com"
set type fqdn
set fqdn "abs-0.twimg.com"
next
end
```

7. **Manual Selection** - Select this mode for the user to select an appropriate realm from the 'selected realms' list.
8. **Automatic Selection** - Select this mode so that each realm is selected in order from the list rather than asking the user to select one. The realm selection starts from the top of the order first and if authentication fails the next realm in the order is tried and so on.
9. 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 above.

**Note:** If **Automatic Selection** is selected then internet services such as Google, Facebook and Twitter will always be checked last.

10. Click on **Next** to continue.

11. In the **Portal Restrictions** page, you can set the time interval that Prevents the creation of self-service accounts with the same personal details (email/phone) for a specified period of time post the original account creation.

### Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ✓ Portal Settings
- ★ **Portal Policy**

## Portal Restrictions

Please configure the account re-creation restrictions.

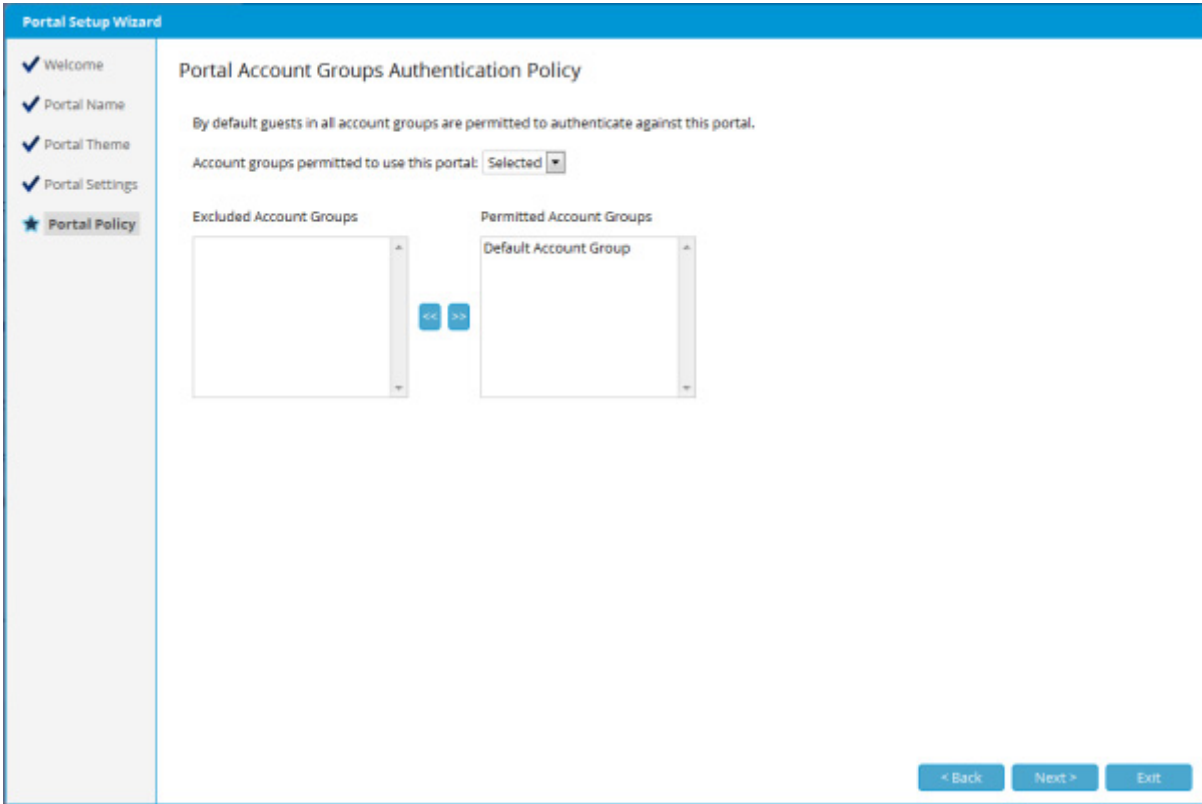
If unrestricted users will be able to create new accounts as expires.

Restriction Length:

Set to 0 for unrestricted account creation.

Restriction Type:

12. Click on **Next** to continue.



13. We can now control which account groups can authenticate against a particular portal (User/device accounts belong to account groups). This is done on the **Portal Account Groups Authentication Policy** screen. The default behaviour is to permit **All** account groups.
14. From the drop down menu you choose between **All** or **Selected**.
15. If you have chosen to select account groups, use the arrows to place the selected account groups into the **Permitted Account Groups** section.

**Portal Setup Wizard**

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ✓ Portal Settings
- ★ **Portal Policy**

### Guest Username Policy

The following options allow you to specify how the usernames for the guest accounts created through this portal should be generated.

- Email address as username — The guest e-mail address will be used as the username for the account.
- Create username based on first and last names — The guest's first and last names will be combined to generate the account username.
- Create random username — The username for the account will be randomly generated.
- Username Prefix — This will be used as prefix to generate the account username.

Username Prefix:   
All generated usernames will be prefixed with this text.

---

**Email address as username**

Email address as username

Create Username With Case:

Enforce unique email:

---

**Create username based on first and last names**

Create username based on first and last names

Minimum username length:

Create Username With Case:

Create Username With Separator:

---

**Create random username**

Create random username

Alphabetic characters to include:

Number to include:

16. Now you can select and choose your site policy, choose how usernames for User accounts for the Portal should be generated.

- **Email address as username** - The User e-mail address will be used as the username for the account.
- **Create usernames based on first and last name** - The Users first name and last names will be combined to generate the account username.
- **Create random username** - The username for the account will be randomly created.
- **Username Prefix** - This will be used as a prefix to generate the account username.

17. Click on Next to continue

**Portal Setup Wizard**

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ✓ Portal Settings
- ★ **Portal Policy**

### Guest Password Policy

By modifying the following options you can define which characters will be used when generating account passwords and how long the password should be.

**Password generation mode**

Auto generated password  
 Guest specified password

---

**Password requirements**

Characters to include:   
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

Password case:

Number to include:

Characters to include:   
0123456789

Number to include:

Characters to include:   
!\$%^&\*\_+[]{}|:~@#-.,<>?

Number to include:

- Choose whether you want the passwords to be -
  - Auto generated password** - password is generated using conditions below
  - Guest specified password** - password is specified by the user creating the account
- Choose how passwords for User accounts for the User Portal should be generated.
  - Alphabetic Characters** - Decide the number of characters to use.
  - Numeric Characters** - Decide the number of characters to use.
  - Other Characters** - Decide the number of characters to use.
- Click on **Next** to continue.



Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ✓ Portal Settings
- ★ Portal Policy

### Guest Account Details

**Standard Fields**

First Name: Required ▾

Last Name: Required ▾

Company: Unused ▾

Email: Required ▾  
This cannot be changed as email address is being used as the username in Username Policy

Mobile: Unused ▾

---

**Additional Fields**

Option 1: Unused ▾

Option 2: Unused ▾

Option 3: Unused ▾

Option 4: Unused ▾

Option 5: Unused ▾

< Back   Next >   Exit

**21. Select which fields should be used to capture User Account Details :-**

- **First Name** - From the drop down menu decide whether this field is Required, Unused or Optional.
- **Last Name** - From the drop down menu decide whether this field is Required, Unused or Optional.
- **Company** - From the drop down menu decide whether this field is Required, Unused or Optional.
- **Email** - From the drop down menu decide whether this field is Required, Unused or Optional.
- **Mobile** - From the drop down menu decide whether this field is Required, Unused or Optional.
- **Additional Fields** - From the drop down menu decide whether this field is Required, Unused or Optional.

**22. Click on Next to continue.**

Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ✓ Portal Settings
- ★ Portal Policy

### Purchase Guest Account Details

Additional fields can be added to your Purchase Account page.

Option 1:  ▾

Option 2:  ▾

Option 3:  ▾

Option 4:  ▾

Option 5:  ▾

< Back   Next >   Exit

- 23.** Select how many fields should be used to capture additional information for Purchased Accounts:-
- **Option 1** - From the drop down menu decide whether this field is Required, Unused or Optional.
  - **Option 2**- From the drop down menu decide whether this field is Required, Unused or Optional.
  - **Option 3** - From the drop down menu decide whether this field is Required, Unused or Optional.
  - **Option 4** - From the drop down menu decide whether this field is Required, Unused or Optional.
  - **Option 5** - From the drop down menu decide whether this field is Required, Unused or Optional.
- 24.** Click on **Next** to continue.

The screenshot shows a 'Portal Setup Wizard' window with a blue header. On the left is a vertical sidebar with a list of steps, each preceded by a checkmark: 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings', and 'Portal Policy'. The main content area is titled 'Portal Setup Complete' and contains the following text: 'The wizard has finished building your portal.'; 'You can preview the portal at <https://192.168.137.20/portal/portaltwo/preview/?show>'; 'You should configure your network devices to redirect to the following URL: **https://{MERU\_CONNECT}/portal/portaltwo/{DEVICE\_IP}**'; 'Please replace {MERU\_CONNECT} with the fully qualified domain name of the Meru Connect and {DEVICE\_IP} with the IP address of the network device (wireless controller, switch, firewall etc) you have added as a RADIUS client.'; 'You must also ensure the following conditions are met:'; and a numbered list: '1. The fully qualified domain name of the Meru Connect should be in DNS and resolvable by guest clients so they can reach the Meru Connect.' and '2. The SSL certificate CN should contain the fully qualified domain name of the Meru Connect and be signed by a trusted CA authority to ensure clients do not receive SSL warnings.' At the bottom right of the window are two buttons: '< Back' and 'Close'.

The Portal setup is now complete. Click on **Close** to finish.

## Guest Portal Operations

---












### Previewing a Portal

You can preview a Portal once its been setup.

1. From the Administration interface go to **Guest Portals --> Portals** as shown below.

## Portals

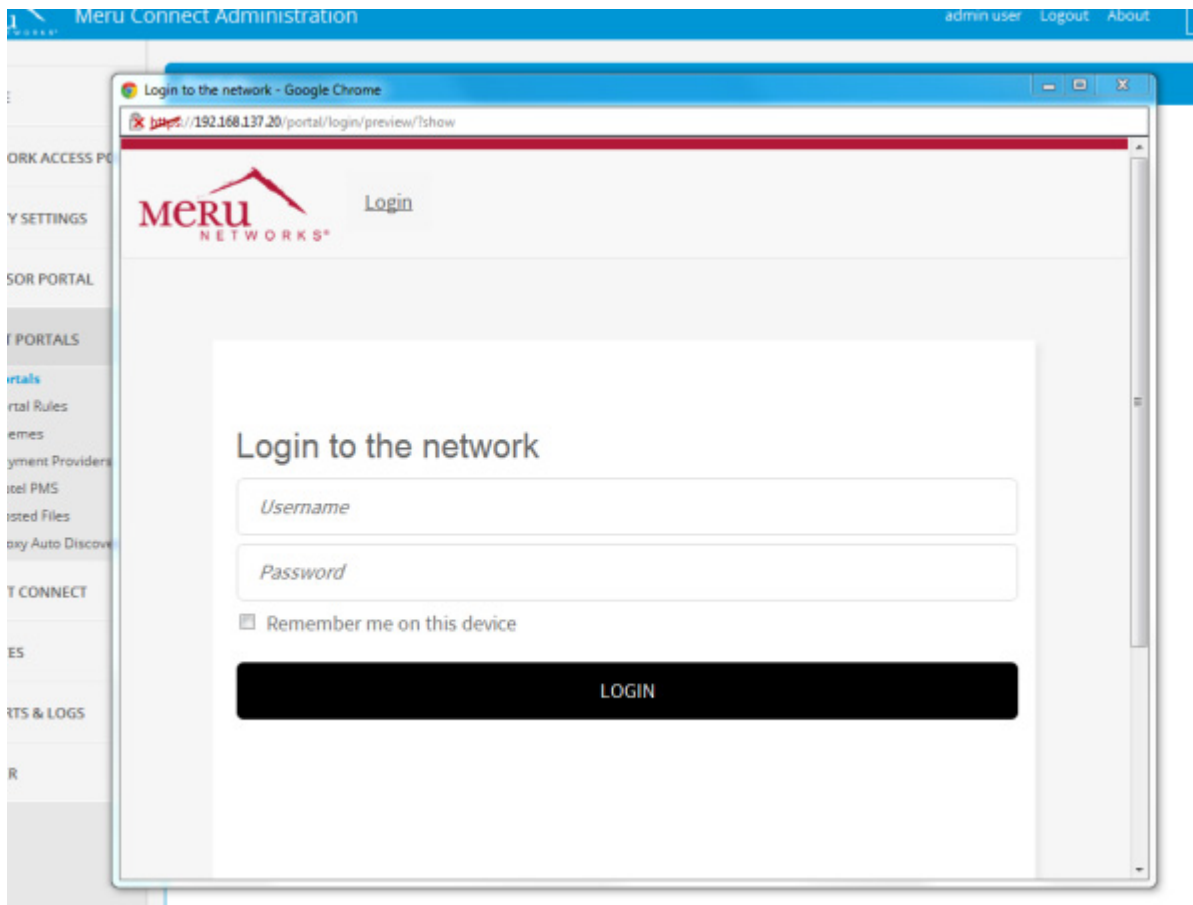
Showing 1-3 of 3 10 per page Go

Name	Description	
<a href="#">access-denied</a>	Default portal that denies access	   
<a href="#">login</a>	Default login portal	   
<a href="#">PortalOne</a>	Portal Number One	  

Page 1 of 1 Go

Add Portal

2. Select the Portal you wish to preview by clicking on the **Preview** Icon next to the Description field.
3. The Portal you have created should then appear as shown below.












## Editing a Portal

Once a Portal has been created, you can edit and customize the content of the Portal, go to **Guest Portals --> Portals**

## Portals

Showing 1-3 of 3 10 per page Go

Name	Description	
<a href="#">access-denied</a>	Default portal that denies access	  
<a href="#">login</a>	Default login portal	  
<a href="#">PortalOne</a>	Portal Number One	  

Page 1 of 1 Go

Add Portal

1. Choose the portal you wish to edit of its content and click on the **edit content** icon.

**Widget Labels**

Please change the text shown on forms and components in the portal.

Default Phone Code: +1

Username: Username

Password: Password

Confirm Password: Confirm Password

Remember me on this device: Remember me on this device

Realm: Realm

Login button: Login

Access without Login button: Connect

Days: Days(s)

Hours: Hour(s)

Minutes: Minute(s)

Time left text: Your account will expire in:

Time left calculating: Calculating...

Time left Unlimited account text: Your account is unlimited

Try again: Try again

New password: New Password

Old Password:

2. On the left hand side of the screen you can see all the different pages/options that have been created when the portal was set up using the **Portal Wizard**. Click on the page/option tab that you wish to edit, for the example above we have selected the **LoginPage**. You can amend any text within the box and insert your own.
3. Click **Save** once you have amended/added any text.
4. Continue to edit another page/option by clicking on the relevant tab.

## Deleting a Portal

You can delete an existing Portal Site from the administration interface.

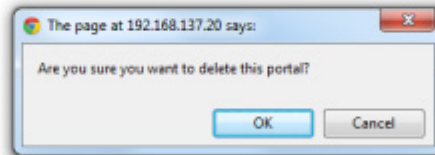
1. From the administration interface, select **Guest Portals --> Portals** as shown below.

Showing 1-3 of 3 10 per page Go

Name	Description	
<a href="#">access-denied</a>	Default portal that denies access	🔍 ⚙️ 📄 🗑️
<a href="#">login</a>	Default login portal	🔍 ⚙️ 📄 🗑️
<a href="#">PortalOne</a>	Portal Number One	🔍 ⚙️ 🗑️

Page 1 of 1 Go

Add Portal



2. Select the portal you wish to delete and click on the **Bin** icon next the descriptions field.
3. Click **Yes** to confirm deletion.

## Copying a Portal












Administrators can copy Portals that have already been created to save time going through the setup wizard if a duplicate portal is needed.

From the Administration interface go to **Guest Portals** --> **Portals** as shown below.



## Portals

Showing 1-3 of 3 10 per page Go

Name	Description	
<a href="#">access-denied</a>	Default portal that denies access	   
<a href="#">login</a>	Default login portal	   
<a href="#">PortalOne</a>	Portal Number One	  

Page 1 of 1 Go

Add Portal

Click on the **Copy Portal** icon next to the portal that you have created

## Copy Portal: login

New Portal Name:

Copy

Cancel

Enter your **New Portal Name** and then click on the **Copy** button, your portal will have been copied as shown below

Portals

✓ Portal copied successfully

Showing 1-4 of 4 10 per page Go

Name	Description	
<a href="#">access-denied</a>	Default portal that denies access	🔍 📄 🗑️
<a href="#">CopiedPortal</a>	Default login portal	🔍 📄 🗑️
<a href="#">login</a>	Default login portal	🔍 📄 🗑️
<a href="#">PortalOne</a>	Portal Number One	🔍 📄 🗑️

Page 1 of 1 Go

Add Portal

## Custom Portal

---

In this chapter we take a look at how to Create a Portal Theme

- The Sample Theme
  - The style.css file
  - The theme.xml file
    - Ⓢ Name
    - Ⓢ Description
    - Ⓢ Author
    - Ⓢ Preview
    - Ⓢ Pages
    - Ⓢ Images
    - Ⓢ Colours
- Creating a Custom Theme
- Installing a Theme

- Available Widgets

## Default Themes

You can download any of the existing default themes that the FortiConnect provides to view its structure.

Log into the web admin user interface of the FortiConnect and browse to **Guest Portals-->Themes** and click on the export button next to 'The Default Fortinet Theme' as show below.

The screenshot displays the 'Themes' management page in the FortiConnect web interface. At the top, there's a blue header with the word 'Themes'. Below it, a table lists available themes. The table has three columns: 'Name', 'Description', and a set of icons for editing and deleting. The themes listed are: 'Access Denied', 'Identity Networks (Blue)', 'Mobile Theme (All Devices)', 'Identity Networks (white)', 'Meru Networks (Responsive Theme)', 'Meru Networks (white)', and 'White Mobile Theme (All Devices)'. Below the table, there's a pagination control showing 'Page 1 of 1'. Underneath the table, there's an 'Import Theme' section with a 'Choose File' button and an 'Import' button.

Name	Description	
Access Denied	This theme only displays an access denied message. It is based on the Meru Networks white theme.	
Identity Networks (Blue)	The default Identity Networks theme.	
Mobile Theme (All Devices)	This theme is for mobile devices.	
Identity Networks (white)	Theme based on the Identity Networks color scheme and logo	
Meru Networks (Responsive Theme)	Responsive theme based on the Meru Networks color scheme and logo	
Meru Networks (white)	Theme based on the Meru Networks color scheme and logo	
White Mobile Theme (All Devices)	This theme is for mobile devices.	

Import Theme:  No file chosen

Unzip the default.zip file and confirm you have the following files :

- css/
  - style.css
- html/
  - °aup.html
  - login.html
  - password.html
  - payment.html
  - selfservice.html
  - success.html
  - logout.html
  - loggedOut.html
- images/

- theme.xml

## The style.css file

This file should be placed in the css directory of the theme structure and should contain all the CSS styles that will be applied to the several HTML pages that make up the Portal site.

## The theme.xml file

The theme.xml file list all resources used by the theme as well as defining the default values for several elements.

The file has 10 main elements:

1. Name
2. Public name
3. Description
4. Author
5. Preview
6. Pages
7. Optional pages
8. Navigation
9. Images
10. Colours
11. Scripts

### Name

This is a mandatory element, it should only contain letters, digits and the underscore symbol, theme names are unique so if there is already a theme with this name installed on the FortiConnect you won't be able to 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 name element.

If the publicName element is not present the theme internal name will be displayed.

### Author

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

### Preview

This attribute has two elements:

- small
- large

Both should have the name of two image files containing thumbnails for the theme, these are used by the hotspot setup pages to give the administrator an idea of how the hotspot will look if he chooses the theme. The recommended size for the small thumbnail is 200 pixels wide by 115 pixels tall and for the large thumbnail 800 pixels wide by 455 pixels tall. The files should be placed at the same level as the theme.xml file.

## Pages

In the pages section of the theme.xml file you will 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.

A simple example would be:

```
<pages>
<login>
<file>login.html</file>
<components>
<component>
<tag>%TITLE%</tag>
<default>Login to the network</default>
</component>
<component>
<tag>%HEADER%</tag>
<default>Login to the network</default>
</component>
<component>
<tag>%MAIN%</tag>
<default/>
</component>
<component>
<tag>%FOOTER%</tag>
<default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
</component>
```

```

</components>
<label>Login</label>
</login>
</pages>

```

The previous XML snippet tells us the HTML template for the login page is located at html/login.html, and on this page we have defined four components that the administrator users can customize with their content, we have also declared the default content for each component:

**Table 1:**

Component	Default Value
Title	Login to the network
Header	Login to the network
Main	
Footer	copyright © yourcompany 2010

If we open the login.html file with a text editor we can see where these components are used:

```

<h1>%HEADER%</h1>
<div class="main">%MAIN%</div>
<div class="widgetContainer">%LOGIN_WIDGET%</div>
<div id="navigation">%NAVIGATION_MENU%</div>
<div id="footer">%FOOTER%</div>

```

As we can see on the HTML the placeholder variables for the several components defined in theme.xml are placed amongst the markup, when the portal pages are generated the placeholders will be replaced with the content associated with them.

We can also see a few placeholders that weren't specified in the theme.xml file, these are:

- **%LOGIN\_WIDGET%** - this will be replaced with the login widget if we were looking at the self service page template we should use **%SELF\_SERVICE\_WIDGET%** you can find a list of available widgets at the of this chapter.
- **%NAVIGATION\_MENU%** - this will be replaced with a set of links to other pages available to users of the Portal.

The content of these placeholders is built dynamically by the FortiConnect 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.

## Navigation

Users can now add links to portal pages, to do this they have to add the following html:

```
<a %TAG%>this is a link</a>
```

%TAG% can be one of the following:

- %LINK\_TO\_LOGIN% - Link to the login page
- %LINK\_TO\_PMS% - Link to the pms login page
- %LINK\_TO\_PAYMENT% - Link to the Credit card payment page
- %LINK\_TO\_SELFSERVICE% - Link to the self service page
- %LINK\_TO\_PASSWORD% - Link to the password change page
- %LINK\_TO\_CLIENTCONFIGURATION% - Link to the smart connect page
- %LINK\_TO\_SUCCESS% - Link to the successful authentication page, this link will only work after successful authentication

To link to a optional page you should have a tag similar to

```
%LINK_TO_OPTIONAL_[PAGENAME]%
```

Where page name matches the name you gave the page on the theme.xml file so if in that file you have a generic page defined like:

```
<optionalPage menuItemWeight="10000">  
<file>help.html</file>  
<components>  
<component>  
<tag>%TITLE%</tag>  
<default>Your title here</default>  
</component>  
<component>  
<tag>%HEADER%</tag>  
<default/>  
</component>  
<component>  
<tag>%MAIN%</tag>  
<default>Your content here</default>
```

```
</component>
<component>
<tag>%FOOTER%</tag>
<default><![CDATA[ &copy; 2020 Fortinet. All Rights Reserved.]]></default>
</component>
</components>
<label>Help</label>
<name>help</name>
</optionalPage>
Your tag should be %LINK_TO_OPTIONAL_HELP%
```

## Images

The images section of the theme.xml file should be used to list all image files that are referenced by the HTML and CSS for the theme.

When you open theme.xml and scroll down to the <images> section you will notice it is empty, you can add an image by replacing the <images/> tag with the following:

```
<images>
<image>
<label>Header image</label>
<description>Image placed on the header of the page</description>
<tag>%IMG_LOGO%</tag>
<file>Logo.png</file>
<dimensions>100x100</dimensions>
</image>
</images>
```

This snippet specifies the label, description and recommended dimensions for the image this information will be 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 will be used in HTML and CSS template files to reference this

particular image, the <file> element specifies which file is the default value for this image, this file should be placed in images/Logo.png.

To use this image in the login HTML template we could change the HTML to:

```
<div id="headerImage"></div>
<h1>%HEADER%</h1>
<div class="main">%MAIN%</div>
```



```
<div class="widgetContainer">%LOGIN_WIDGET%/div>
```

```
<div id="navigation">%NAVIGATION_MENU%/div>
```

```
<div id="footer">%FOOTER%/div>
```

If we wanted to reference this image on our CSS file, lets say as a background image we would have code like this:

```
.cssClass {  
background-image:url('%IMG_LOGO%');  
}
```

## Colors

The colours section should contain a list of all customizable colours used in the theme.

The default theme already has a set of colours defined, to add a new one we would insert the following snippet between the `<colour></colour>` tags:

```
<colour>  
  
<label>Default font colour</label>  
  
<description/>  
  
<tag>%CL_DEFAULT_FONT_COLOUR%/tag>  
  
<value>#001844</value>  
  
</colour>
```

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

To use this colour in CSS we should have code like the following:

```
.cssClass {  
color:%CL_DEFAULT_FONT_COLOUR%;  
}
```

## Scripts

The script section should contain a list of all javascript files you wish to use.

The default theme does not use any custom javascript files, to add a new javascript file we would insert the following snippet in the theme.xml file:

```
<scripts>  
  
<script>
```

```
<tag>%JS_UTILS%</tag>
<value>utils.js</value>

</script>

</scripts>
```

The `<tag>` element specifies what placeholder variable will be used in HTML to reference this file, the `<value>` element specifies the file name, the file should be placed in the "js" directory at the root of the theme package. To include the code in `utils.js` on the html template files we should have code like the following:

```
<script type="text/javascript" src="%JS_UTILS%"></script>
```

## Creating a Custom Theme

Now that we know what are the building blocks of a Portal theme we can use the default theme we downloaded to create our own theme.

Lets start by defining the requirements for our pages:

- Layout - Content displayed on the middle of the page, with three main areas that will be customizable by the administrator.
- Images - We will use two images one will be displayed on the page header and the other will be the favicon displayed on the browser address bar.
- Colours - We will define a background colour for the page and a different background colour for the main content area.

Start by editing the `login.html` template and modifying the HTML to suit your needs, in our case we should have something similar to:

```
<div id="content">

  <div id="header">

    <div id="headerImage"></div>

    <h1 class="pageTitle">%HEADER%</h1>

  </div>

  <div id="main">

    <div class="mainContent">%MAIN%</div>

    <div class="widgetContainer">%LOGIN_WIDGET%</div>

  </div>

  <div id="footer">

    <div id="navigation">%NAVIGATION_MENU%</div>
```

```
<div class="copyright">%FOOTER%</div>
```

```
</div>
```

```
</div>
```

You will need to copy any image files to the images/ directory.

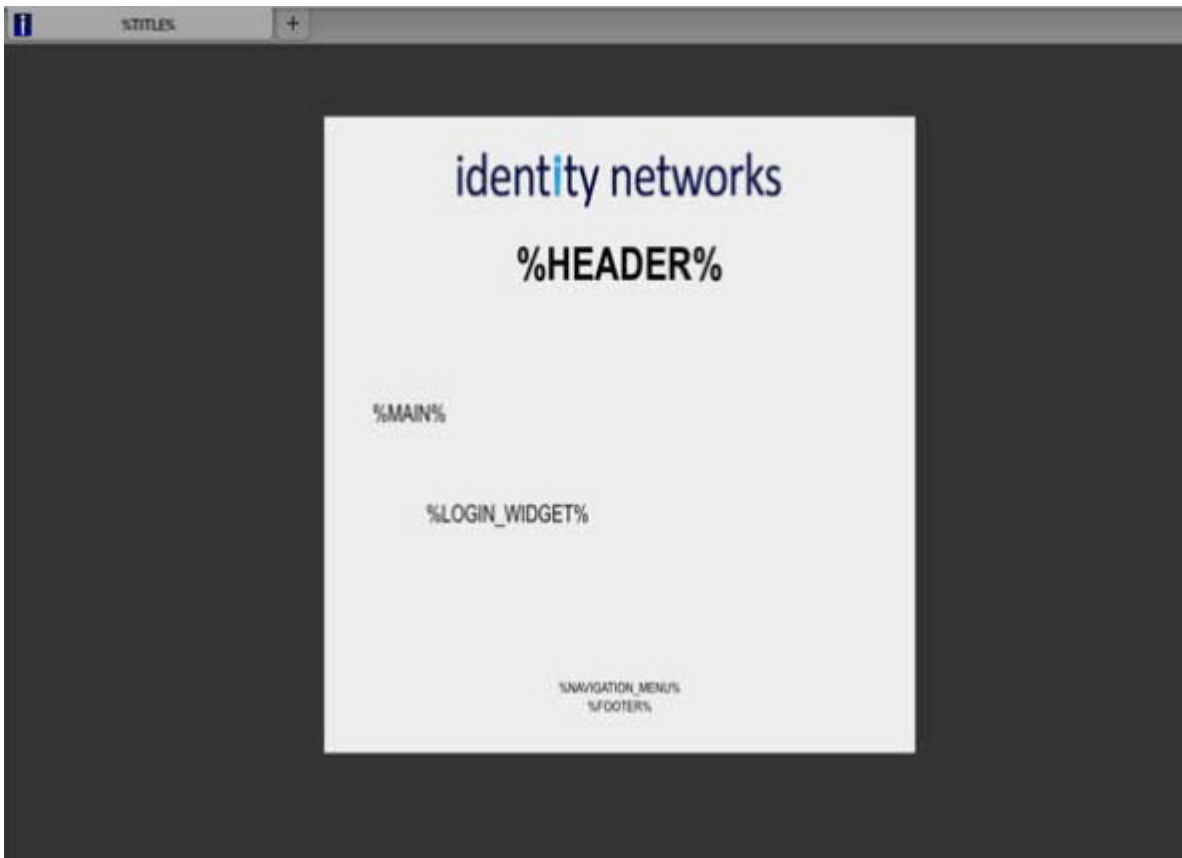
The next step will be to edit the css/style.css file and define the styles that we will apply to the HTML markup we defined previously. The following code would implement the layout we proposed:

```
body{
    font-family:Arial;
    background-color:#333333;
}
#content{d width:45%;
    margin:auto;
    padding:20px;
    margin-top:50px;
    background-color:#eeeeee;
}
#header{
    text-align:center;
    margin-bottom:25px;
    padding:5px;
}
#main{
    padding:25px;
}
.widgetContainer {
    width:80%;
    padding:50px; }
#footer{
    text-align:center;
    margin-top:25px;
```

```
padding:5px;
font-size:x-small;
}
.navigation{
padding:5px;
}
```

Again you will notice that the actual colour values are used in this file instead of placeholders, this allows us to view the page in the browser while we develop the design of our pages.

If you open the login.html file in your browser you will see something like:



You can also replace the placeholders visible on the body of the page with dummy content to get a better feel of how it would look on your page, this is also useful to take preview screenshots to include in your theme package.

Once you are happy with the layout, its time to update the theme.xml, so all elements that are customizable by the administrator are declared, in our case the file would look similar to:

```
<?xml version="1.0"?>
```

```
<hotspotTheme>
  <name>sample_theme</name>
  <description>plain theme</description>d<author></author>d  <preview>d
    <small>thumb.png</small>d  <large>preview.png</large>d </preview>
</pages>
  <login>
    <file>login.html</file>
    <components>
      <component>
        <tag>%TITLE%</tag>
        <default>Login to the network</default>
      </component>
      <component>
        <tag>%HEADER%</tag>
        <default>Login to the network</default>
      </component>
      <component>
        <tag>%MAIN%</tag>
        <default/>
      </component>
      <component>
        <tag>%FOOTER%</tag>
        <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
      </component>
    </components>
    <label>Login</label>
  </login>
  <selfService>
    <file>selfservice.html</file>
```

```
<components>
  <component>
    <tag>%TITLE%/tag>
    <default>Login to the network</default>
  </component>
  <component>
    <tag>%HEADER%/tag>
    <default>Create your guest account</default>
  </component>
  <component>
    <tag>%MAIN%/tag>
    <default/>
  </component>
  <component>
    <tag>%FOOTER%/tag>
    <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
  </component>
</components>
<label>Self Service</label>
</selfService>
<payment>
  <file>payment.html</file>
  <components>
    <component>
      <tag>%TITLE%/tag>
      <default>Login to the network</default>
    </component>
    <component>
      <tag>%HEADER%/tag>
```

```
    <default>Purchase your account</default>
</component>
<component>
    <tag>%MAIN%</tag>
    <default/>
</component>
<component>
    <tag>%FOOTER%</tag>
    <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
</component>
</components>
<label>Purchase Account</label>
</payment>
<password>
<file>password.html</file>
<components>
    <component>
        <tag>%TITLE%</tag>
        <default>Login to the network</default>
    </component>
    <component>
        <tag>%HEADER%</tag>
        <default>Change your password</default>
    </component>
    <component>
        <tag>%MAIN%</tag>
        <default/>
    </component>
    <component>
```

```
<tag>%FOOTER%</tag>
<default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
</component>
</components>
<label>Change Password</label>
</password>
<aup>
<file>aup.html</file>
<components>
<component>
<tag>%TITLE%</tag>
<default>Login to the network</default>
</component>
<component>
<tag>%HEADER%</tag>
<default>Acceptable Usage Policy</default>
</component>
<component>
<tag>%MAIN%</tag>
<default>By clicking "Accept" you agree to the terms and
conditions.....</default>
</component>
<component>
<tag>%FOOTER%</tag>
<default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
</component>
</components>
<label>Acceptable Usage Policy</label>
</aup>
<generic>
```



```
<file>generic.html</file>

<components>

  <component>

    <tag>%TITLE%</tag>

    <default>Login to the network</default>

  </component>

  <component>

    <tag>%HEADER%</tag>

    <default/>

  </component>

  <component>

    <tag>%MAIN%</tag>

    <default>your text here</default>

  </component>

  <component>

    <tag>%FOOTER%</tag>

    <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>

  </component>

</components>

<label>Generic page</label>

</generic>

</pages>

<images>

  <image>

    <label>Header image</label>

    <description>Image placed on the header of every page</description>

    <tag>%IMG_LOGO%</tag>

    <file>Logo.png</file>

    <dimensions>100x100</dimensions>
```

```
</image>
<image>
  <label>Favicon</label>
  <description>Image to be displayed in browser address bar</description>
  <tag>%IMG_FAV_ICON%</tag>
  <file>Favicon16.ico</file>
  <dimensions>16x16</dimensions>
</image>
</images>
<colours>
  <colour>
    <label>Body background color</label>
    <description/>
    <tag>%CL_BODY_BACKGROUND%</tag>
    <value>#333333</value>
  </colour>
  <colour>
    <label>Content area background color</label>
    <description/>
    <tag>%CL_CONTENT_BACKGROUND%</tag>
    <value>#eeeeee</value>
  </colour>
</colours>
</hotspotTheme>
```

Since we are using the same customizable areas we didn't make any changes to the <pages> element content, it is generally a good idea to use the same names for the content areas e.g. %HEADER%, %FOOTER%, etc... as this will allow users to switch between themes using the content they have defined already.

Now that we have updated the theme.xml and we are happy with the design of our page we should replace any colour and image references with their respective placeholder on both the login.html file and the style.css file.

The login html file should look similar to :

```
<div id="content">
  <div id="header">
    <div id="headerImage"></div>
    <h1 class="pageTitle">%HEADER%</h1>
  </div>
  <div id="main">
    <div class="mainContent">%MAIN%</div>
    <div class="widgetContainer">%LOGIN_WIDGET%</div>
  </div>
  <div id="footer">
    <div id="navigation">%NAVIGATION_MENU%</div>
    <div class="copyright">%FOOTER%</div>
  </div>
</div>
```

The style.css file should look similar to:

```
body{
  font-family:Arial;
  background-color:%CL_BODY_BACKGROUND%;
}
#content{
  width:45%;
  margin:auto;
  padding:20px;
  margin-top:50px;
  background-color:%CL_CONTENT_BACKGROUND%;
}
#header{
  text-align:center;
  margin-bottom:25px;
  padding:5px;
}
```

```

#main {
    padding:25px;
}

.widgetContainer {
    width:80%;
    padding:50px;
}

#footer{
    text-align:center;
    margin-top:25px;
    padding:5px;
    font-size:x-small;
}

.navigation{
    padding:5px;
}

```

In this case we want all pages to have the same basic layout, so we need edit the remaining files in the html/ directory and replace their contents with the code from login.html, the only change we need to do is replace the %LOGIN\_WIDGET% placeholder with the relevant widget for the page in question, the following code would be present in the selfservice.html file:

```

<div id="content">
    <div id="header">
        <div id="headerImage"></div>
        <h1 class="pageTitle">%HEADER%</h1>
    </div>
    <div id="main">
        <div class="mainContent">%MAIN%</div>
        <div class="widgetContainer">%SELF_SERVICE_WIDGET%</div>
    </div>
    <div id="footer">
        <div id="navigation">%NAVIGATION_MENU%</div>
        <div class="copyright">%FOOTER%</div>
    </div>

```

```
</div>
```

```
</div>
```

Now that the HTML and CSS files are done we need to give our theme a name and description, declare our preview images and fill in the author information in theme.xml.

Assuming we took two screenshots of our page, preview\_small.png and preview\_large.png and placed these files in the root directory of our theme we should edit the theme.xml file to look similar to:

```
<?xml version="1.0"?>
<hotspotTheme>
  <name>tutorial_theme</name>
  <description>Simple theme built during the tutorial</description>
  <author>myname</author>
  <preview>
    <small>preview_small.png</small>
    <large>preview_large.png</large>
  </preview>
  <pages>
    <login>
      <file>login.html</file>
      <components>
        <component>
          <tag>%TITLE%</tag>
          <default>Login to the network</default>
        </component>
        <component>
          <tag>%HEADER%</tag>
          <default>Login to the network</default>
        </component>
        <component>
          <tag>%MAIN%</tag>
          <default/>
        </component>
      </components>
    </login>
  </pages>
</hotspotTheme>
```

```
</component>

<component>
  <tag>%FOOTER%</tag>
  <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
</component>

</components>

<label>Login</label>
</login>

<selfService>
  <file>selfservice.html</file>
  <components>
    <component>
      <tag>%TITLE%</tag>
      <default>Login to the network</default>
    </component>
    <component>
      <tag>%HEADER%</tag>
      <default>Create your guest account</default>
    </component>
    <component>
      <tag>%MAIN%</tag>
      <default/>
    </component>
    <component>
      <tag>%FOOTER%</tag>
      <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
    </component>
  </components>
  <label>Self Service</label>
</selfService>
```

```
<payment>
  <file>payment.html</file>
  <components>
    <component>
      <tag>%TITLE%</tag>
      <default>Login to the network</default>
    </component>
    <component>
      <tag>%HEADER%</tag>
      <default>Purchase your account</default>
    </component>
    <component>
      <tag>%MAIN%</tag>
      <default/>
    </component>
    <component>
      <tag>%FOOTER%</tag>
      <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
    </component>
  </components>
  <label>Purchase Account</label>
</payment>
<password>
  <file>password.html</file>
  <components>
    <component>
      <tag>%TITLE%</tag>
      <default>Login to the network</default>
    </component>
```

```
<component>
  <tag>%HEADER%/tag>
  <default>Change your password</default>
</component>
<component>
  <tag>%MAIN%/tag>
  <default/>
</component>
<component>
  <tag>%FOOTER%/tag>
  <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
</component>
</components>
<label>Change Password</label>
</password>
<aup>
<file>aup.html</file>
  <components>
    <component>
      <tag>%TITLE%/tag>
      <default>Login to the network</default>
    </component>
    <component>
      <tag>%HEADER%/tag>
      <default>Acceptable Usage Policy</default>
    </component>
    <component>
      <tag>%MAIN%/tag>
      <default>By clicking "Accept" you agree to the terms and
        conditions.....</default>
    </component>
  </components>
</aup>
```



```
</component>
<component>
  <tag>%FOOTER%</tag>
  <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
</component>
</components>
<label>Acceptable Usage Policy</label>
</aup>
<generic>
  <file>generic.html</file>
  <components>
    <component>
      <tag>%TITLE%</tag>
      <default>Login to the network</default>
    </component>
    <component>
      <tag>%HEADER%</tag>
      <default/>
    </component>
    <component>
      <tag>%MAIN%</tag>
      <default>your text here</default>
    </component>
    <component>
      <tag>%FOOTER%</tag>
      <default><![CDATA[Copyright &copy; yourcompany 2010]]></default>
    </component>
  </components>
  <label>Generic page</label>
```

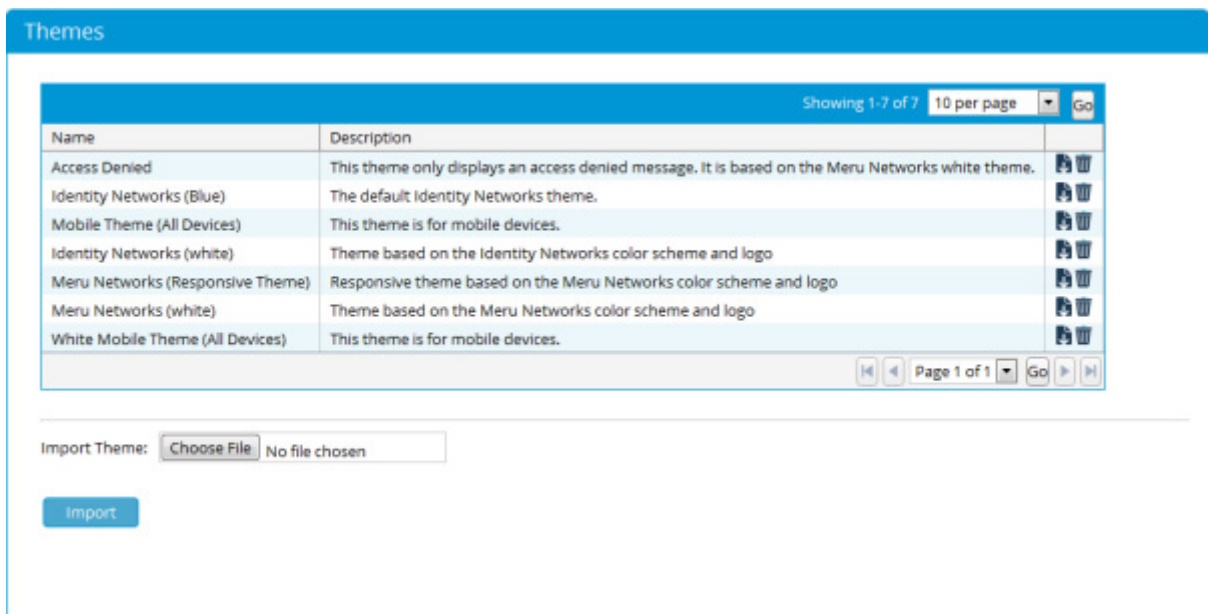
```
</generic>
</pages>
<images>
  <image>
    <label>Header image</label>
    <description>Image placed on the header of every page</description>
    <tag>%IMG_LOGO%</tag>
    <file>Logo.png</file>
    <dimensions>100x100</dimensions>
  </image>
  <image>
    <label>Favicon</label>
    <description>Image to be displayed in browser address bar</description>
    <tag>%IMG_FAV_ICON%</tag>
    <file>Favicon16.ico</file>
    <dimensions>16x16</dimensions>
  </image>
</images>
<colours>
  <colour>
    <label>Body background color</label>
    <description/>
    <tag>%CL_BODY_BACKGROUND%</tag>
    <value>#333333</value>
  </colour>
  <colour>
    <label>Content area background color</label>
    <description/>
    <tag>%CL_CONTENT_BACKGROUND%</tag>
```

```
<value>#eeeeee</value>
</colour>
</colours>
</hotspotTheme>
```















The final step is to create a zip file containing all the theme files, the directory structure of the zip file should be similar to that of the default theme.

## Installing a Custom Theme

To install a theme go to the **Guest Portals --> Themes** from the Administration interface.



The screenshot displays the 'Themes' management interface. At the top, there is a blue header with the title 'Themes'. Below the header, a table lists various themes. The table has two columns: 'Name' and 'Description'. Each row also includes a set of icons for editing and deleting. The table shows 7 themes, with the first row being 'Access Denied' and the last row being 'White Mobile Theme (All Devices)'. Below the table, there is a section for importing a new theme. It includes a text input field labeled 'Import Theme:' with a 'Choose File' button and the text 'No file chosen'. Below this is a blue 'Import' button. The interface also features pagination controls at the bottom right of the table, indicating 'Showing 1-7 of 7' items, '10 per page', and 'Page 1 of 1'.

Name	Description	
Access Denied	This theme only displays an access denied message. It is based on the Meru Networks white theme.	 
Identity Networks (Blue)	The default Identity Networks theme.	 
Mobile Theme (All Devices)	This theme is for mobile devices.	 
Identity Networks (white)	Theme based on the Identity Networks color scheme and logo	 
Meru Networks (Responsive Theme)	Responsive theme based on the Meru Networks color scheme and logo	 
Meru Networks (white)	Theme based on the Meru Networks color scheme and logo	 
White Mobile Theme (All Devices)	This theme is for mobile devices.	 

Import Theme:  No file chosen

Click the **Choose File** button and browse your computer for the theme file, after selecting the file click the **Import** button and verify the page is refreshed and the new theme is present in the Themes list.

# Available Widgets

**Table 2:**

Page	Widget
Login	%LOGIN_WIDGET%
Payment	%PAYMENT_WIDGET%
Self Service	%SELF_SERVICE_WIDGET%
Acceptable Usage Policy	%AUP_WIDGET%
Password Change	%PASSWORD_WIDGET%
Logout	%LOGOUT_WIDGET%
Logout Popup	%LOGOUT_POPUP%
Time Left	%TIME_LEFT_WIDGET%

## Portal Rules

---

The FortiConnect can be used to create a set of Portal Rules for redirecting Users to different Portals that have been created.

From the FortiConnect Administration interface go to **Guest Portals --> Portal Rules** as shown below.

## Portal Rules

Each rule is checked in the following order. If a rule is matched the guest is directed to the rule's portal (or is denied access) and no other rules are checked. If no rule matches the default rule is applied.

Set your network devices to redirect to the following URL to use portal rules:

**https://{MERU\_CONNECT}/portal/{DEVICE\_IP}**

Order	Name	Description	Rule	Portal	Hit Count	
1	<a href="#">Default</a>	Default if no other rules match		login	0	

[Test portal rules](#)

Save

Cancel

Add Rule

Each rule that is created is checked in the order shown. If a rule is matched, the User is directed to the rules portal (or denied access) and no other rules are checked. If no rule matches then the default rule is applied.

**Note:** FortiConnect comes with the Default rule.

1. To add a rule click on the **Add Rule** button.

## Edit Rule

Guests are directed to the specified portal if all the specified conditions are met.

Rule Name:

Rule Description:

idm-host-ip-address

[add condition](#)

Rule Action:  Go to portal

No portal (sends HTTP 403 Unauthorised header)

Save

Cancel

- In the fields provided input the following -
  - Rule Name** - Create a name for your rule.
  - Rule Description** - Enter a description for your rule.
  - Rule Action** - Check the **Go To Portal** option and then use the drop down menu to select from one of the portals you have created, or one of the default portals, to direct the User to the relevant portal. Check **No portal** if you do not wish to redirect the User.
- From the drop down lists provided create a set of rules that applies to your portal. The example that has been created above reflects Users using 'Mobile' as their device, you will see that the Rule Action has been set to 'Go To Portal' mobile'. Therefore any Users using a mobile device will be directed to a portal is designed for mobile users.
- Click **add** condition once created.
- Click **Save** to complete.

## Portal Rules

✓ Portal rule saved

Each rule is checked in the following order. If a rule is matched the guest is directed to the rule's portal (or is denied access) and no other rules are checked. If no rule matches the default rule is applied.

Set your network devices to redirect to the following URL to use portal rules:

**https://{MERU\_CONNECT}/portal/{DEVICE\_IP}**

Order	Name	Description	Rule	Portal	Hit Count	
1	<a href="#">Rule One</a>	test	idm-host-ip-address equals 10.10.1.1	access-denied	0	 
2	<a href="#">Default</a>	Default if no other rules match		login	0	 

[Test portal rules](#)

Save

Cancel

Add Rule

As you can see the rule has now been created and added to the list.

6. Use the up and down arrow icons next to the order number to move the order of the rules. Click on **Add Rule** to create any further rules.
7. You can test any portal rules you have created by clicking on the **Test Portal Rules** link, this will display a screen as shown below.

Test Portal Rules

This finds the rule that matches the environment you define below.

Browser:   on  [Detect my browser](#)

Mobile device:

Browser Language:

Time:  on  in  [Now](#)

RADIUS Client IP Address:

User IP Address:

Meru Connect IP Address:

8. Find any rule that matches the environment you define :-
  - **Browser** - From the drop down menu's select and define the browser you wish to test against.
  - **Mobile Device** - Check if using a mobile device.
  - **Browser Language** - From the drop down menu select the browser language.
  - **Time** - From the drop down menu's select a time you wish to test.
  - **RADIUS Client IP Address** - Enter the RADIUS Clients IP address.
  - **User IP Address** - Enter the User's IP Address.
  - **FortiConnect IP Address** - Enter the FortiConnects IP Address.
9. Click on **Find Matching Rule** to test.

## Hotel Property Management System Integration

---

FortiConnect supports integration with a number of Hotel Property Management Systems. FortiConnect allows communication with the Hotel Property Management System to enable billing for internet access direct to a guest's hotel room bill. This is achieved by adding a Hotel Property Management System login widget to a portal which will communicate with the Hotel Property Management System.



Different Hotel Property Management Systems can be added via the Admin Interface > **Guest Portals** > **Hotel PMS**.

Supported Hotel Property Management System's include:-

- HOBIC (via TCP/IP)
- MICROS Fidelio Suite / Opera (via TCP/IP)
- Infoden RMS
- Comtrol Lodging Link (via TCP/IP) - a list of support Hotel Property Management Systems are available here <http://www.comtrol.com/pub/en/Property-Management-Systems-Partners>

Each Portal will be able to define it's own access plans which determine the access time allowed and associated charge to be posted to the Hotel Property Management System configured for that portal.

The first time a user goes to the portal and supplies their credentials (these can be last name and room number, username and password, etc) they will be taken to a page with the available access plans, once the user select ones and proceeds with the authentication process their room will be charged.

The user will be able to login without being charged until their account expires, once the account expires the user will be again taken to the access plan selection where they can purchase more time on the network.

## Ordering and Support with PMS Vendors

Some PMS vendors require additional part numbers to be ordered to allow integration, please check with the vendor you wish to integrate with before ordering.

For support with Opera PMS, the following part number needs to be ordered from Micros

### What Part Numbers Do I Need?

Part No	Product ID (FKT)	Description
IO-5009-271	IFC_IMN	Identity Manager by Meru Networks

## Adding a Hotel Property Management System

To add a Hotel Property Management System from the administration interface:

1. Select **Guest Portals** > **Hotel PMS** as shown below.

## Hotel Property Management Systems

10 per page

Name ▲▼	Type ▲▼	Description ▲▼
No Property Management Systems defined		

2. Click the **Add** button

Add New Hotel Property Management System

Name:

Description:

Type:

IP Address:

Port:


3. Fill in the appropriate fields to add the Hotel Property Management System :-
  - Name - Name of the Hotel Property Management System
  - **Description** - Description of the Hotel Property Management System.
  - **Type** - From the drop down menu select the type of Hotel Property Management System you will integrate with.
  - **IP Address** - Enter the IP address of the Hotel Property Management System.
  - **Port** - Enter the Port Number required for the Hotel Property Management System.
4. Click on **Save** once complete.

## Editing and Deleting a Hotel Property Management System

5. To Edit an existing Hotel Property Management System go to **Guest Portals --> Hotel PMS** as shown below

## Hotel Property Management Systems

Showing 1-1 of 1 | 10 per page | Go

Name ▲▼	Type ▲▼	Description ▲▼	
<a href="#">PMS One</a>	HOBIC	Test PMS	

Page 1 of 1 | Go

Add

- Click on the link of the Hotel Property Management System you wish to edit

## Edit Hotel Property Management System

Name:

Description:

Type:

IP Address:

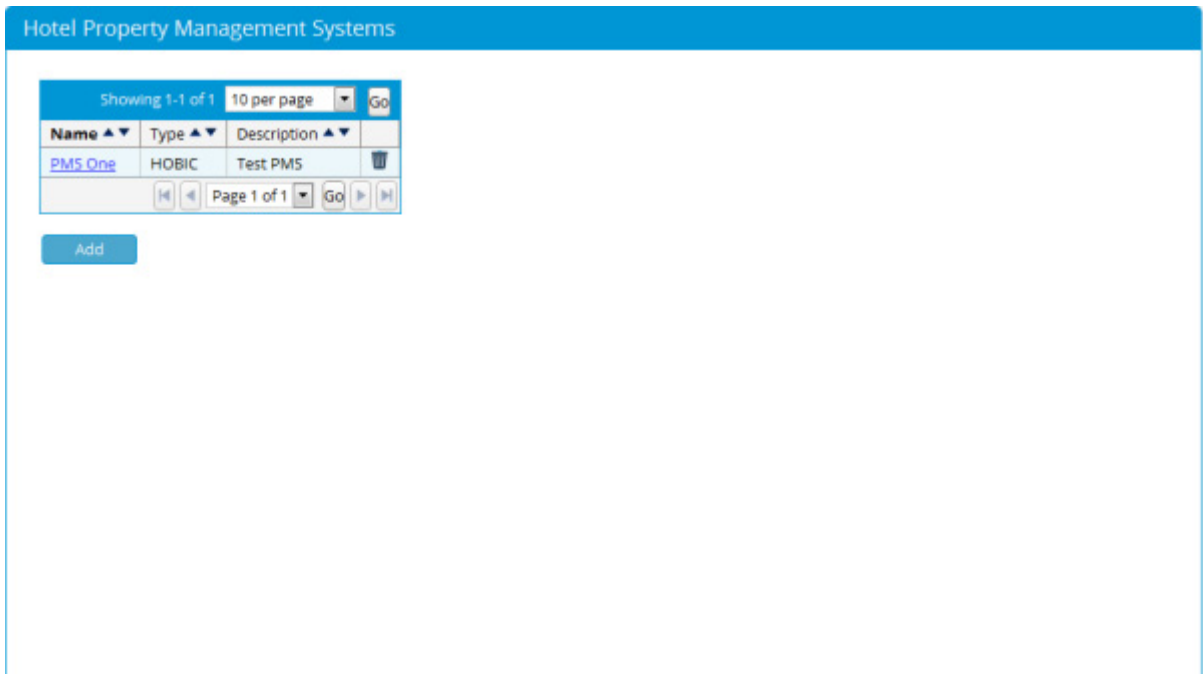
Port:

- Fill in the appropriate fields to edit the Hotel Property Management System :-
  - Name - Name of the Hotel Property Management System
  - Description** - Description of the Hotel Property Management System.

- **Type** - From the drop down menu select the type of Hotel Property Management System you will integrate with.
- **IP Address** - Enter the IP address of the Hotel Property Management System.
- **Port** - Enter the Port Number required for the Hotel Property Management System.

Click on **Save** once complete.


8. To **delete** a Hotel Property Management System go to **Guest Portals --> Hotel PMS** as shown below



9. Click on the **Bin** icon to the right of the Hotel Property Management System you wish to **delete** and click on yes to confirm as shown below.

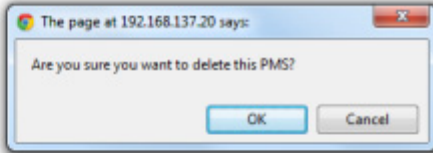
## Hotel Property Management Systems

Showing 1-1 of 1    10 per page    Go

Name ▲▼	Type ▲▼	Description ▲▼	
<a href="#">PMS_One</a>	HOBIC	Test PMS	

Page 1 of 1    Go

Add



## PMS Payment Reports

Administrators can run a Payment Report which details all transactions purchased through a Property Management Systems account.

1. From the Admin UI Interface, go to **Reports & Logs-->Payments Report**, you will be presented with a screen similar to the one below.

## Payments Report

Payment Method:	<input type="text" value="Credit Card Billing"/>	Payment Provider:	<input type="text" value="All"/>
Portal:	<input type="text" value="All"/>	Access Plan:	<input type="text" value="All"/>
Transaction ID:	<input type="text"/>	From:	<input type="text" value="25"/> <input type="text" value="Nov"/> <input type="text" value="2014"/>
Username:	<input type="text"/>	To:	<input type="text" value="2"/> <input type="text" value="Dec"/> <input type="text" value="2014"/>
Name on Card:	<input type="text"/>		

Run

Download CSV

### Purchased Guest Accounts Summary

Portal	Number of Accounts	Total
No Records Found		

Transaction ID ▲▼	Name on Card ▲▼	Portal ▲▼	Payment Provider ▲▼	Access Plan	Username ▲▼	Amount ▲▼	Date ▲▼
No Records Found							

- To run a report on **PMS Billing** select the PMS Billing option from the **Payment Method** field :-
  - Hotel PMS** - From the drop down menu select a Hotel PMS.
  - Portal** - From the drop down menu select a Portal.
  - Access Plan** - From the drop down menu select an access plan.
  - Transaction ID** - From the drop down menu select a Transaction ID.
  - Username** - From the drop down menu select a Username.
  - Customer Name** - From the drop down menu select a Customer Name.
  - Room Number** - From the drop down menu select a Room Number.
  - From** - From the drop down menu select a From Date.
  - To** - From the drop down menu select a To Date.
- Click **Run** to display the report on screen, or click **Download CSV** to download as a file to your desktop.
- A detailed report will show.
  - Transaction ID** - Guests Transaction ID
  - Name on Card** - Guests name on card provided.

- **Portal** - Portal the Guest accessed.
- **Guest** - Guest account username.
- **Payment Provider** - Which Payment Provider the Guest used.
- **Access Plan** - Access plan the Guest used for Guest access.
- **Username** - Username of the Guest.
- **Amount** - Amount the Guest was charged.
- **Date** - Date and Time the Guest user accessed.

# Configuring Payment Providers for Credit Card Billing

---

When using the FortiConnect to allow Users to purchase accounts using **credit card billing**, you need to add the details of the payment provider. The payment provider details are needed to allow your payment provider to perform credit card billing into your account.

## Adding a Payment Provider

From the administration interface, select **Guest Portals > Payment Providers** as shown below.



## Payment Providers

10 per page

Name ▲▼	Type ▲▼	Description ▲▼	
No payment providers defined			

1. Click **Add** and enter the relevant details in the fields as shown below.

## Add New Payment Provider

**Account Details**

Account Name:

Account Description:

Payment Provider:

Operation Mode:  (<https://secure.authorize.net/gateway/transaction.dll>)

API Login:

Transaction Key:

Available Cards

- Visa
- MasterCard
- American Express
- Diners Club
- Discover Card
- En Route
- JCB
- Carte Blanche

Supported Cards

Payment Page Settings

Show/Hide input fields on the payment page of the Guest Portal using this account.

Security Code:

Issue Number:

Mobile Number:

Billing Address:

Postal/ZIP Code:

Country:

### 2. Enter the details as follows:

- **Account Name**—Enter the name of the payment provider account.
- **Account Description**—Enter the description of the payment provider account.
- **Payment Provider**—Choose the relevant payment provider from the dropdown menu provided.
- **Operation Mode** - From the dropdown menu select whether this will be a **production** or **test** payment gateway. The link to the right shows the URL that will be used for the payment gateway's API.
- **API Login**—Enter the API login for the payment provider account.
- **Transaction Key**—Enter the transaction key for the payment provider account.
- From the **Available Cards** list, select the cards you wish to allow for transactions and click the relevant arrows to add or remove them.
- You can test your connection and send a test transaction by clicking on the **Test Connection** button.

### 3. 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 to use each field using the drop-down menu -

- **Required** - Field requires input

- **Optional** - Field can be left blank
- **Unused** - Field will not appear

4. Once completed, click the **Save** button.

Selecting a different payment provider will enable more or less options depending on the payment provider settings required, this is shown below using **Payflow Pro** as an example.

The screenshot shows a web form titled "Add New Payment Provider" with a blue header. The form is divided into several sections:

- Account Details:** Includes input fields for "Account Name", "Account Description", "Payment Provider" (set to "PayPal Payflow Pro"), "Operation Mode" (set to "Production" with a URL "[https://payflowpro.paypal.com]"), "User", "Password" (with a "Confirm:" field), "Merchant Name", and "Partner".
- Available Currencies:** A list of currencies including Afghani (AFN), Algerian Dinar (DZD), Argentine Peso (ARS), Armenian Dram (AMD), Aruban Guilder (AWG), Australian Dollar (AUD), Azerbaijanian Manat (AZN), and Bahamian Dollar (BSD).
- Supported Currencies:** An empty list for selecting supported currencies.
- Available Cards:** A list of cards including Visa, MasterCard, American Express, Diners Club, and Discover Card.
- Supported Cards:** An empty list for selecting supported cards.


Navigation arrows (left and right) are present between the "Available" and "Supported" lists for both currencies and cards.

## Editing or Deleting a Payment Provider

1. From the administration interface, select **Guest Portals > Payment Providers** as shown below.

## Payment Providers

Showing 1-1 of 1 10 per page Go

Name ▲▼	Type ▲▼	Description ▲▼	
<a href="#">Payment_One</a>	PayPal Payflow Pro	Payment	

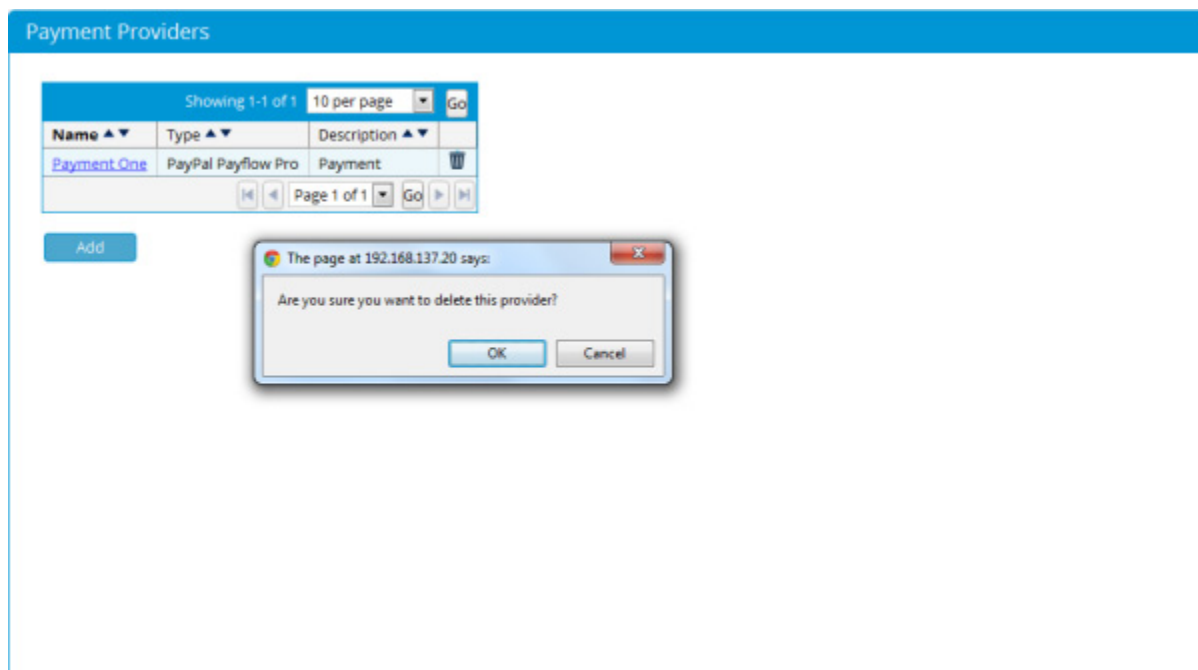
Page 1 of 1 Go

Add

2. Click the name of the payment provider you want to edit.
3. Enter the details as follows:
  - **Account Name**—Enter the name of the payment provider account.
  - **Account Description**—Enter the description of the payment provider account.
  - **Payment Provider**—Choose the relevant payment provider from the dropdown menu provided.
  - **API Login**—Enter the API login for the payment provider account.
  - **Transaction Key**—Enter the transaction key for the payment provider account.
4. Once completed, click the **Save Payment Provider** button.

To delete a payment provider :

5. Click on the **Bin** icon next to the payment provider you wish to delete and click on **yes** to confirm as shown below.



## Payments Reports

Administrators can now run a Payment Report which details all transactions purchased through a Hotspot account.

1. From the Admin UI Interface, go to **Reports & Logs->Payments Report**, you will be presented with a screen similar to the one below

## Payments Report

Payment Method:  Payment Provider:   
 Portal:  Access Plan:   
 Transaction ID:  From:     
 Username:  To:     
 Name on Card:

**Purchased Guest Accounts Summary**

Portal	Number of Accounts	Total
No Records Found		

10 per page <input type="button" value="Go"/>							
Transaction ID ▲▼	Name on Card ▲▼	Portal ▲▼	Payment Provider ▲▼	Access Plan	Username ▲▼	Amount ▲▼	Date ▲▼
No Records Found							

2. To run a report on **Credit Card Billing** select the Credit Card Billing option from the **Payment Method** field :-
  - **Payment Provider** - From the drop down menu select a Payment Provider.
  - **Portal** - From the drop down menu select a Portal.
  - **Access Plan** - From the drop down menu select an access plan.
  - **Transaction ID** - From the drop down menu select a Transaction ID.
  - **Username** - From the drop down menu select a Username.
  - **Name on Card** - From the drop down menu select a Name on Card.
  - **From** - From the drop down menu select a From Date.
  - **To** - From the drop down menu select a To Date.
3. Click **Run** to display the report on screen, or click **Download CSV** to download as a file to your desktop.
4. A detailed report will show :-
  - **Transaction ID** - Users Transaction ID
  - **Customer** - Users name on card provided.

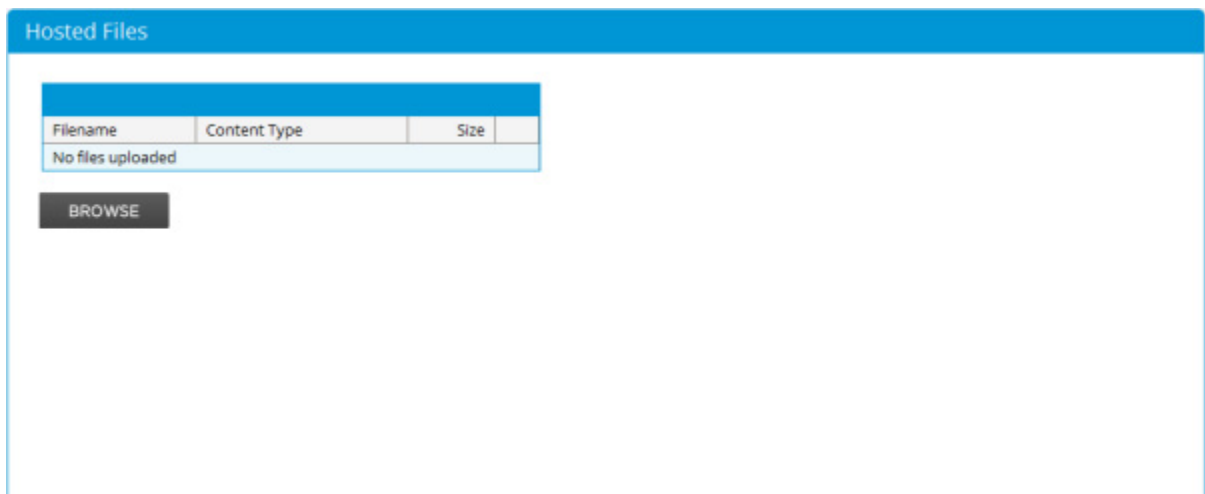
- **Guest Portal** - Portal the User accessed.
  - **Guest** - User account username.
  - **Payment Account** - Which Payment Provider the User used.
  - **Access Plan** - Access plan the Used for Guest access.
  - **Amount** - Amount the User was charged plus tax if required.
  - **Date** - Date and Time the User user accessed.
5. You can then manually add a transaction for the User.
    - **Transaction Type** - Select whether you wish to **Charge** or **Refund** the User.
    - **Amount** - Select the amount you wish to **Charge** or **Refund** the User.
    - **Reason** - Add a reason for the **Charge** or **Refund**.
  6. Click **add** to confirm.
  7. Click on the **Send Purchase Receipt** button to send a receipt of the transaction to the users email address.

## Hosted Files

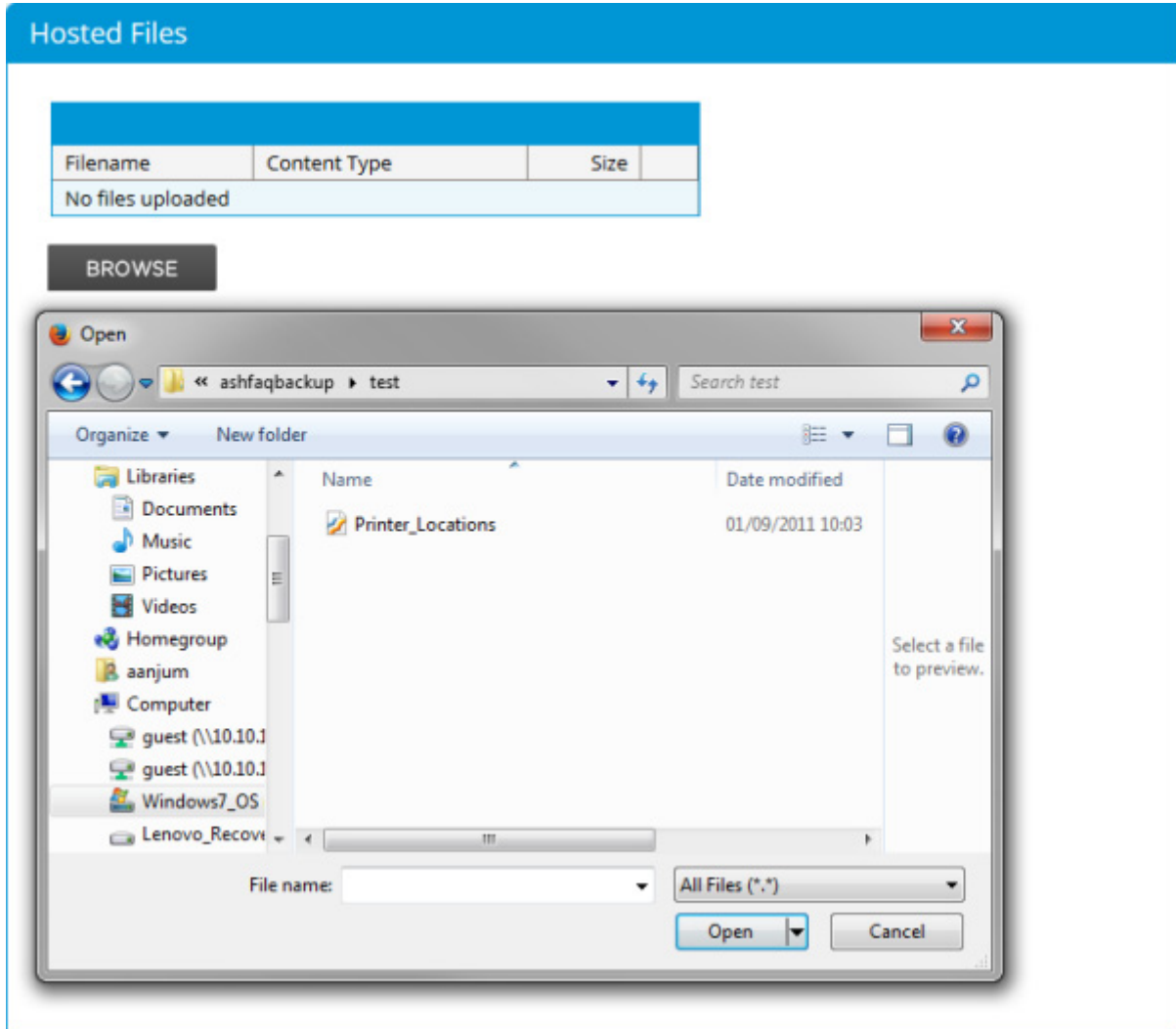
---

FortiConnect supports the uploading of arbitrary files for use in Portals.

To upload any files, go to **Guest Portals-->Hosted Files** on the FortiConnect Administration interface as shown below.



1. To upload a file click on the **BROWSE** button to locate the file you wish to upload for use in a Portal as shown below.





2. Select the file you wish to upload and click on **Save**, the file will then be displayed as shown below.



Hosted Files

✔ "Printer\_Locations.pdf" uploaded

Filename	Content Type	Size	
<a href="#">Printer_Locations.pdf</a>	application/pdf	274Kb	 

BROWSE

3. To view the file click on the **magnifying glass** icon.
4. To delete a file click on the **bin** icon.

## Adding links to Portals

To add your link to a page in your Portal, we can follow the instructions below.



**Note:** For this example we will add to the **Login Page** on the Portal using pre authentication, steps and screen shots for other pages will differ.

Go to **Guest Portals**-->**Hosted Files** on the FortiConnect Administration interface.

1. Click on the **Filename** of the link you wish to add to your page as shown below.

Hosted Files

"Printer\_Locations.pdf" uploaded

Filename	Content Type	Size	
<a href="#">Printer_Locations.pdf</a>	application/pdf	274Kb	 

**Printer\_Locations.pdf**

Filename: Printer\_Locations.pdf

Size: 274Kb (280 244 bytes)

Uploaded: 17-Dec-2014 14:12

MD5: 8967d09077d1036fc35a234396b59512

URL: [https://10.10.1.37/hosted\\_file/e\\_a\\_0\\_0\\_2fa/16o1/Printer\\_Locations.pdf](https://10.10.1.37/hosted_file/e_a_0_0_2fa/16o1/Printer_Locations.pdf)

Content Type:

Character Set:

2. Copy the URL of the link you wish to use for your Portal and click on **close**.
3. Go to **Guest Portals-->Portals** on the FortiConnect Administration interface.
4. Click on the **Edit Portal Content** Icon next to the Portal you wish to add the link to, and identify which area on the Portal you wish have the link displayed.

## Login Page

Cookies Instructions Page	Customise the content of the Login page
Close this window Page	
Authenticating waiting Page	
Session management Page	
<b>Login Page</b>	
Acceptable Usage Policy Page	
Purchase Account Page	
Successful Authentication Page	
Logout Page	
Logged Out Page	
Client Configuration Page	
IOS auto login Page	
Widget Labels	

Page label:

Header:

Main:

Title:

5. Copy the Link into the appropriate area and wrap it with **Standard HTML Anchor Tags**.
6. Click **Save**

## Proxy Auto Discovery

---

Administrators can host Web Proxy Auto Discovery PAC files on the FortiConnect, to do this go to **Guest Portals --> Proxy Auto Discovery** as shown in the screen shot below.

## Web Proxy Auto Discovery Settings

Enable Web Proxy Auto Discovery:

Proxy Server:

Port:

Do not proxy requests to Meru Connect:

Save

Cancel

1. Check the **Enable Web Proxy Auto Discovery** check box.
2. Enter the **Proxy Server** settings in the field provided.
3. Enter the **Port** number in the field provided.
4. Check the **Do not proxy requests to FortiConnect** if you wish to do so.

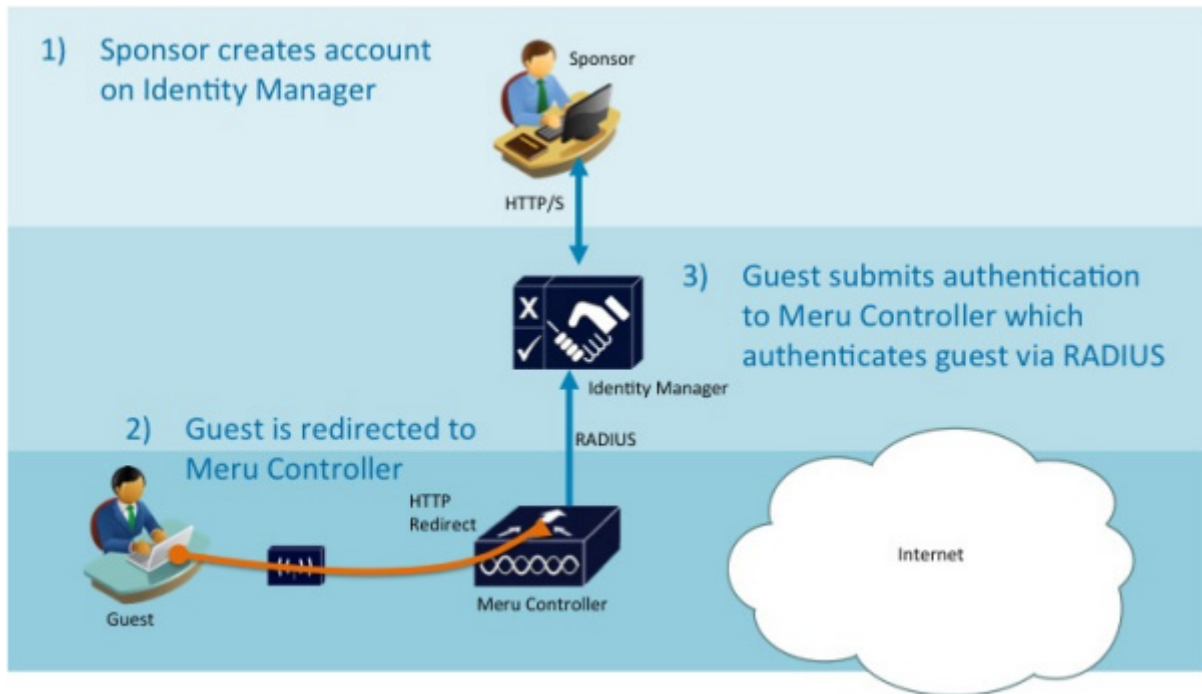
Click on **Save** to continue.

# Integrating with a FortiWLC

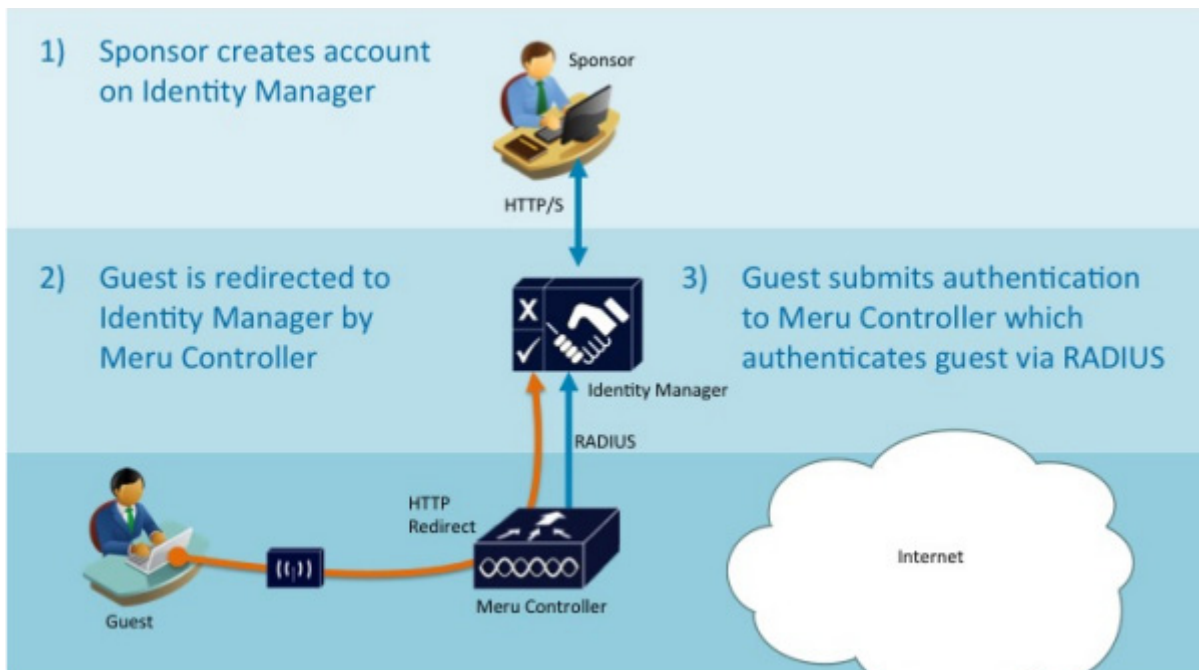
FortiConnect can be integrated with FortiWLC enterprise wireless LAN controllers and integrated FortiGate enterprise firewall LAN controllers to provide a fully integrated solution for authenticating, managing and reporting on users accessing the network with web authentication.

There are two different options for FortiConnect integration:

1. Internal Captive Portal on Fortinet Controllers - You can use the integrated portal pages on the Fortinet Controller to provide the portal web pages. users authenticate against the Fortinet Controller which in turn authenticates the user against the FortiConnect using RADIUS.



2. External Captive Portal on FortiConnect - You can host the portal pages directly on the FortiConnect, this provides additional benefits and features such as Self Service, Smart Connect, Password Change, Billing Support and Acceptable Use Pages. This works by having the Fortinet Controller redirect the user to the FortiConnect. The FortiConnect web pages submit the authentication to the Fortinet Controller which then authenticates the user against the FortiConnect using RADIUS.



## Baseline Configuration

Prior to configuring the integration the following was carried out using the steps shown in the relevant configuration guides for FortiConnect and Fortinet Configuration Guides.

- Fortinet
  - Ⓢ initial setup
  - Ⓢ licenses installed
  - Ⓢ access points added to the system
  - Ⓢ add an ESS profile
- FortiConnect
  - Ⓢ initial setup
  - Ⓢ licenses installed
  - Ⓢ sponsors configured and permitted to create user accounts

This configuration must be performed before moving on with following the instructions in the rest of this chapter.

# Adding the Fortinet Controller to FortiConnect

## *Adding a RADIUS Client to the FortiConnect*

The first step is to configure the FortiConnect to allow the Fortinet Controller to authenticate using RADIUS.

1. Login to the admin interface of the FortiConnect at <https://identitymanager/admin>
2. Navigate to **Devices > RADIUS Clients**
3. Click the **Add RADIUS Client** button and you will see the screen as shown below

**RADIUS Clients**

**Client** | Attributes | SNMP | MAC Authentication | RadSec Authentication

Name:

Device IP Address / Prefix Length:   
For example 192.168.1.1/32 or fec0:0001/128

Secret:  Confirm:

Type:   
If your RADIUS client vendor is not listed please select Generic RADIUS Device

Description:

**Change-of-Authorization**

Use COA:

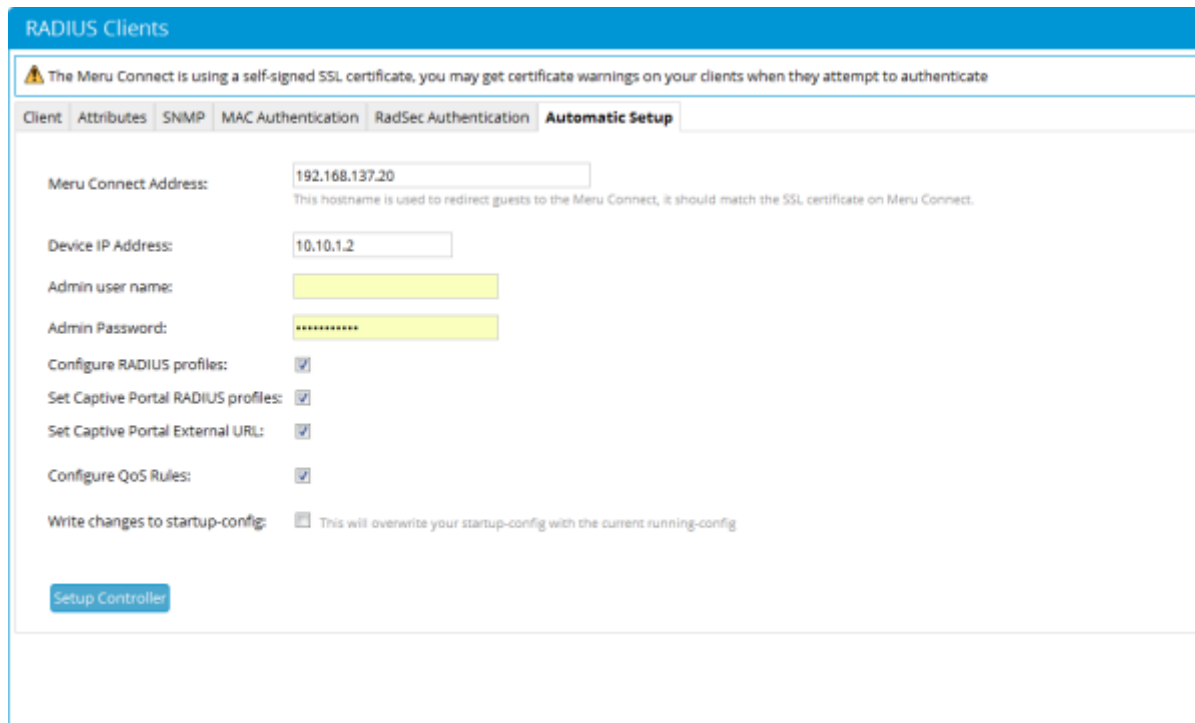
Port:

4. Enter the **Name** that you want to remember the device with.
5. Enter the **Device IP Address** of the Fortinet Controller. This is the IP address that will be sending RADIUS requests to the FortiConnect.
6. Enter a shared **Secret** and **Confirm** it, this value will need to be entered onto the Fortinet Controllers RADIUS setup.
7. Set the **Type** to Fortinet (Two Options are available, Fortinet SD 5.3 & Earlier and Fortinet SD 6.0 & Later)

Click **Save**.

# Automatically Configuring the Fortinet Controller to authenticate against FortiConnect

8. When you are adding RADIUS for authentication with a Fortinet Controller you will see the tab appear as shown below.



The screenshot shows the 'Automatic Setup' tab for RADIUS Clients configuration. At the top, there is a warning message: 'The Meru Connect is using a self-signed SSL certificate, you may get certificate warnings on your clients when they attempt to authenticate'. Below this, there are several configuration fields and checkboxes:

- Client** | **Attributes** | **SNMP** | **MAC Authentication** | **RadSec Authentication** | **Automatic Setup**
- Meru Connect Address:** 192.168.137.20  
This hostname is used to redirect guests to the Meru Connect, it should match the SSL certificate on Meru Connect.
- Device IP Address:** 10.10.1.2
- Admin user name:** [Redacted]
- Admin Password:** [Redacted]
- Configure RADIUS profiles:**
- Set Captive Portal RADIUS profiles:**
- Set Captive Portal External URL:**
- Configure QoS Rules:**
- Write changes to startup-config:**  This will overwrite your startup-config with the current running-config

A blue button labeled 'Setup Controller' is located at the bottom left of the configuration area.

9. Within this tab you can automate several configuration steps between the FortiConnect and the Fortinet Controller. Steps you previously took when setting up the client and SNMP will also be automated once you click on the **Setup Controller** button :-
- **FortiConnect Address** - Enter the Address of the FortiConnect
  - **Device IP Address** - Enter the IP Address of the controller, this is the IP address
  - **Admin User Name** - Enter the admin user name for the controller
  - **Admin Password** - Enter the admin password for the controller
  - **Configure RADIUS Profiles** - Check the box to Configure RADIUS profiles for authentication and account
  - **Set Captive portal RADIUS profiles** - Check the box to set captive portal RADIUS profiles



- **Set Captive portal mode** - Check the box to set the captive portal mode to customized
- **Configure QoS Rules** - Check the box to configure Pre Authentication QoS Rules
- **Transfer Pages to Controller** - Check the box to transfer portal redirection pages to controller
- **Configure SNMP** - Check the box to configure SNMP settings (only visible when SNMP has been enabled within the SNMP tab)
- **Write changes to startup-config** - Check this box to write the current controller running configuration to the startup-config file, this allows config to be retained between reboots.

10. Click on the **Setup Controller** button to apply the selection confirmation to the controller.

11. Click on the **Download portal pages** link for manual upload to the RADIUS client

12. Configuration of the settings above do not include configuration of **ESS** and **Security Profile** on the Fortinet Controller, the sections below will detail how to do this.

**Note: System Director 6.0 & Later** - for versions of System Director 6.0 and later we configure the Captive Portal External URL with a redirection URL pointing to the FortiConnect. Also, Automatic Setup no longer requires you to Transfer Custom Portal Pages from the FortiConnect to the controller, Set the Captive Portal Mode to Customized and Set the Captive Portal Authentication Method to Internal as shown in the screenshot below.

Identity Manager Address:   
This hostname is used to redirect guests to the Identity Manager, it should match the SSL certificate on Identity Manager.

Device IP Address:

Admin user name:

Admin Password:

Configure RADIUS profiles:

Set Captive Portal RADIUS profiles:

Set Captive Portal External URL:

Configure QoS Rules:

Write changes to startup-config:  This will overwrite your startup-config with the current running-config

# Manually Configuring the Fortinet Controller to authenticate against FortiConnect

---

## ***Adding the FortiConnect as a RADIUS Server***

You can manually configure the Fortinet Controller to authenticate against the FortiConnect. The first step is to configure the FortiConnect as a RADIUS server to allow the Fortinet Controller to authenticate users using RADIUS against the FortiConnect.

### RADIUS for Authentication

1. Login to the admin interface of the Fortinet Controller
2. Navigate to **Configuration > Security > Radius**
3. Click **Add**
4. Enter the **RADIUS Profile Name** as **IDM-Auth**
5. Enter a **Description**
6. Enter the **RADIUS IP** as the **IP address of your FortiConnect**
7. Enter the **RADIUS Secret** to match the value you entered on the FortiConnect.
8. Enter the **RADIUS Port** as **1812**
9. Set the **MAC Address Delimiter** to **Hyphen (-)**
10. Enter the **Password Type** as **Shared Key**
11. Click **OK**

## RADIUS Profile Table - Add

RADIUS Profile Name	<input type="text" value="IDM-Auth"/>	Enter 1-16 chars., <b>Required</b>
Description	<input type="text" value="Manager Authentication"/>	Enter 0-128 chars.
RADIUS IP	<input type="text" value="10"/> . <input type="text" value="10"/> . <input type="text" value="10"/> . <input type="text" value="200"/>	
RADIUS Secret	<input type="password" value="••••••"/>	
RADIUS Port	<input type="text" value="1812"/>	Valid range: [1024-65535]
MAC Address Delimiter	<input type="text" value="Hyphen (-)"/>	
Password Type	<input type="text" value="Shared Key"/>	

### RADIUS for Accounting

1. Navigate to **Configuration > Security > Radius**
2. Click **Add**
3. Enter the **RADIUS Profile Name** as **IDM-Acct**
4. Enter a **Description**
5. Enter the **RADIUS IP** as the **IP address of your FortiConnect**
6. Enter the **RADIUS Secret** to match the value you entered on the FortiConnect.
7. Enter the **RADIUS Port** as **1813**
8. Set the **MAC Address Delimiter** to **Hyphen (-)**
9. Click **OK**

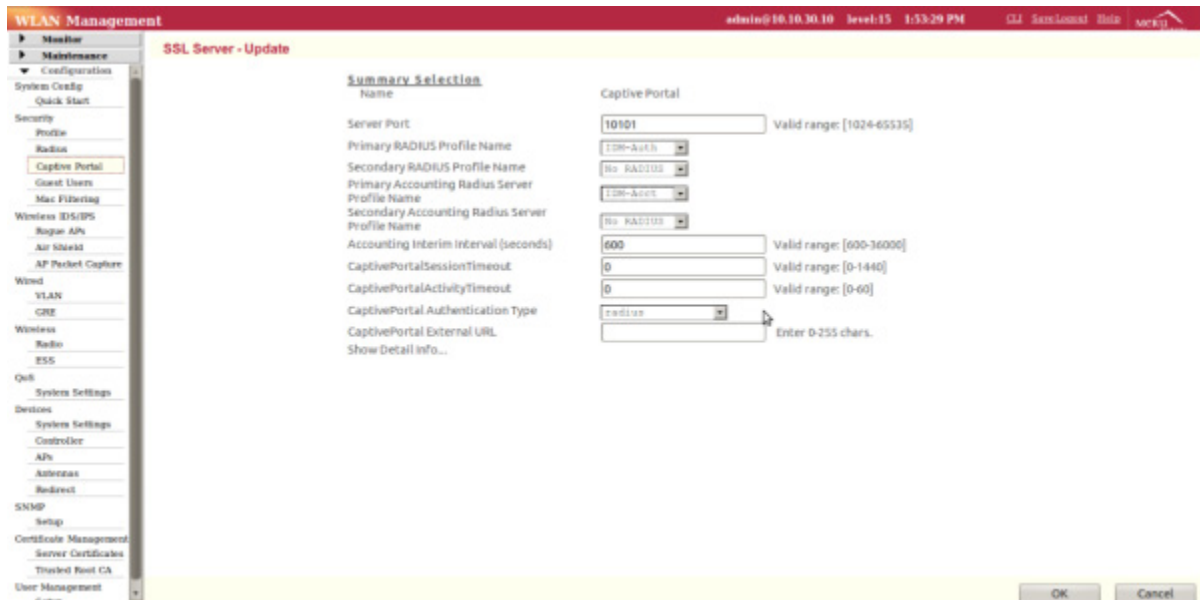
## RADIUS Profile Table - Add

RADIUS Profile Name	<input type="text" value="IDM-Acct"/>	Enter 1-16 chars., <b>Required</b>
Description	<input type="text" value="ity Manager Accounting"/>	Enter 0-128 chars.
RADIUS IP	<input type="text" value="10"/> . <input type="text" value="10"/> . <input type="text" value="10"/> . <input type="text" value="200"/>	
RADIUS Secret	<input type="password" value="••••••"/>	
RADIUS Port	<input type="text" value="1812"/>	Valid range: [1024-65535]
MAC Address Delimiter	<input type="text" value="Hyphen (-)"/>	
Password Type	<input type="text" value="Shared Key"/>	

### Configure RADIUS Authentication for Captive Portals

Once you have added the FortiConnect as a RADIUS server you need to tell the Fortinet Controller to use these RADIUS servers for web authentication.

1. Navigate to **Configuration > Security > Captive Portal**
2. Set the **Primary RADIUS Profile Name** to **IDM-Auth**
3. Set the **Primary Accounting Radius Server Profile Name** to **IDM-Acct**
4. Set the **Captive Portal Authentication Type** to **radius**
5. Click **OK**



## Configure the Security Profile for Captive Portal

To enable the captive portal you need to change the security profile for the ESS profile that you want to use for user access.

In the following configuration example we will modify the default Security Profile, and create a new ESS profile which uses it.

### Configure the Security Profile

1. Navigate to **Configuration > Security > Profile**
2. Check the default Security Profile and click **Settings**
3. Change the **Captive Portal** setting to **WebAuth**
4. Set the **Captive Portal Authentication Method** to **internal**
5. Click **Ok**.

## Security Profile Table - Update

### Summary Selection

Profile Name

idm

L2 Modes Allowed

Clear  802.1x  Static WEP keys  WPA  
 WPA PSK  WPA2  WPA2 PSK  MIXED  
 MIXED\_PSK

Data Encrypt

WEP64  WEP128  TKIP  CCMP-AES  
 CCMP/TKIP  Clear

Primary RADIUS Profile Name

No RADIUS

Secondary RADIUS Profile Name

No RADIUS

WEP Key (Alphanumeric/Hexadecimal)

Static WEP Key Index

1 Valid range: [1-4]

Re-Key Period (seconds)

0 Valid range: [0-65535]

Captive Portal

WebAuth

Captive Portal Authentication Method

internal

802.1X Network Initiation

Off

### Create an ESS

1. Navigate to **Configuration > Wireless > ESS**
2. Add a new ESS by clicking the **Add** button
3. Set the **ESS Profile Name** and **SSID** to **guestnetwork**
4. Set the **Security Profile Name** to **default**
5. Click **Add**

## ESS Profile - Add

ESS Profile Name	<input type="text" value="guestnetwork"/>	Enter 1-32 chars., R
Enable/Disable	<input type="button" value="Enable"/> ▾	
SSID	<input type="text" value="guestnetwork"/>	Enter 0-32 chars.
Security Profile Name	<input type="button" value="idm"/> ▾	
Primary RADIUS Accounting Server	<input type="button" value="No RADIUS"/> ▾	
Secondary RADIUS Accounting Server	<input type="button" value="No RADIUS"/> ▾	
Accounting Interim Interval (seconds)	<input type="text" value="3600"/>	Valid range: [600-3600]
Beacon Interval (msec)	<input type="text" value="100"/>	Valid range: [20-1000]
SSID Broadcast	<input type="button" value="On"/> ▾	
Bridging	<input type="checkbox"/> AirFortress <input type="checkbox"/> IPV6 <input type="checkbox"/> AppleTalk	
New AP's Join ESS	<input type="button" value="On"/> ▾	

You should now be able to authenticate a user with web authentication against the FortiConnect.

## SNMP Integration

For audit purposes you will want to know the IP address assigned to each of your users. The IP address of the user is also required for correlating the syslog messages from firewalls.

SNMP needs to be setup to obtain the IP address of the user from the Fortinet Controller as it isn't sent in the RADIUS Accounting messages (before System Director Release 5.1). When a user authenticates the FortiConnect receives the MAC address of user from the Fortinet Controller in the calling-station-id field. The FortiConnect then contacts the Fortinet Controller using SNMP to find the IP address for this device and fills in the Framed-IP-Address details in the RADIUS Accounting database.

## Configuring SNMP on the Fortinet Controller

The best way of setting up SNMP on the Fortinet Controller is to use the command line. This enables you to setup SNMP version 3 which supports authentication and encryption. SNMPv3 is also more efficient in terms of communication than SNMPv1. Only SNMP version 1 can be setup from the web interface on the Fortinet Controller.

To setup SNMP on the controller perform the following steps:

Connect to the command line of the controller, using the console port, telnet or ssh. Login as the admin user.

1. Enter configuration mode by entering the following:

```
fortinet-mc1500(15)# configure terminal
```

2. Enter the SNMP global settings:

```
fortinet-mc1500(15)(config)# snmp-server contact admin@fortinet.com
```

```
fortinet-mc1500(15)(config)# snmp-server description fortinet_MC-1500_Controller
```

```
fortinet-mc1500(15)(config)# snmp-server location Manchester
```

3. Configure an SNMPv3 User:

```
fortinet-mc1500(15)(config)# snmpv3-user identitymanager
```

4. Setup the authentication and privacy protocols and passwords

```
fortinet-mc1500(15)(config-snmpv3-user)# auth-protocol md5-auth
```

```
fortinet-mc1500(15)(config-snmpv3-user)# auth-key 1Dent1ty
```

```
fortinet-mc1500(15)(config-snmpv3-user)# priv-protocol des-priv
```

```
fortinet-mc1500(15)(config-snmpv3-user)# priv-key 1Dent1ty
```

5. Setup the IP address of the FortiConnect that can connect to the Controller using SNMP

```
fortinet-mc1500(15)(config-snmpv3-user)# target-ip-address [FortiConnect IP address]
```

6. Finish configuration.

```
fortinet-mc1500(15)(config-snmpv3-user)# end
```

7. Lastly you need to start SNMP running on the controller:

```
fortinet-mc1500(15)# snmp start
```

8. You can verify that the snmp service is running by entering **snmp status**

SNMP is now configured correctly on the controller.



## Configuring SNMP on the FortiConnect

To enable the FortiConnect to use SNMP to fill in missing Framed-IP-Address for RADIUS clients you need to enable SNMP on each RADIUS client.

Perform the following steps to enable SNMP for the FortWLC:

1. From the FortiConnect Administration interface navigate to **Devices > RADIUS Clients**
2. Select the Fortinet Controller from the list of devices.
3. Select the SNMP tab

**RADIUS Clients**

Client | Attributes | **SNMP** | MAC Authentication | RadSec Authentication | Automatic Setup

SNMP is used for recording the Framed-IP-Address of the guest when the RADIUS client does not set this in RADIUS accounting messages. You do not need to enable this if the device sets it correctly.

Enable:

Alternative SNMP device IP Address:  If the RADIUS Client doesn't support SNMP access to the ARP table, query this device instead

Version: **V3** V2: & V3 perform better than V1

Read Community:

Authentication Protocol: **MD5**

Authentication Username:

Authentication Passphrase:  Confirm:

Privacy Protocol: **DES**

Privacy Passphrase:  Confirm:

Security Type: **Authentication**

4. Check the **Enable** checkbox
5. Set the **Version** to **V3**
6. Select the **Authentication Protocol** as **MD5**
7. Enter the **Authentication Username** as **identitymanager**
8. Set the **Authentication Passphrase** to **1Dent1ty** and **Confirm** it

9. Set the Privacy Protocol to DES
10. Set the Privacy Passphrase to 1Dent1ty and Confirm it
11. Set the Security Type to Encryption
12. Click Save.

Now that you have enabled SNMP every minute after a user has logged in the FortiConnect will obtain their IP address from the Fortinet Controller and record it in the RADIUS Accounting record.

# Using FortiConnects Portals with Fortinet Controllers

---

## Allowing access to the FortiConnect

To allow traffic to reach the FortiConnect so that it can be used as the external portal you need to have the Personal Enforcement Firewall feature enabled on the controller and then setup QoS rules to allow the traffic through

### ***Controller Qos Rules***

Configure the 2 QOS rules one for incoming and other for outgoing traffic to the FortiConnect. At this point you should have the FortiConnects system's Ip address and the corresponding Port number is 443 for HTTPS.

### ***To add the QOS Rules***

1. Click on the **Configuration Panel-->QOS-->System Settings**.
2. Click on **QOS and Firewall Rules** Tab as shown in the figure below.
3. Click on the **ADD** button below as shown in the figure below



## QoS and Firewall Rules (18 entries)

Global Quality-of-Service Parameters		QoS and Firewall Rules			QoS Codec Rules		
<input type="checkbox"/>	ID	Destination IP	Destination Netmask	Destination Port	Source IP	Source Netmask	Source Port
<input type="checkbox"/>	3	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0
<input type="checkbox"/>	4	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	5060
<input type="checkbox"/>	7	0.0.0.0	0.0.0.0	5200	0.0.0.0	0.0.0.0	0
<input type="checkbox"/>	8	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	5200
<input type="checkbox"/>	119	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	0
<input type="checkbox"/>	10	10.0.0.0	255.0.0.0	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	11	172.27.0.0	255.255.192.0	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	13	172.26.0.0	255.255.192.0	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	14	172.27.0.0	255.255.192.0	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	15	172.26.0.0	255.255.192.0	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	16	0.0.0.0	0.0.0.0	4500	0.0.0.0	0.0.0.0	4500
<input type="checkbox"/>	27	10.0.0.10	255.255.255.255	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	26	10.0.0.0	255.0.0.0	0	192.168.37.0	255.255.255.0	0
<input type="checkbox"/>	28	192.168.34.0	255.255.255.0	0	0.0.0.0	0.0.0.0	0
<input type="checkbox"/>	1	0.0.0.0	0.0.0.0	1720	0.0.0.0	0.0.0.0	0
<input type="checkbox"/>	2	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1720
<input type="checkbox"/>	30	192.168.34.20	255.255.255.255	443	0.0.0.0	0.0.0.0	0
<input type="checkbox"/>	31	0.0.0.0	0.0.0.0	0	192.168.34.20	255.255.255.255	443

## Add a QoS Rule for Destination Traffic

Once you have clicked the **Add** button, you will see the screen below.

### QoS and Firewall Rules - Add

ID	<input type="text"/>	Valid range: [0-600]
Destination IP	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	
Destination Netmask	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	
Destination Port	<input type="text" value="0"/>	Valid range: [0-655]
Source IP	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	
Source Netmask	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	
Source Port	<input type="text" value="0"/>	Valid range: [0-655]
Network Protocol	<input type="text" value="0"/>	Valid range: [0-255]
Firewall Filter ID	<input type="text"/>	Enter 0-16 chars.
Packet minimum length	<input type="text" value="0"/>	Valid range: [0-150]
Packet maximum length	<input type="text" value="0"/>	Valid range: [0-150]
QoS Protocol	<input type="text" value="SIP"/>	
Average Packet Rate	<input type="text" value="0"/>	Valid range: [0-200]
Action	<input type="text" value="FORWARD"/>	
Drop Policy	<input type="text" value="Tail"/>	
Token Bucket Rate	<input type="text" value="0"/> <input checked="" type="checkbox"/> Kbps <input type="checkbox"/> Mbps	
Priority	<input type="text" value="0"/>	Valid range: [0-8]
Traffic Control	<input type="text" value="Off"/>	
DiffServ Codepoint	<input type="text" value="DiffServ Disabled"/>	

Configure the following with



1. ID should be a unique number not used for any other rule.
2. **Destination IP address** should be the **FortiConnects IP address**, The **Net Mask** should be 255.255.255.255. Select the check box in the **Match** column next to it.
3. Set the **Destination port** to 443. Select the check box in the **Match** column next to it.
4. Set the **Network Protocol** to 6. Select the check box in the **Match** column next to it.
5. Enter **Firewall Filter ID** ensuring there are no spaces (use a name such as IdentityManager) and select the check box in the **Match** column next to it.
6. Select the **QOS protocol** as other.
7. Once done click on **OK**

Similarly Add a QOS Rule for Source Traffic

To Configure the Source Rule follow the steps below:

1. Click on **ADD**
1. ID should be a unique number not used for any other rule.
2. **Source IP address** should be the **FortiConnects IP address**, The **Net Mask** should be 255.255.255.255. Select the check box in the **Match** column next to it.
3. Set the **Source port** to 443. Select the check box in the **Match** column next to it.
4. Set the **Network Protocol** to 6, Select the check box in the **Match** column next to it.
5. Enter **Firewall Filter ID** (give same name as given above for destination traffic) and select the check box in the **Match** column next to it.
6. Select the **QOS protocol** as others.
7. Once done click on **OK**

Once the above steps are completed you will get a screen as shown below

<input type="checkbox"/> 	30	192.168.34.20	255.255.255.255	443	0.0.0.0	0.0.0.0	0	6
<input type="checkbox"/> 	31	0.0.0.0	0.0.0.0	0	192.168.34.20	255.255.255.255	443	6

## Security Profile

To configure a security profile for the FortiConnect portal authentication follow the following steps: click **Configuration > Security > Profile**. Then you will get a Security profile table with list security profiles if configured. Click on **ADD** as shown in the figure below

## Security Profile Table - Add

Security Profile Name	<input type="text" value="idm-security"/>	Enter 1-32 chars., R
L2 Modes Allowed	<input checked="" type="checkbox"/> Clear <input type="checkbox"/> 802.1x <input type="checkbox"/> Static WEP keys <input type="checkbox"/> WPA <input type="checkbox"/> WPA PSK <input type="checkbox"/> WPA2 <input type="checkbox"/> WPA2 PSK <input type="checkbox"/> MIXED <input type="checkbox"/> MIXED_PSK	
Data Encrypt	<input type="checkbox"/> WEP64 <input type="checkbox"/> WEP128 <input type="checkbox"/> TKIP <input type="checkbox"/> CCMP-AES <input type="checkbox"/> CCMP/TKIP <input type="checkbox"/> Clear	
Primary RADIUS Profile Name	<input type="text" value="No RADIUS"/>	
Secondary RADIUS Profile Name	<input type="text" value="No RADIUS"/>	
WEP Key (Alphanumeric/Hexadecimal)	<input type="text"/>	
Static WEP Key Index	<input type="text" value="1"/>	Valid range: [1-4]
Re-Key Period (seconds)	<input type="text" value="0"/>	Valid range: [0-65535]
Captive Portal	<input type="text" value="WebAuth"/>	
Captive Portal Authentication Method	<input type="text" value="internal"/>	
802.1X Network Initiation	<input type="text" value="On"/>	

Configure a security profile for the External Captive Portal as shown below,

1. Enter a name to the Security Profile
2. Select Captive Portal to WebAuth
3. Select Captive Portal Authentication method to internal
4. Set the Passthrough Firewall Filter ID to the same name as the Firewall Filter ID defined in the QOS rule.

## Uploading Custom Portal Pages

This section details how to upload the custom portal pages to the FortWLC.

1. To upload the pages Manually, go to Devices --> RADIUS Clients and click on the Automatic Setup Tab as shown below.

Client Attributes SNMP MAC Authentication RadSec Authentication **Automatic Setup**

Identity Manager Address:   
This hostname is used to redirect guests to the Identity Manager, it should match the SSL certificate on Identity Manager.

Device IP Address:

Admin user name:

Admin Password:

Configure RADIUS profiles:

Set Captive Portal RADIUS profiles:

Set Captive portal mode:

Configure QoS Rules:

Transfer pages to controller:

Write changes to startup-config:  This will overwrite your startup-config with the current running-config

[Download portal pages](#) for manual upload to the RADIUS client.

2. Click on the **Download Portal Pages** link and this will download a .zip file containing the pages which you can then manually upload to the controller.
3. To manually upload go to **Maintenance-->Captive Portal** on the FortWLC and click on the **Import File** link.



## Import File

### Step 1

#### Select a File

- Clicking the **Browse...** button allows to choose the file you wish to Import.
- Only Files with the extensions: **.html, .gif, .jpg, .png, .bmp, .css, .js** are allowed.
- The extension defines the content of the file to be imported.

### Step 2

#### Import the selected File

- Click **Import File** button to start the Import Process.
- 

4. Click on **Choose File** and select the pages that are in the .zip file.
5. Then browse to your FortWLC and select **Maintenance-->Captive Portal** and click on the **Customization** link as shown below.

## Captive Portal Customization

### Step 1

#### Select a Mode

Captive Portal has 2 Modes of Operation: **Default** and **Customized**

- **Default Mode:** HTML documents are generated at installation and the user cannot change the
- **Customized Mode:** The login page and other GUI elements are served from a custom directory
  - Get Files Downloads the HTML pages which can be customized **(.html)**.
  - Delete Files Erase the custom directory **(.gif, .jpg, .png, .bmp, .css, .js, .html, .pl)**.
  - Restore Default The custom directory is restored to the installation content **(.html)**.
  - To test the customization:
    1. Import the customized file(s) **(.gif, .jpg, .png, .bmp, .css, .js, .html, .pl)**
    2. Type the test URL **https://controller/vpn/customfile.html**
    3. See Online Help for more information

### Step 2

#### Change the Mode

6. Set the Mode Selection to Customized and click "Change Mode"

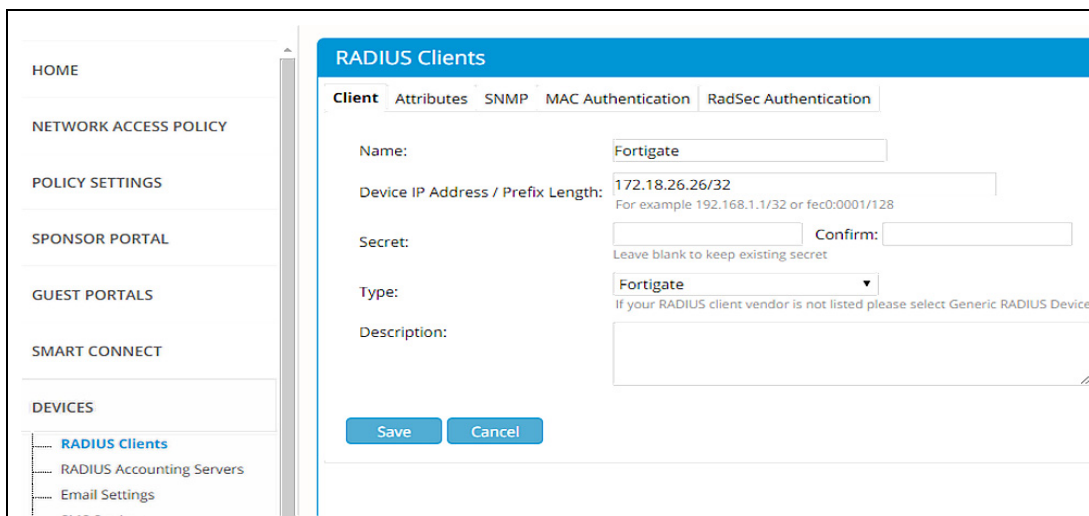
## Add Fortigate as a RADIUS server

---

Fortigate can be added as a Radius client in FortiConnect. However, there are following limitations:

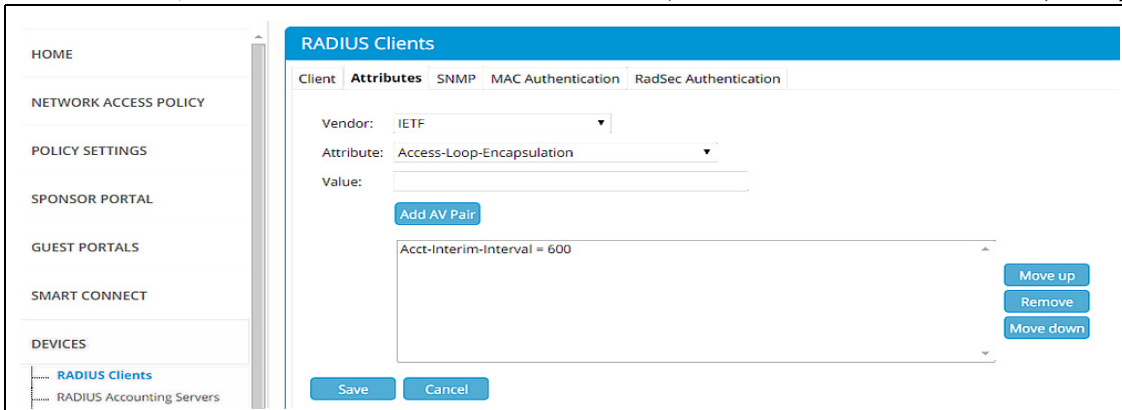
- Device Authentication feature will not work as Fortigate does not send NAS IP Address/Called-Station-Id parameters.
- OAuth feature is supported only if the required host names are in the allowed list on FortiGate. This enables client redirection to the OAuth provider site for authentication.
- As Fortigate does not send AP name and AP id some guest reports and accounting logs will have empty fields against them.
- Redirection URL after successful guest authentication **must** be set in Fortigate configuration.
- In Mac / iPad, when using Safari to perform guest authentication, intermittently the browser will timeout or will take long time to redirect to the portal success page.

To integrate, start by creating a RADIUS client entry of type **Fortigate**. Provide Fortigate server IP address.



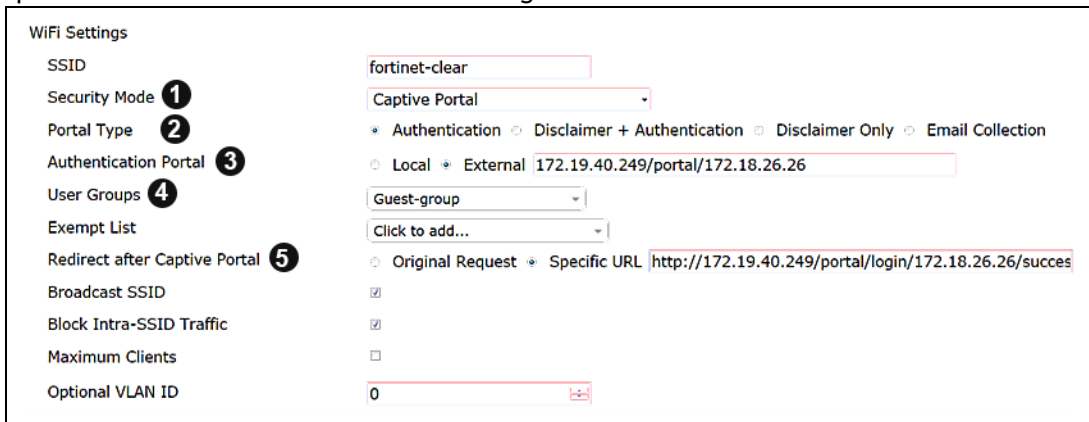
The screenshot displays the 'RADIUS Clients' configuration interface. On the left, a navigation menu includes 'HOME', 'NETWORK ACCESS POLICY', 'POLICY SETTINGS', 'SPONSOR PORTAL', 'GUEST PORTALS', 'SMART CONNECT', and 'DEVICES'. Under 'DEVICES', 'RADIUS Clients' is selected. The main content area shows the configuration form for a RADIUS client. The 'Client' tab is active, and the 'Name' field contains 'Fortigate'. The 'Device IP Address / Prefix Length' field contains '172.18.26.26/32'. The 'Secret' field is empty, and the 'Confirm' field is also empty. The 'Type' dropdown menu is set to 'Fortigate'. The 'Description' field is empty. There are 'Save' and 'Cancel' buttons at the bottom of the form.

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



After you have completed configuring Fortigate server details in the FortiConnect server, log in to your Fortigate server and do the following to complete the integration.

**Step 1** In the Fortigate server WebUI, go to **WiFi Controller > SSID**. Create a new SSID and ensure that you provide details as listed after the following screenshot.



1. Set **Security Mode** to *Captive Portal*.

2. Select **Portal Type** as *Authentication*.

3. Enter the **Authentication Portal** address in this format: *<FortiConnect-serverIP>/portal/Fortigate-serverIP>*.

For example, if FortiConnect server IP is 172.19.40.249 and Fortigate server IP is 172.18.26.26, then your IP address is 172.19.40.249/portal/172.18.26.26.

4. Provide a destination URL to **Redirect after Captive Portal authentication**.

**Step 2** Go to **Wifi Controller > FortiAP Profiles** and create or edit a profile. In the profile, set the SSID of each radio to the SSID created in step 1.

Select Channel Width: 20MHz

Channel:  36  40  44  48  149  153  157  161  165

Auto TX Power Control:  Disable  Enable

TX Power: 100 %

SSID: **forti-clear (SSID: fortinet-clear)**

**Radio 2**

Mode

Spectrum Analysis

WIDS Profile: Click to set...

Radio Resource Provision

Client Load Balancing:  Frequency Handoff  AP Handoff

Band: 2.4GHz 802.11n/g/b

Channel:  1  2  3  4  5  6  7  8  9  10  11

Auto TX Power Control:  Disable  Enable

TX Power: 100 %

SSID: **forti-clear (SSID: fortinet-clear)**

Cancel

**Step 3** Go to **Policies and Objects > Objects > Addresses**. Create a new entry with a name for the FortiConnect Server and its IP address.

Name: Meru Connect RADIUS

Type: IP/Netmask

Subnet / IP Range: 172.18.26.26/255.255.255.255

Interface: any

Show in Address List:

Comments: 0/255

OK Cancel

**Step 4** Go to Policies and Objects > Policy > IPv4. Create the following rules:

Seq.#	From	To	Source	Destination	Schedule	Service	Action	NAT	SSL Inspection	Log	Count
1	any	forti-clear (SSID: fortinet-clear)	Meru Connect	all	always	ALL	ACCEPT Enable	Enable	All	0 Packets / 0 B	
2	forti-clear (SSID: fortinet-clear)	any	all	Meru Connect	always	ALL	ACCEPT Enable	Enable	All	96,893 Packets / 57.75 MB	
3	any	any	all	all	always	DNS DHCP	ACCEPT Enable	Enable	All	62,194 Packets / 6.37 MB	
4	forti-clear (SSID: fortinet-clear)	any	all Guest-group	all	always	ALL	ACCEPT Enable	UTM	All	2,053 Packets / 1.15 MB	

**Step 5** Go to User & Device > Authentication > RADIUS Servers. Create a new entry of the FortiConnect server. The secret key entered here should be used while adding the Fortigate server in FortiConnect. Ensure that you enter the Fortigate server IP address as the **NAS IP / Called Station ID**.

Name	Meru Connect RADIUS
Primary Server IP/Name	172.19.40.249
Primary Server Secret	●●●●●●●● <span>Test Connectivity</span>
Secondary Server IP/Name	<input type="text"/>
Secondary Server Secret	<input type="text"/> <span>Test Connectivity</span>
Authentication Method	<input checked="" type="radio"/> Default <input type="radio"/> Specify
NAS IP / Called Station ID	172.18.26.26 <span>← This Fortigate Server IP</span>
Include in every User Group	<input checked="" type="checkbox"/>
<span>OK</span> <span>Cancel</span>	

**Step 6** Now, go to the Fortigate CLI, and execute the following commands to complete the integration:

Allow external web access

```
# set captive portal exempt enable
```

Configure accounting time interval

```
# set acct-interim-interval [duration] (between 600 - 86400 seconds)
```

Configure FortiConnect as the Radius accounting server

```
# config accounting-server
```

```
# edit 1
```

```
# set status enable
```

```
# set server <IP Address of FortiConnect>
```

```
# Set secret <Secret>
```

# Backup and Restore

You should backup the FortiConnect on a regular basis so that in the event of a hardware failure you do not lose critical data. The FortiConnect 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 FortiConnect or a remote FTP server.

This chapter includes the following sections:

- Configuring Backup
- Restoring Backups

## Configuring Backup

---

This section describes the following

- Setting Backup Settings
- Taking Snapshots
- Scheduling Backups

## Setting Backup Settings

---

1. From the administration home page, select **Server > Backup/Restore** as shown below.

The screenshot shows the 'Backup/Restore' configuration page. The 'Backup Settings' tab is selected. The form includes the following fields and controls:

- Backup Type:** A dropdown menu set to 'FTP and local backup'.
- Server:** An empty text input field.
- Port:** A text input field containing '21'.
- Passive Mode:** A checked checkbox.
- Directory:** An empty text input field.
- Username:** An empty text input field.
- Password:** A text input field.
- Confirm:** A text input field for password confirmation.
- Max number of server backups:** An empty text input field with a note: 'Leave blank for unlimited backup files'.

At the bottom of the form are three buttons: 'Save', 'Cancel', and 'Test Remote Backup'. Below the form is a 'Snapshot' section with a 'Download: Snapshot' button.

2. To perform the backup to a remote FTP server, click the **Backup Settings** tab:
  - Enter the **Remote Server Address** for the FTP server.
  - Enter the **TCP Port** to be used (usually port 21).
  - Enter the **Directory** to store the backup.
  - Enter a **Username** and **Password** (confirming the password) that allows access to the FTP server.
  - Selecting the **Mode is Passive** box activates **passive** for the FTP Mode. Leaving it unchecked keeps this inactive.
3. Click the **Save Settings** button to save the backup settings.

## Taking Snapshots

---

You can save a point-in-time snapshot to allow you to download a backup of the FortiConnect at an exact moment.

1. From the administration home page, select **Server > Backup/Restore** and select the **Backup Settings** tab.
2. To save a snapshot backup, click the **Snapshot** button at the bottom of the form.



3. You are prompted by your web browser to save the backup file to disk.

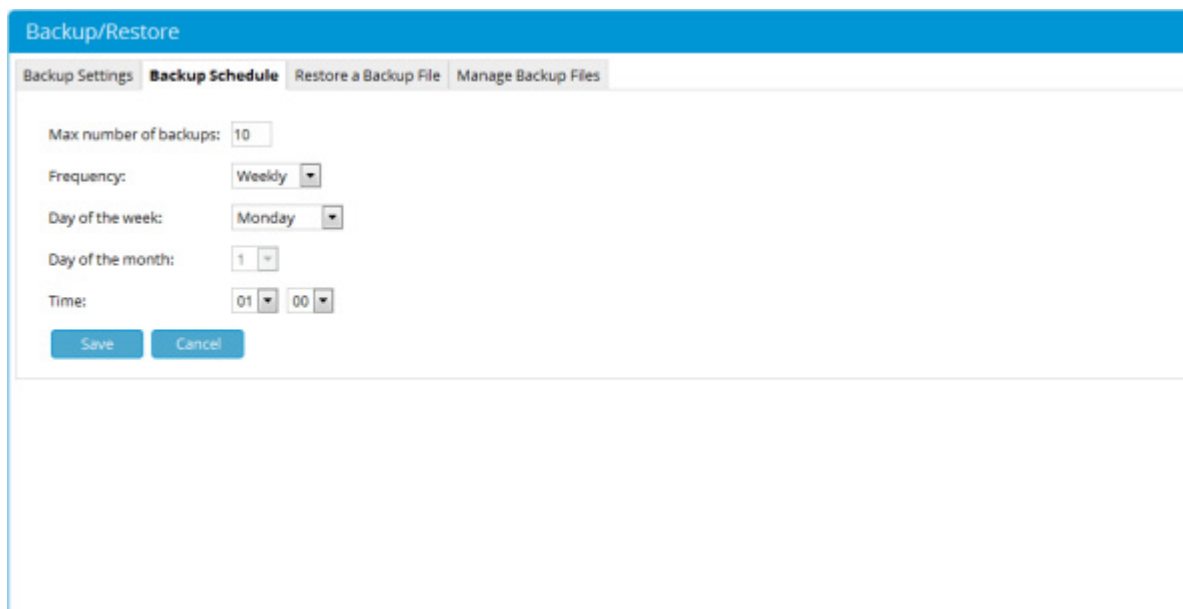
**Note:** You will receive a warning in your 'Audit Log' messages if there is insufficient disk space to complete the operation. The default disk space requirement is 40% of the database.

## Scheduling Backups

---

You can schedule backups to occur every day, week, or month at 1:00 AM. Scheduled backups are stored in either the /guest/backup directory of the FortiConnect or on a remote FTP server.

1. From the administration home page, select **Server > Backup/Restore** and select the **Backup Schedule** tab as shown below.



The screenshot shows the 'Backup/Restore' configuration page. The 'Backup Schedule' tab is selected. The configuration fields are as follows:

- Max number of backups: 10
- Frequency: Weekly
- Day of the week: Monday
- Day of the month: 1
- Time: 01:00

Buttons for 'Save' and 'Cancel' are visible at the bottom of the configuration area.

2. To perform local backups:

- Enter the Maximum number of backups that you want to save. The FortiConnect removes old backups that exceed this amount by discarding the oldest backup when new ones are created. Note - If you do not want to limit the number of files, you can specify a number less than 1, for example, 0 or -1.
- Specify how often you want the FortiConnect to perform backups in the Frequency dropdown menu. You can specify 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:** Fortinet recommends specifying a date between the 1st and 28th day of the month to ensure that you automatically back up your system every month of the year.

3. Click the **Save Settings** button to save settings.

**Note:** You will receive a warning in your 'Audit Log' messages if there is insufficient disk space to complete the operation. The default disk space requirement is 40% of the database.

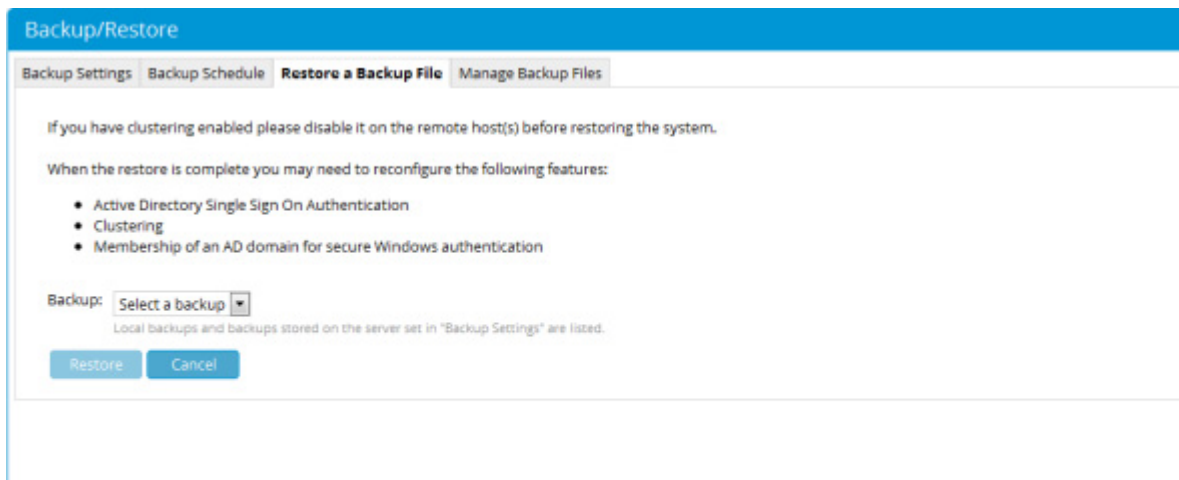
## Restoring Backups

---

You can restore a backup to the FortiConnect from the administration interface.

**Note:** Since FortiConnect 17.0 operates exclusively on a 64-bit OS, direct upgrade from FortiConnect 16.9 and older versions cannot be performed. Hence, you are required to migrate data from 16.9 to 17.0 and to facilitate this, restore a backup from version 16.9 onto an appliance running 17.0 using this procedure.

1. From the administration home page, select **Server > Backup/Restore** and click the **Restore a Backup File** tab as shown below.



The screenshot shows the 'Backup/Restore' configuration page in FortiConnect. The 'Restore a Backup File' tab is selected. The page contains the following elements:

- Navigation tabs: Backup Settings, Backup Schedule, **Restore a Backup File**, Manage Backup Files.
- Warning text: "If you have clustering enabled please disable it on the remote host(s) before restoring the system."
- Instruction: "When the restore is complete you may need to reconfigure the following features:"
- Feature list:
  - Active Directory Single Sign On Authentication
  - Clustering
  - Membership of an AD domain for secure Windows authentication
- Backup selection: A dropdown menu labeled "Backup:" with the text "Select a backup" and a downward arrow.
- Footnote: "Local backups and backups stored on the server set in 'Backup Settings' are listed."
- Buttons: "Restore" and "Cancel".

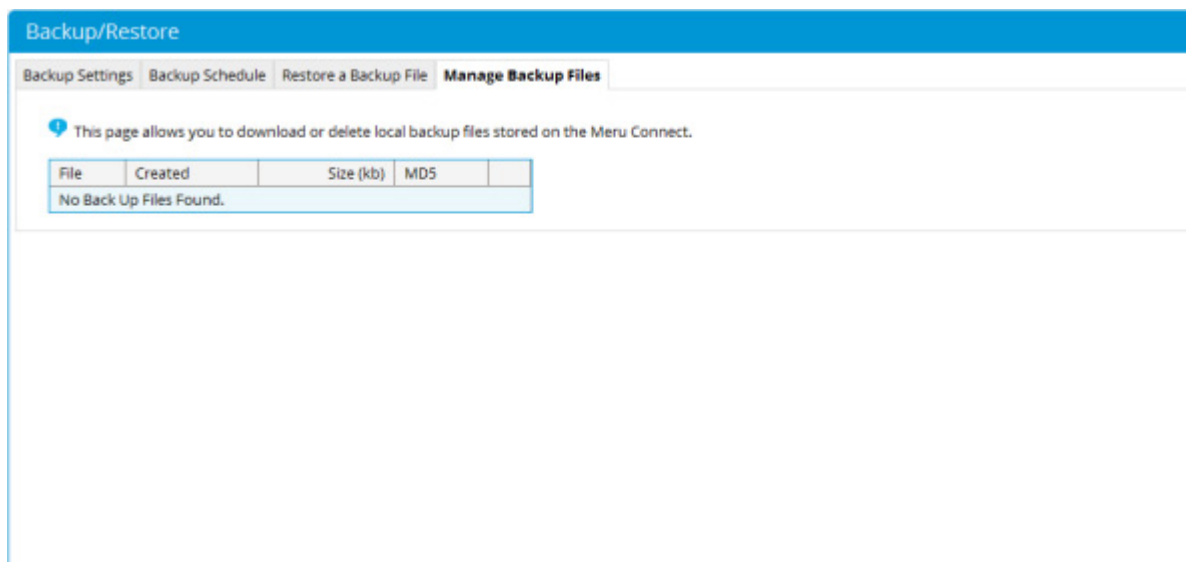
2. From the **Backup** dropdown menu select the backup archive you want to restore.
3. Click the **Restore** button.
4. The backup is uploaded to the FortiConnect and the data is restored. Once the data has been restored, the server will reboot so that the database is correctly loaded.

## Manage Backups

---

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

1. From the FortiConnect Administration interface select **Server --> Backup/Restore** and click on the **Manage Backup Files** tab as shown below.



2. From here you can click on the **Download** icon to save a file locally, or click on the **Bin** icon to delete the file.



# 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 the FortiConnect's in-built 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 these large number of devices.

Smart Connect solution allows you to create and apply different policies to a device based on the identified device type after it classifies the device. Hence, 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

the FortiConnect to automatically setup the settings, username, password and any certificates that you require.

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. Once a user is authenticated and authorized, FortiConnect applies Smart Connect Policy rules on that user to find the appropriate Smart Connect Profile for that user to connect to the secure network.

All policies are checked in a specific order, defined by the Administrator, if a policy is matched then the remaining policies are ignored. If no policy gets matched then the Default Smart Connect Policy is applied.

This section details how to use the setup wizard within FortiConnect to enable Smart Connect.

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 Profile

---

Create a Smart Connect Profile defining your network type and authentication settings for client in your network.

To add a Network Profile for Smart Connect go to the **Smart Connect --> Smart Connect Profiles** section on the FortiConnect administrative console and click **Add**. The **Smart Connect Profile Wizard** appears.

Click on **Next** to begin configuring the profile. The following settings are configured in a Smart Connect profile.

- Network Settings
- Authentication
- Proxy Settings
- Certificates
- Additional Certificates
- Other Options

## Network Settings

Update the basic configurations of your network in this tab.

1. Enter a unique **Network Name** for your network.
2. Select the applicable **Network Type**.
  - **Wired** - If it is a wired network then no further information is required, click on **Next** to continue.
  - **Wireless** - If it is a wireless network then update the following.
    - Enter the **SSID** name.
    - Place a check in the checkbox if the SSID is broadcast.
    - Optionally, you can specify the SSIDs you wish to remove from the client. This may be required for any open network where client access is to be restricted.

Smart Connect Profile Wizard

✓ Welcome

★ Network Settings

Authentication

Proxy Settings

Certificates

Additional Certificates

Other Options

### Network Settings

Please provide a name and type for the network.

Network Name: MyNetwork

Network Type:  wired  wireless

SSID: SSID123

SSID is Broadcast:

#### Remove SSIDs

Please enter the SSIDs that you would like to remove from the client.  
It is advisable to remove the SSIDs for any open networks that you don't want the client to automatically connect to.

< Back Next >

3. Click on **Next** to continue.

## Authentication

Based on the network type that you specify in the previous tab, you are provided the authentication methods. If in the **Network Settings** page you selected a **wireless** network type, then there are two main types of authentication methods to choose from, **Enterprise** and **Pre-Shared Key**, depending on the option you choose you will be required to enter different credentials.

If you select **WPA**, **WPA2**, or **WPA/WPA2 Enterprise** authentication method, update the following.

1. Using the drop down menu select an **EAP Type** for authentication for different client devices, **Windows**, **Apple iOS**, **Android**, **Linux**, and **Chrome OS**. EAP-TLS and PEAP cannot be configured automatically for Windows XP.
2. Determine in the **Include Credentials** option whether you want to include or not include the user name and password in the profile sent to the user.
3. Select a specific user name format for the client to **Authenticate with**. If you select realm, then define the realm.
4. Select the **Detect and override username format when authenticating against Active Directory** based on your requirement.
5. If your EAP Type is **EAP-TLS** then use the drop down menu to select where to generate certificates from. Details on how to do this are at the bottom of the Smart Connect Section under SCEP Server and User Certificate Authority.

**Smart Connect Profile Wizard**

- ✓ Welcome
- ✓ Network Settings
- ★ **Authentication**
- Proxy Settings
- Certificates
- Additional Certificates
- Other Options

### Authentication

Please provide the authentication details for the network.

Authentication: WPA/WPA2 Enterprise  
Windows systems will use WPA2

EAP Type:

Windows	PEAP/MSCHAPv2
Apple iOS / OS X	PEAP/MSCHAPv2 and PEAP/GTC
Android	PEAP/GTC
Linux	PEAP/GTC
Chrome OS	PEAP/MSCHAPv2

---

**PEAP/MSCHAPv2 and PEAP/GTC**

Include Credentials:  Include username/password in profile sent to user  
 Don't include username/password in profile sent to user

Authenticate with:  realm/username  
 realm/username  
 username@realm  
 username

Realm:

Detect and override username format and realm when authenticating against Active Directory:

If selecting a Pre-Shared Key option then your options differ as shown below.

If you select **Pre-Shared Key** authentication method, enter the Pre-Shared Key in the field provided and click the **show** box if you wish to display this. When WPA/WPA2 is selected as the pre-shared key, Windows uses WPA2.

**Smart Connect Profile Wizard**

- ✓ Welcome
- ✓ Network Settings
- ★ **Authentication**
- Proxy Settings
- Certificates
- Additional Certificates
- Other Options

### Authentication

Please provide the authentication details for the network.

Authentication: WPA-Pre-Shared Key

Pre-Shared Key:

If in the **Network Settings** page you selected a **wired** network type, then only **802.1X** authentication method is available.

When **802.1X** authentication method, update the following.



1. Using the drop down menu select an **EAP Type** for authentication for different client devices, **Windows, Apple iOS, Android, Linux, and Chrome OS**. EAP-TLS and PEAP cannot be configured automatically for Windows XP.
2. Determine in the **Include Credentials** option whether you want to include or not include the user name and password in the profile sent to the user.
3. Select a specific user name format for the client to **Authenticate with**. If you select realm, then define the realm.
4. Select the **Detect and override username format when authenticating against Active Directory** based on your requirement.
5. If your EAP Type is **EAP-TLS** then use the drop down menu to select where to generate certificates from. Details on how to do this are at the bottom of the Smart Connect Section under SCEP Server and User Certificate Authority.

**Smart Connect Profile Wizard**

- ✓ Welcome
- ✓ Network Settings
- ★ **Authentication**
- Proxy Settings
- Certificates
- Additional Certificates
- Other Options

### Authentication

Please provide the authentication details for the network.

Authentication: IEEE 802.1x ▼

EAP Type:

- Windows: PEAP/MSCHAPv2 ▼
- Apple iOS / OS X: PEAP/MSCHAPv2 and PEAP/GTC ▼
- Android: PEAP/GTC ▼
- Linux: PEAP/GTC ▼
- Chrome OS: PEAP/MSCHAPv2 ▼

---

**PEAP/MSCHAPv2 and PEAP/GTC**

Include Credentials:  Include username/password in profile sent to user  
 Don't include username/password in profile sent to user

Authenticate with:  realm/username  
 realm/username  
 username@realm  
 username

Realm:

Detect and override username format and realm when authenticating against Active Directory:

[< Back](#) [Next >](#)

Once completed click **Next** to continue configuring the profile.

## Proxy Settings

This tab allows configuring the proxy server settings for the client.

Using the drop down menus select from the following.

- **Apple OS X proxy Mode** - From the drop down menu, select whether Proxy Server Settings should be **Disabled** or set to **Auto Discovery**.
- **Windows Proxy Mode** - From the drop down menu, select whether Proxy Server Settings should be **Disabled** or set to **Auto Discovery**.
- **Android Proxy Mode** - From the drop down menu, select whether Proxy Server Settings should be **Disabled** or set to **Manual Settings**. For info on manual settings see below.
- **Linux Proxy Mode** - From the drop down menu, select whether Proxy Server Settings should be **Disabled** or set to **Auto Discovery**.

- **Apple IOS Proxy Mode** - From the drop down menu, select whether Proxy Server Settings should be **Auto Discovery**, **PAC URL**, **Disabled** or set to **Manual Settings**.
- **Chrome OS Proxy Mode**: - From the drop down menu, select whether Proxy Server Settings should be **Auto Discovery**, **PAC URL**, **Disabled** or set to **Manual Settings**.

**Smart Connect Profile Wizard**

✓ Welcome  
 ✓ Network Settings  
 ✓ Authentication  
 ★ **Proxy Settings**  
 Certificates  
 Additional Certificates  
 Other Options

### Proxy Server Settings

Please specify how you would like to configure the client's proxy server settings.

Apple OS X Proxy Mode: Auto Discovery ▼  
 Windows Proxy Mode: Disabled ▼  
 Android Proxy Mode: Disabled ▼  
Proxy settings are supported for Android 3.1 and later  
 Linux Proxy Mode: Auto Discovery ▼  
 Apple IOS Proxy Mode: Disabled ▼  
 Chrome OS Proxy Mode: Disabled ▼

< Back

If you select **Manual Settings** for your proxy server settings, update the following.

- **Server** - Enter your server's hostname or IP Address.
- **Port** - Enter the appropriate port number.
- **Authentication** - From the drop down menu 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 password.
- **Username Format** - Select a method of username format.
- **Realm** - Enter the Realm if required.

## Manual settings

Server:

Port:

Authentication:  Proxy authentication is not supported on Android or ChromeOS

Username:  Leave blank to use same credentials as 802.1X authentication

Password:  Confirm:

Username Format:  *realm \username*  
 *realm/username*  
 *username@realm*  
 *username*

Realm:  Leave blank to use the same realm as 802.1X authentication

If you select **PAC URL** settings for your proxy server, update the following.

- **ProxyPACURLString Optional** - The URL of the PAC file that defines the proxy configuration.
- **ProxyPACFallbackAllowed Boolean Optional** - When disabled the device is prevented from connecting directly to the destination if the PAC file is unreachable. This is enabled by default.

## PAC Settings

PAC URL:

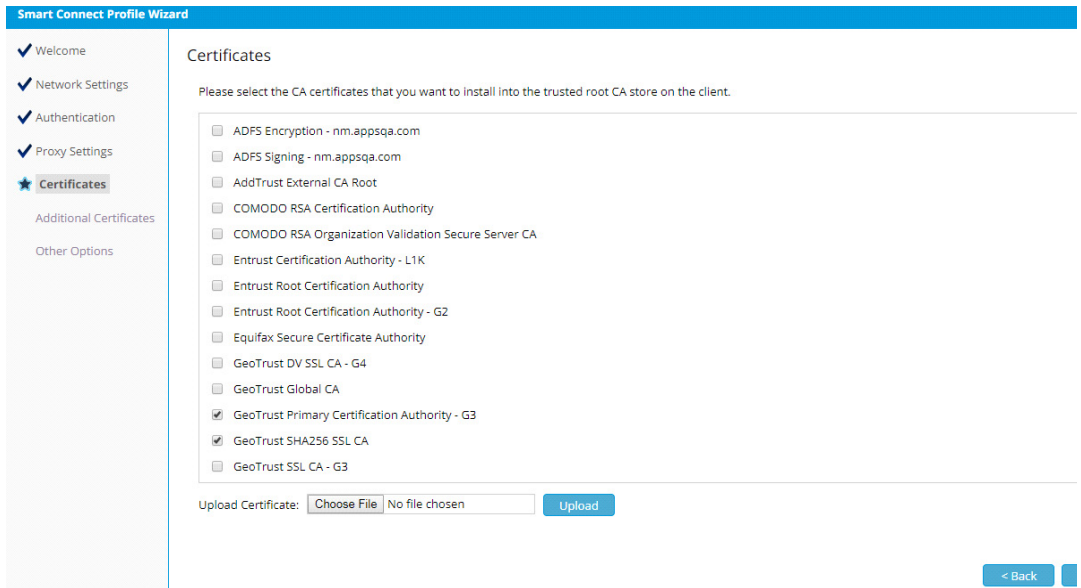
PAC Fallback Allowed:

Once completed click on **Next** to continue configuration.

## Certificates

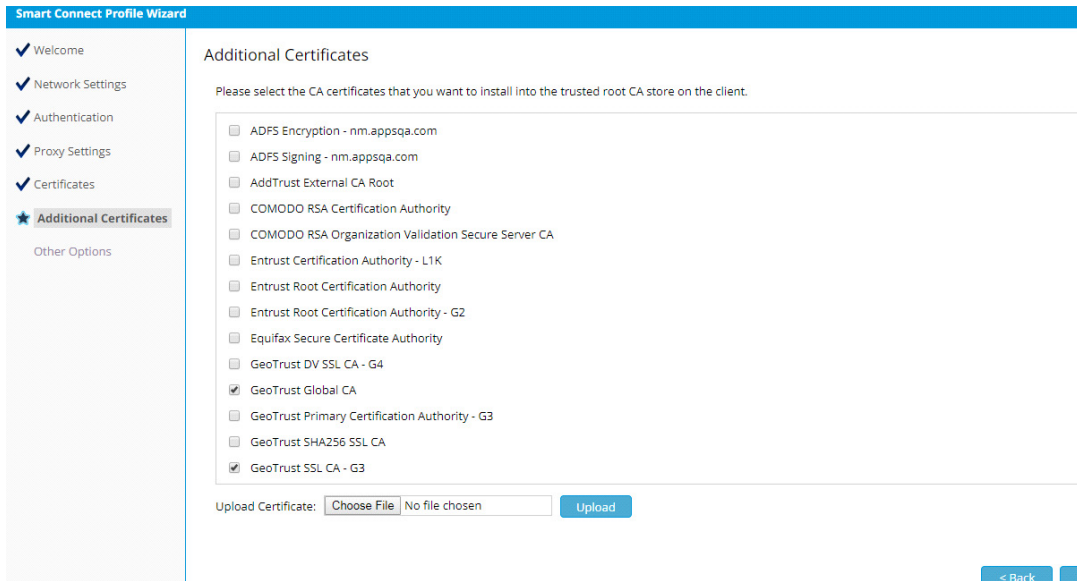
**Note:** This screen is displayed only if the authentication method is NOT Pre-shared key. If **Pre-Shared Key** has been selected then you are not required to configure this tab.

You can upload any certificates you wish to install or select any pre-installed certificates available on the Identity Manager. Click on **Next** to continue configurations.



## Additional Certificates

This tab allows you to upload or install some additional CA certificates.

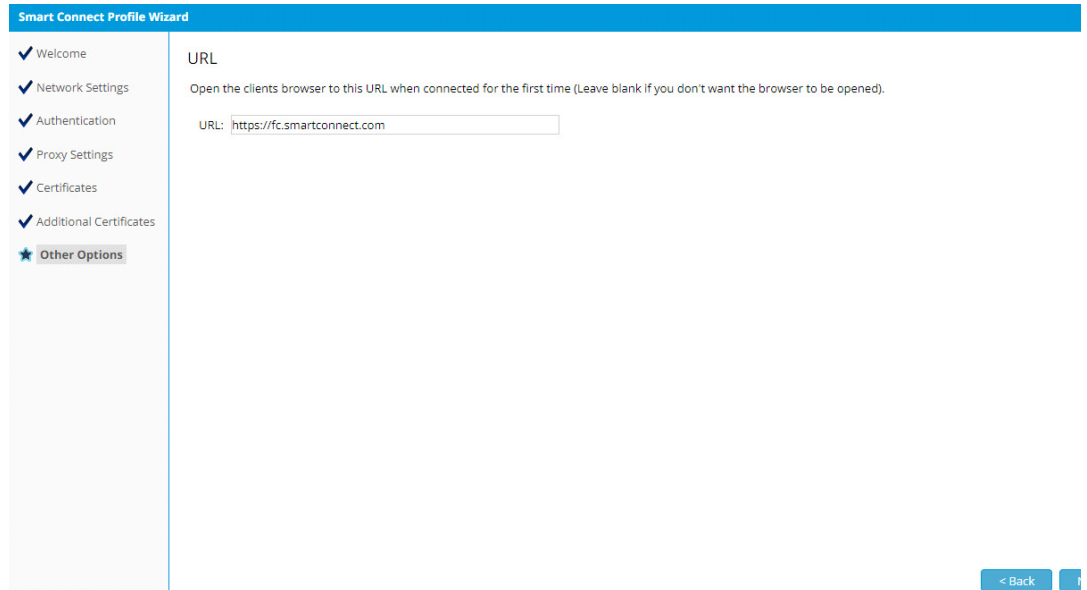


**Note:** The certificate for the FortiConnect is denoted by [localhost]

## Other Options

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.



The screenshot shows the 'Smart Connect Profile Wizard' interface. On the left, a vertical list of steps is shown: 'Welcome', 'Network Settings', 'Authentication', 'Proxy Settings', 'Certificates', 'Additional Certificates', and 'Other Options' (which is highlighted with a star icon). The main area is titled 'URL' and contains the instruction: 'Open the clients browser to this URL when connected for the first time (Leave blank if you don't want the browser to be opened)'. Below this is a text input field with the URL 'https://fc.smartconnect.com' entered. At the bottom right, there is a '< Back' button and a 'Close' button (partially visible).

Click **Close** to complete.

To edit or delete a profile go to **Smart Connect --> Smart Connect Profiles**.

Click on the link of the **Smart Connect Profile** you wish to edit underneath the **Name** Column. This will open up the **Smart Connect Profile setup wizard** to complete your changes. To delete a Smart Connect Profile, click on the **Bin** Icon to the right of the profile you wish to delete, click on **yes** to confirm deletion.

## Smart Connect Policy

---

Create a Smart Connect Policy defining which Smart Connect Profile is applied to each secure client. To add a Smart Connect Policy from the FortiConnect Administrative console, go to **Smart Connect --> Smart Connect Policy** and click **Add**. The **Smart Connect Rule Wizard** appears.

### Details

Enter a name for your **Rule** and a **Description** in the fields provided then click on **Next**.

Smart Connect Rule Wizard

✓ Welcome

★ Details

Conditions

Assign Profile

### Rule Name

Name:

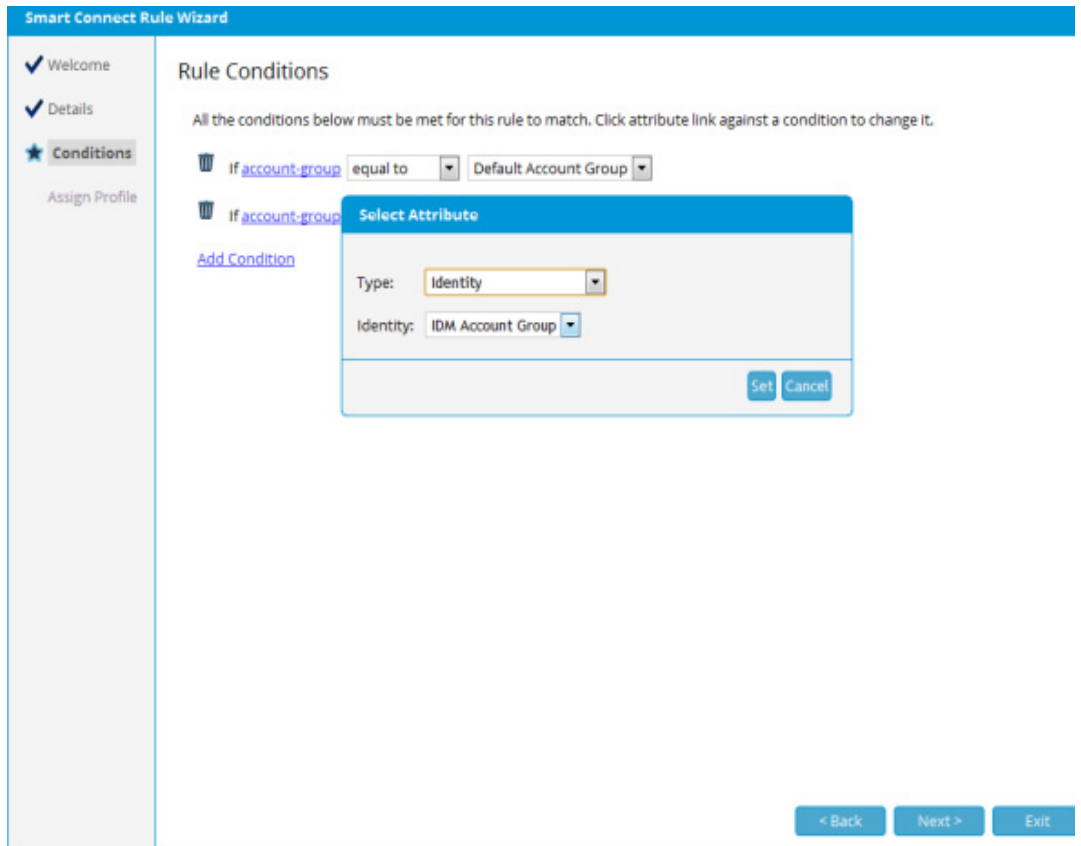
Description:

< Back   Next >   Exit

## Conditions

You can add conditions to your policy by adding attributes, click on the **attribute** link to add as shown below. To add more conditions click on the **Add Condition** link. Select the appropriate **Attribute** from the drop down menu and click on **Set**.

By Default, all users are assigned to the Default Account Group.



## Assign Profile

Select the Smart Connect profiles that you want to assign to users that match the rule you have created.

- **No Smart Connect** - Select if the profile should not be assigned a Smart Connect Profile.
- **Assign Smart Connect Profiles** - Select to assign a Smart Connect profile. Select and order the available wired and wireless profiles to be assigned.

**Note:** FortiConnect supports multiple wired and wireless profiles.

1. Enable/Disable **Allow users to continue using the open networks instead of running Smart Connect** when they authenticate as per your requirement.
2. Enable/Disable **Use Apple Configuration profiles for clients running OS X 10.7 or greater**.

To edit or delete a policy go to **Smart Connect --> Smart Connect Policy**. Click on the **Edit Policy** icon next to the policy you wish to edit and make the required changes. To delete a policy click on the **Bin** Icon next to the Policy you wish to delete.

# Language Templates

---

Administrators can add and remove different language templates for different network clients.

Click on the **Default** link to check the language, you will open up a screen as shown below detailing different platforms.

The screenshot shows a web interface titled "Language Templates: Default". At the top, there are tabs for "Android", "Windows", "Linux", "Mac OSX", and "Apple IOS", with "Android" currently selected. Below the tabs, there are several input fields for configuring the language template:

- Application Logo:** A text input field with a "Choose File" button and "No file chosen" text.
- Username Label:** A text input field containing "Username".
- Password Label:** A text input field containing "Password".
- Login Button:** A text input field containing "Login".
- Connecting:** A text input field containing "Connecting..".
- Failed to Connect to Network:** A text input field containing "Failed to Connect to Network".
- Connected:** A text input field containing "Connected".
- Connected Message:** A text input field containing "You are now connected to the %ssid% secure wireless network. %ssid% will be replaced by network SSID".
- Invalid Credentials:** A text input field containing "Invalid Credentials".

At the bottom of the form, there are two buttons: "Save" and "Cancel".

- From the tabs select which Platform you wish to edit.
- To upload an **application logo**, click on choose file and select a logo from your files.
- Edit any language as necessary by changing the text in the fields provided.

**Note:** Different platforms may have different fields.

- Click on **Save** to keep any changes made to the text.

To add a Language Template go to **Smart Connect --> Language Templates** from the Administrative console and click **Add**.



Enter the name of your Template and click on **Add** once complete. Your template will be created and be based on the pre-defined default template and will automatically direct you to the **Android** tab. You can make the required changes in the appropriate tabs. To upload a logo click on **Choose File** and upload a logo from your files. Click **Save** once completed.

Language Templates: Meru Template

Template "Meru Template" created based on default template

**Android** Windows Linux Mac OSX Apple IOS

Application Logo:  No file chosen

Username Label: Username

Password Label: Password

Login Button: Login

Connecting: Connecting..

Failed to Connect to Network: Failed to Connect to Network

Connected: Connected

Connected Message: You are now connected to the %ssid% secure wireless network.  
%ssid% will be replaced by network SSID

Invalid Credentials: Invalid Credentials

To edit or delete a template, go to **Smart Connect --> Language Templates** from the Administrative console and click on the edit icon ext to the template you wish to edit. Make any necessary changes and click on **Save** once completed.

To **delete** a Language Template cClick on the **Bin** icon next to the template you wish to delete and click on **yes** to confirm deletion.

## Code Signing Certificates

---

FortiConnect supports the upload of Authenticode Code Signing Certificates & CSR / Key generation. This allows the Windows Smart Connect executable to be signed on generation and reduces the number of security warnings that appear when it's downloaded and run.

If certificates are uploaded, the executable will be 'published' by the organization name specified on the certificate and no longer show as having an 'unknown publisher'.

The nature of Windows messages should now be informational alerts rather than security warnings.

**Note:** Contact should be made to the **Certificate Authority** with a view to purchasing any relevant certificates, in this case a **Microsoft Authenticode Code Signing Certificate** is required. Depending on the **Certificate Authority** you approach, they may require a **CSR** (Certificate Signing Request), you can create the **CSR** following instructions in the next section.

From the FortiConnect Interface go to **Smart Connect -->Code Signing Certificates** and select the following.

### **Certificate Signing Request**

- **Create CSR** - Create a CSR (detailed further below)
- **Download CSR** - Download the CSR file

### **Download**

- **Download Current Certificate** - Downloads the current certificate.
- **Download Current Private Key** - Download the current private key.
- **Download Current Combined Certificate & Private Key** - Download the current combined certificate and private key.

### **Upload Certificate**

- **Upload Code Signing Certificate** - Click on Choose File and select and upload a code signing certificate.

### **Upload Certificate and Private Key**

- **Upload Code Signing Certificate** - Click on Choose File and select and upload a code signing certificate.
- **Upload Code Signing Private Key** - Click on Choose File and select and upload a code signing private key.

### **Upload Combined Certificate and Private Key (\*.pfx, \*.p12)**

- **Upload Combined Code Signing File** - Click on Choose File and select and upload the combined certificate and private key.
- **Passphrase** - Enter the passphrase if one is associated with the combined certificate and private key file.

## Code Signing Certificates

### Certificate Signing Request

[Create CSR](#)

Download CSR

### Download

Download Current Certificate

Download Current Private Key

Download Current Combined Certificate & Private Key

### Upload Certificate

Upload Code Signing Certificate:  No file chosen

### Upload Certificate and Private Key

Upload Code Signing Certificate:  No file chosen

Upload Code Signing Private Key:  No file chosen

### Upload Combined Certificate & Private Key (\*.pfx, \*.p12)

Upload Combined Code Signing File:  No file chosen

Passphrase:

Leave blank if no passphrase associated with file

3. Click on **Upload** to upload certificates.

## Create CSR

If you are required to create a CSR then click on the **Create CSR** link and you will be presented with the screen below.

1. Using the fields provided enter the following required information.

- **Organization** - The legal name of your organization
- **Email** - Email address
- **Organizational Unit (Section)** - Organizational Unit
- **Locality** - City or Area
- **State or Province** - State or Province
- **Country** - From the drop down menu select your country.

2. Enable **Regenerate Private Key** if you wish to regenerate the private key.

3. Click on **Create** to create your CSR

**Create CSR**

**Code Signing CSR**

Organization:   
Legal name of your Organization without abbreviation, including any suffixes e.g. Inc, Corp etc.

Email:

Organizational Unit (Section):

Locality (e.g. City):

State or Province:

Country:

---

**Private Key Regeneration**

**WARNING:** Regenerating the private key will invalidate any existing code signing certificates

Regenerate Private Key:

# SCEP and User Certificate Authorities

---

FortiConnect allows distribution of certificates to devices when they are authenticated onto the network. This can be done in a few different ways.

- If you wish to generate user certificates on an external server (e.g. Active Directory) then you can add an entry in **Smart Connect--> SCEP Servers**.
- You can also generate certificates internally on the FortiConnect, you may configure this in **Smart Connect --> User Certificate Authorities**.
- Certificates can be uploaded manually during setup in **Network Access Policy --> Authentication Policy**.

To allow authentication with a user certificate you must edit a Network Access Policy by going to **Network Access Policy --> Authentication Policy**. and select the certificate source(s) that are associated with the policy during setup.

When the network user requests a Smart Connect profile, a user certificate is generated, this is done by selecting EAP-TLS as an EAP type in a Smart Connect Profile using the wizard in **Smart Connect --> Smart Connect Profiles**, you may then choose one of the above certificate sources so when the network user requests a Smart Connect profile the user certificate is generated.

The sections below detail how to Add a **SCEP Server** and how to generate Certificates internally using **User Certificate Authorities**.

# Managing an SCEP Server

If you wish to generate user certificates on an external server (e.g. Active Directory) then you can add an entry from the FortiConnect Interface at **Smart Connect--> SCEP Servers**.

1. To add a SCEP server click on **Add** the **SCEP Server Wizard** is displayed.
2. Click **Next** to configure the **SCEP Server** settings.
3. In the fields provided, enter the following -
  - **Name** - Enter the Name of the SCEP Server
  - **SCEP URL** - Enter the URL of the SCEP Server (HTTP only)
  - **CA Identifier** - Enter the CA Identifier for your SCEP Server (note that this is not required if connecting to NDES on a windows server)
  - **Challenge Password** - Required if connecting to NDES on a Windows Server. If left blank then the users current password is used when generating their client certificate.
  - **Key Size** - From the drop down menu select whether the key size should be 1024 or 2048 bits
  - **OCSP Responder URL** - Optional Field, but if required enter the URL to send an OCSP request for validating user certificates when authenticating.

**SCEP Server Wizard**

✓ Welcome

★ SCEP Settings

Test SCEP Server

Name:

SCEP URL:

CA Identifier:   
Not required if connecting to NDES on a Windows server.

Challenge Password:   
Required if connecting to NDES on a Windows server. If left blank the user's current password is used when generating their client certifi

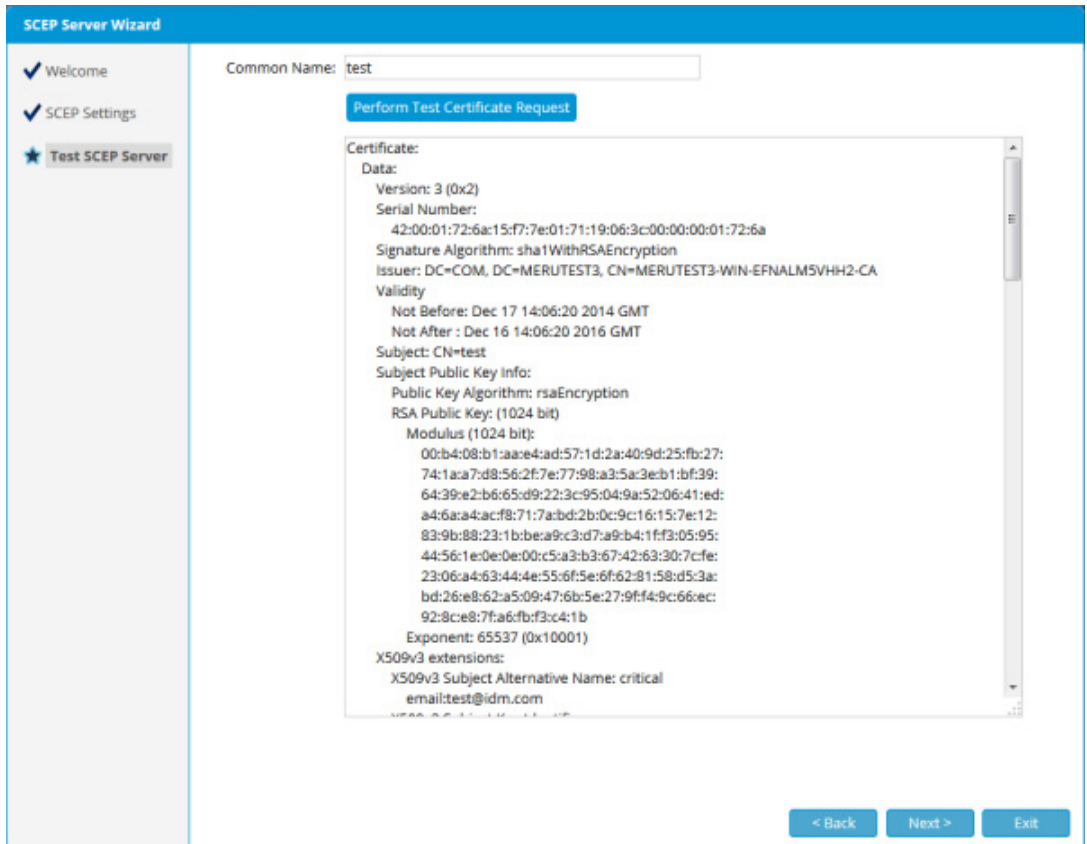
Key Size:   
The user's certificate will be generated with this key size.

OCSP Responder URL:   
Optional. An OCSP request will be sent to this URL to validate a user's certificate when authenticating.

< Back   Next >

4. Click **Next** to continue.

5. Click **Perform Test Certificate Request** on the **Test SCEP Server** screen to test the configured certificate request. The test result is populated.



6. Click **Next** to complete the setup.

To edit or delete an SCEP Server click on the name of the SCEP Server you wish to edit and perform the appropriate changes. If you wish to delete an SCEP Server click on the **Bin** icon next to the SCEP Server you wish to delete. Click **Ok** to confirm.

## Managing a User Certificate Authority

Certificates can be generated internally on the FortiConnect, you may configure this in **Smart Connect --> User Certificate Authorities**.

To Add a Certificate Authority click the **Create**.

7. In the fields provided, enter the following -
  - **Common Name** - Common Name of the Certificate Authority
  - **Organization** - Organization
  - **Organization Unit** - Organization Unit or Section of the Certificate Authority
  - **Locality** - Locality of the Certificate Authority

- **State or Province** - State or Province of the Certificate Authority
- **Country** - From the drop down menu select the country of the Certificate Authority
- **Maximum Lifetime** - Use the drop down menus to define the Maximum Lifetime of any generated certificate.

### Add Certificate Authority

Common Name:

Organization:

Organizational Unit (Section):

Locality (e.g. City):

State or Province:

Country:

Maximum Lifetime:   When generating client certs

**8.** Click **Create** once complete

To edit or delete a User Certificate Authority, go to **Smart Connect --> User Certificate Authorities**. Click on the Name of the User Certificate Authority you wish to edit and perform the appropriate changes. If you wish to delete a User Certificate Authority, click on the Bin Icon next to the Name of the User Certificate Authority you wish to **Delete**. Click on **Ok** to confirm.

**Note:** EAP-TLS & PEAP/EAP-TLS cannot be provisioned automatically on Windows XP Clients by Smart Connect.

## Device Logs

---

Smart Connect uses Device Logs as a troubleshooting functionality for devices connected to the network using Smart Connect.

1. To view the **Device Logs** go to **Reports & Logs --> Smart Connect Device Logs** on the FortiConnect Administration Interface as shown below.

## Smart Connect Device Logs

Username:  Platform: All

Between:     And:

10 per page

Username ▲▼	Platform ▲▼	Model ▲▼	Time ▲▼	Device Logs
No Records Found				

- Using the fields provided you can tailor your search as defined:-
  - Username** - If you are searching for a specific user enter the username here.
  - Platform** - From the drop down menu select which platform you wish to perform your search on.
  - Between** - Enter the date and time you wish to start your search from.
  - And** - Enter the date and time you wish to end your search from.
- Click on **Run** to perform the search.
- Once the search has been completed, the table will populate with your search results, to view the **Device Logs** from a specific search click on the **View** link next to the result as shown below.



Device Log

Back to Devices Download CSV

Showing 1-10 of 66 10 per page Go

Log Time ▲▼	Message ▲▼
17-Dec-2014 12:41:28	2014-12-17T12:41:25+00:00 Install successful
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Set profile priority [0]
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Applying profile [C:\Users\ashfaq\AppData\Local\Temp\7ZipSfx.000\sam-secure.xml]
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Wireless adapter found. adapter Des=Intel(R) PRO/Wireless 3945ABG Network Connection
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Enumerating wireless adapter.
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Applying wireless profile for sam-secure
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Adding profile [C:\Users\ashfaq\AppData\Local\Temp\7ZipSfx.000\]
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 1 additional wireless profiles to add: C:\Users\ashfaq\AppData\Local\Temp\7ZipSfx.000\
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Adding secondary wireless profiles
17-Dec-2014 12:41:28	2014-12-17T12:41:24+00:00 Wireless adapter found. adapter Des=Intel(R) PRO/Wireless 3945ABG Network Connection

Page 1 of 7 Go

- The Device log will display the:-
  - Log Time** - Date and Time of the log
  - Message** - Log message.
- Click on the **Download CSV** button if you wish to download the logs as a CSV file.  
Click on the **Back to Devices** button to perform another search.



# Replication and High Availability

To provide high availability, the FortiConnect solution can be configured so it is part of a cluster with all members of the cluster synchronizing their databases between one another. This provides the ability for the solution to carry on working in the event of loss of connectivity or failure to a single unit.

High availability is provided in an active/active scenario, where all FortiConnect can service requests from sponsors or network devices at the same time. This capability also allows you to load balance the requests between the boxes.

**Note:** Not all system settings are replicated. Refer to Data Replicated to review which settings are not replicated.

**Note:** For load balancing, external load balancers must be used to load balance the web interface. RADIUS requests can also be load balanced via external load balancers or by configuration.

**Note:** Replication is only supported on FortiConnect servers running identical versions of software. This chapter includes the following sections:

- Configuring Replication
- Configuring Provisioning
- Replication Status
- Recovering from Failures
- Deployment Considerations

## Cluster Configuration

---

Multiple instances of FortiConnect are supported in a cluster. Each system is fully active at any point in time and can receive and respond to requests with no dependence on any other system in the cluster.

**Note:** You will need to set up one of your FortiConnect systems as the Registration Server then add any other Normal Servers afterwards.

**Note:** To enable replication, all servers in a cluster must be able to validate each others certificate, to do this, each server will need a certificate signed by a trusted CA and can be uploaded to **Server --> SSL Settings** before you continue.

**Note:** In previous versions of FortiConnect files/certificates/themes would have to be uploaded individually to each box in the cluster, however, in FortiConnect 13.6 an upload to a FortiConnect will automatically be applied to all others in the cluster at the same time.

1. From the FortiConnect Interface go to **Server --> Cluster Configuration** and you will be presented with the **Setup** screen as shown below.

**Cluster Configuration**

**Setup**

Meru Connect supports multiple instances of MCT in the cluster. Each instance is fully active at any point in time and can receive and respond to requests with no dependence on any other instance in the cluster.

- **Disabled** - Cluster support is disabled.
- **Registration Server** - In each cluster one and only one system should be enabled as Registration Server. All other servers contact the Registration Server during initial setup to learn about all other servers in the cluster.
- **Normal Server** - Each other server should be setup as a Normal server.

Once initial setup has taken place all servers behave identically.

Server Mode:  Disabled  Registration Server  Normal Server

Registration Server:   
Hostname or IP address

Shared Secret:  Confirm:

The Shared Secret should be the same on all servers in the cluster. It is used to authenticate servers to each other.

Validate Certificate common name:  Certificates can be uploaded in [Server > SSL Settings](#)  
SSL is used to encrypt connections between servers, you can choose to validate the certificates presented by each IDM.

**Save**

2. There are 3 options to choose from for server mode -
  - **Disabled** - Cluster support is disabled.
  - **Registration Server** - In each cluster one and only one system should be enabled as Registration Server. All other servers contact the Registration server at initial setup to learn about all other servers in the cluster.
  - **Normal Server** - Each server should behave identically.
3. Once you have made your selection enter the appropriate details in the fields provided.
  - **Registration Server** - If **Normal Server Mode** has been selected, enter the Hostname or the IP Address of your chosen Registration Server.
  - **Shared Secret** - Enter the Shared Secret and Confirm. The Shared Secret should be the same for all servers in the cluster.
  - **Validate Certificate Common Name** - SSL is used to encrypt connections between servers, you can select this option to validate the certificates presented by each FortiConnect.
4. Click on **Save** to continue.
5. Your screen will change and some extra tabs will appear along the top as shown below.

**Note:** When adding a new server other than the Registration Server, all data will be wiped from that server when it is added to the cluster.

Cluster Configuration

Cluster configuration saved.

Setup **Status** IP Address High Availability

**Replication Service**

Service is running

**Servers in Cluster**

Server	Status	Configured As	IP Address	Outgoing Batches	Provisioning
idm37.identitynetworks.com (this server)	Working	Registration Server	10.10.1.37		<span style="color: green;">●</span>

6. You will then be taken to the Status Tab which will detail -
- **Replication Service** - Whether your replication service is running.
  - **Servers in Cluster** - A list of servers in your cluster, their status, what they have been Configured As, its IP Address, any Outgoing Batches and Provisioning.

## IP Address High Availability (VRRP)

IP Address high availability allows a single virtual IP Address to be defined and shared between two FortiConnect Servers so that in the event of failure, the Virtual IP address is picked up by the backup server of the pair which then continues to service requests.

FortiConnect provides High Availability between 2 nodes in a local cluster belonging to the same subnet by using the VRRP Protocol. IP Address High Availability can be performed by following the steps below.

1. From the FortiConnect Interface go to **Server --> Cluster Configuration** and click on the **IP Address High Availability** tab as shown below.

The screenshot shows the 'Cluster Configuration' page with the 'IP Address High Availability' tab selected. The page contains the following elements:

- Navigation:** 'Setup' | 'Status' | 'IP Address High Availability' (selected)
- Information:** A blue icon followed by text: 'IP Address High Availability uses the VRRP protocol to allow two Meru Connect boxes to provide active/backup services for a shared IP Address. Devices are configured to use this Virtual IP Address which by default runs on the Master node. In the event of the Master node failing, the Backup node will take over the IP address and service requests.'
- Status:** 'Status: This server is currently inactive' with a grey circle indicator.
- Enable VRRP:** A checkbox labeled 'Enable VRRP:' which is checked.
- Server Settings:**
  - Server Mode:** A dropdown menu currently set to 'Master'.
  - Virtual IP Address:** An empty text input field.
  - Shared Secret:** Two adjacent empty text input fields labeled 'Shared Secret:' and 'Confirm:'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom left.

2. IP Address High Availability uses the VRRP protocol to allow two FortiConnects to provide active/backup services for a shared IP Address. Devices are configured to use this virtual IP Address which by default runs on the Master node. In the event of the Master node failing the Backup node will take over the IP address and service requests.
  - **Enable VRRP** - Check this box to enable VRRP settings.
  - **Server Mode** - From the drop down menu select whether you wish to setup the **Master** or **Backup** mode.
  - **Virtual IP Address** - Enter the virtual IP address for the server.
  - **Shared Secret** - Enter and then confirm the shared secret for the server.
3. Click on **Save** once completed.
4. Once this has been completed the Server Status will change as shown on the screen below.

### Cluster Configuration

Settings saved & VRRP activated

Setup | Status | **IP Address High Availability**

**IP Address High Availability** uses the VRRP protocol to allow two Meru Connect boxes to provide active/backup services for a shared IP Address. Devices are configured to use this Virtual IP Address which by default runs on the Master node. In the event of the Master node failing, the Backup node will take over the IP address and service requests.

Status: This server is currently active [as master] for virtual IP (10.10.1.199) ●

Enable VRRP:

---

**Server Settings**

Server Mode:

Virtual IP Address:

Shared Secret:  Confirm:   
Leave blank to keep existing password

## Configuring Provisioning

---

Certain operations should only be performed by one of the FortiConnects in the cluster, provisioning accounts on external devices and sending notifications to users are examples of such operations.

One FortiConnect should be defined as the provisioning node. The provisioning server will perform the provisioning by default. If an FortiConnect is not the provisioning server, it checks the status of the provisioning server and the other servers in the cluster. If it fails to contact the provisioning server and fallback servers three times, then it will assume these are down and will then perform the provisioning. This process happens every minute when the provisioning service runs.

1. From the administration interface of the cluster registration server, select **Server > Cluster Configuration--> Status**.
2. Click on the grey circle in the **Provisioning** column to specify the server should handle provisioning.
3. The circle should turn green.

**Note:** Only one of the servers should have Provisioning enabled, otherwise you may get errors when creating or deleting accounts twice.

# Replication Status

---

At any time, you can check the replication status of the FortiConnects. This is useful to make sure replication is happening as set.

From the administration interface, select **Server > Cluster Configuration --> Status**.

Here you can check the status of the replication service, list the FortiConnects in the cluster, identify the provisioning server and see the number of records waiting to be replicated from the FortiConnect you are connected to the remaining nodes.

## Recovering from Failures

---

## Network Connectivity

---

When the network connectivity between two FortiConnects fails, the FortiConnect stores upto 1GB of changes. When connectivity is restored, if the amount of changes is less than 1GB, they will synchronize with each other. If more than 1GB of changes are stored, the FortiConnect stops the replication process and you need to setup replication again.

## Device Failure

---

If one of the FortiConnects in a cluster fails and needs to be replaced, you should simply join the replacement FortiConnect to the cluster. If the FortiConnect that failed was the registration server, you will need to promote one of the remaining servers in the cluster to the position of registration server before joining the new FortiConnect to the cluster.

To elevate one FortiConnect to the position of registration server you will need to -

1. From the administration interface of the Identity Manger that will be the new registration server you will need to, select **Server > Cluster Configuration--> Setup** as shown below.
2. Set the **Server Mode to Registration Server**.
3. Click **Save**.



# Deployment Considerations

---

## Connectivity

---

The FortiConnects need to be provided with IP connectivity between the units. Fortinet recommends making the network path between the devices resilient so that synchronization can always be performed. However, if the devices are disconnected, they will continue to function and store changes until they are connected back together and can re-establish communication. At this point, they will re-synchronize databases.

Depending on the amount of activity that your FortiConnect performs, you need to make sure that there is enough bandwidth between the servers to enable synchronization to occur as rapidly as possible.

You can test connectivity by creating a large number of accounts and watching how quickly the appliances synchronize by watching the status on the replication.

## Load Balancing

---

## Web Interface

---

Sponsor and Administration sessions can be serviced by both FortiConnects when configured for replication. However, the FortiConnect does not perform any redirection or automatic load balancing of requests.

To enable requests to both FortiConnects concurrently, you must implement an external load balancing mechanism. Options include:

- Network based Load Balancing— devices can be used to load balance web requests to the FortiConnects. The only requirement for the load balancing is that clients are serviced by the same FortiConnect for their entire session. Individual requests cannot be load balanced between servers, as the FortiConnect does not replicate sponsor/admin session information to reduce bandwidth requirements. The most common method of achieving this is sticking connections to the same FortiConnect based upon source IP address.
- DNS Round robin—Using your DNS server, configure the domain name of the FortiConnect to return all IP addresses for the FortiConnect in a round-robin configuration. This method does not provide failover between appliances in the event of a failure.

- Publishing multiple URLs—This allows each user to choose the server they want to use.

# RADIUS Interface

---

The RADIUS interface on either FortiConnect can take requests at the same time.

Fortinet recommends configuring one to be the primary for some RADIUS clients and another FortiConnect to be the primary for the other RADIUS clients. For failover, the RADIUS clients can have secondary RADIUS servers defined as another FortiConnect, if they support configuration of two servers.

# Data Replicated

---

FortiConnect Replication replicates data that is stored in the database between all FortiConnects in the cluster. The following information is not replicated and is locally defined on each FortiConnect.

- Email settings—SMTP Server
- Network settings
  - Domain name
  - Hostname
  - IP Address
  - Subnet mask
  - Default gateway
  - Nameserver 1
  - Nameserver 2
- Date/Time settings
  - Date Time Locale
  - NTP server 1
  - NTP server 2
- SSL settings
  - SSL Certificate
  - Root CA Certificate
  - Private key
- Backup
  - Max number of backups
  - Frequency
  - FTP settings

# Management, Logging and Troubleshooting

This chapter describes the following:

- Dashboard
- SNMP Configuration
- System Logging
- RADIUS Authentication Logs
- User Accounts
- RADIUS Accounting
- System Performance
- PCI Compliance
- Packet Capture
- Auto Updates

## Dashboard

---

Once the FortiConnect Setup Wizard has been completed the Dashboard will be the first thing an Administrator will see when they login to the network and can be reached by navigating to **Home --> Dashboard**

Meru Connect Administration admin user Logout About A A A C

HOME

- Dashboard
- My Settings
- Setup Wizard

NETWORK ACCESS POLICY

POLICY SETTINGS

SPONSOR PORTAL

GUEST PORTALS

SMART CONNECT

DEVICES

REPORTS & LOGS

SERVER

© 2011-2014 Meru Networks. All rights reserved.

**Dashboard**

**Critical Alerts & Messages**

Message	Date/Time
No Records Found	

**Messages**

- CPU usage is very high.

**Guest Statistics**

**User Accounts**

Total:	0
Active:	0
Inactive:	0
Expired:	0
Suspended:	0
Rejected:	0
Pending Approval:	0

**Meru Connect License**

Expiry: 59 days left:	
User Limit:	100
Licenses in use:	0
Limit exceeded in last 7 days:	0

**System**

**CPU**

Number of CPUs:	1
Usage:	High
Load Average:	
Last minute:	20.46
Last 5 minutes:	12.39
Last 15 minutes:	5.33

**Memory and Disk**

Total server memory:	1.0GB
Total disk space:	35.4GB
Free disk space:	32.0GB

**NTP (Time Synchronization)**

Status:	Stopped
---------	---------

**Replication**

Enabled:	No
Service:	Stopped

**Application Logs Refresh**

Sponsor/Admin User	Action	Date/Time
admin	Login successful [admin]	02-Dec-2014 12:44:52
admin	Configuration settings saved	02-Dec-2014 12:28:12
admin	Test URL returned [0] [Could not resolve host: scep; Unknown error; URL: http://scep]	02-Dec-2014 12:21:54
admin	Login successful [admin]	02-Dec-2014 12:19:13
admin	Client language template ( 2 ) updated	02-Dec-2014 12:07:18
admin	Client Language template ( Meru Template ) added, with component values as Default template	02-Dec-2014 12:06:21
admin	Client network configuration [Client Access] saved	02-Dec-2014 11:50:15
admin	Client network configuration [Client Access] saved	02-Dec-2014 11:49:33
admin	Client network configuration [Client Access] saved	02-Dec-2014 11:48:39

There are 4 sections this dashboard contains as follows:

1. Critical Alerts & Messages
2. Guest Statistics
3. System
4. Application Logs

## Critical Alerts & Messages

This section refreshes itself automatically every minute to display the latest data and also shows the 10 latest critical alerts.

It will also show the following messages as and when the conditions are met :

- Packet capture is running
- The server has less than 1GB of memory

- The total disc spaces is less then 20GB
- The free disc space is less than 1GB
- RADIUS is running in debug mode
- No response from the DNS server
- License is going to expire within 30 days
- Have set detailed log level in Log Settings
- Replication is on but service is stopped
- CPU usage is high

## Guest Statistics

---

This sections refreshes itself automatically after 67 seconds to display the latest data on the number of different users with different statuses.

Statuses that will be displayed are as listed :

- Created
- Authenticated
- Connected
- Active
- Pending Approval
- Rejected
- Suspended
- Expired

It also shows the following in this section :

- License expiry date - It will detail whether the license installed on the system is a permanent license or if expiry remains is less than 61 days then the number of days remaining will be shown.
- Users limit - Number of times the limit has been exceeded in the last 7 days.

## System

---

This section refreshes itself periodically to display the latest data on performance as follows :

- CPU usage
- Average CPU load in the last 1, 5 and 15 minutes

- Total system memory in GB
- Total disc space
- Free space available
- NTP status
- Replication status

## Application Logs

---

This section does not refresh itself automatically but does contain a link to refresh once clicked and displays the most recent 100 application log entries into the system.

## SNMP Configuration

---

FortiConnect supports management applications monitoring the system over SNMP (Simple Network Management Protocol). SNMP Versions 1, 2c and 3 are supported.

The appliance can also send SNMP traps and informs when certain settings exceed a defined value.

## SNMP Agent Configuration

---

From the administration interface, select **Server > SNMP** as shown below.

## SNMP Agent

Agent Traps

### SNMP Version 1

Enable V1:

Read Community:

---

### SNMP Version 2c

Enable V2c:

Read Community:

---

### SNMP Version 3

Enable V3:

Username:

Password:  Confirm:

Authentication Protocol:

Privacy Protocol:

Security Type:

---

### Allowed IP Addresses

IP Range	
0.0.0.0/0	<input type="button" value="Delete"/>
<input type="text"/>	<input type="button" value="Add"/>

You can configure the following options:

- Configuring SNMP Version 1
- Configuring SNMP Version 2c
- Configuring SNMP Version 3
- Configuring SNMP Allowed Addresses

## Configuring SNMP Version 1

---

1. To enable SNMP Version 1, check the **Enable V1** checkbox.
2. Enter an SNMP Read Community name to be used for read access.

3. Configure the Allowed IP Addresses allowed to access the appliance using SNMP by following the instructions in Configuring SNMP Allowed Addresses.
4. Click **Save**

## Configuring SNMP Version 2c

---

1. To enable SNMP Version 2c, check the **Enable V2c** checkbox.
2. Enter an SNMP Read Community name to be used for read access.
3. Configure the Allowed IP Addresses allowed to access the appliance using SNMP by following the instructions in Configuring SNMP Allowed Addresses.
4. Click **Save**.

## Configuring SNMP Version 3

---

1. To enable SNMP Version 3, check the **Enable V3** checkbox.
2. Enter a Username to be used for read access.
3. Enter the Password and confirm it to make sure it has been entered correctly.
4. Select an Authentication Protocol from the dropdown menu: MD5 (HMAC-MD5-96) or SHA (HMAC-SHA-96).
5. Select a Privacy Protocol from the dropdown menu: DES or AES.
6. Select the Security Type to use from the dropdown menu: Authentication or Encryption.
7. Configure the Allowed IP Addresses allowed to access the appliance using SNMP by following the instructions in Configuring SNMP Allowed Addresses.
8. Click **Save**.

## Configuring SNMP Allowed Addresses

---

1. Enter an IP Address Range made up of an IP Address and a prefix length. For example:
  - 0.0.0.0/0 to allow any address to access the appliance by SNMP.
  - 192.168.1.0/24 to allow any address from the 192.168.1.0-255 to access the appliance.
  - 172.16.45.2/32 to allow only the host 172.16.45.2 to access the appliance.



2. Click the **Add** button.
3. You can repeat Step 1 and Step 2 for as many addresses as you like.
4. Click **Save**.

## Configuring SNMP Trap Support

---

The FortiConnect can be configured to send SNMP Traps to an SNMP Manager based upon certain system events.

### Configuring SNMP Traps

1. From the administration interface, select **Server > SNMP** and click on the **Traps** tab as shown below.

The screenshot shows the 'SNMP Traps' configuration page in the FortiConnect administration interface. The page has a blue header with the title 'SNMP Traps'. Below the header, there are two tabs: 'Agent' and 'Traps', with 'Traps' being the active tab. The configuration is organized into several sections:

- Traps**:
  - Enable Traps**: A checkbox that is checked.
  - Trap Version**: A dropdown menu set to 'Version 1'.
  - Community**: A text input field containing 'public'.
- Disk Space**:
  - Send trap if free disk space less than**: A dropdown menu set to '50%' with '(currently 90% free)' displayed next to it.
- Load Average**:
  - Send trap if Load Average goes above**: Three rows of configuration:
    - 25 over one minute (currently 2.29)
    - 10 over five minutes (currently 7.74)
    - 5 over fifteen minutes (currently 4.65)
- Send Traps To**:
  - A table with one row for 'IP Address' and one empty row below it. An 'Add' button is located to the right of the first row.

At the bottom of the page, there are two buttons: 'Save' and 'Cancel'.

2. Check the **Enable Traps** checkbox if you want to enable traps.

3. Select the Trap Version from the dropdown: Version 1, Version 2c or Informs.
4. Enter the community string which will be validated by the receiving trap service.
5. The FortiConnect sends a trap if the disk space goes below a specified value. Enter the value you want the trap to be sent at in the Disk Space dropdown field.
6. Specify the Load Average that you want a trap to be sent if it exceeds the value over 1 minute, 5 minutes or 15 minutes. Load Average is calculated using the standard Linux formula and can be seen from the command line with the **uptime** command.
7. Enter each IP Address that you want to send a SNMP trap to and click the Add button.
8. Click the **Save** button to save the changes.

The following traps are sent :-

- a cold start trap is sent when SNMP traps are enabled or reconfigured
- a trap is sent when disk space falls below the percentage set in the UI
- a CPU load trap is sent if the load averages exceed those that are set in the UI
- when the server is low on temporary (swap) disk space
- support dskTable to give a simpler view of disk statistics.

## Reports and Logging

---

### System Logging

---

All actions within the FortiConnect 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
- Create system logs

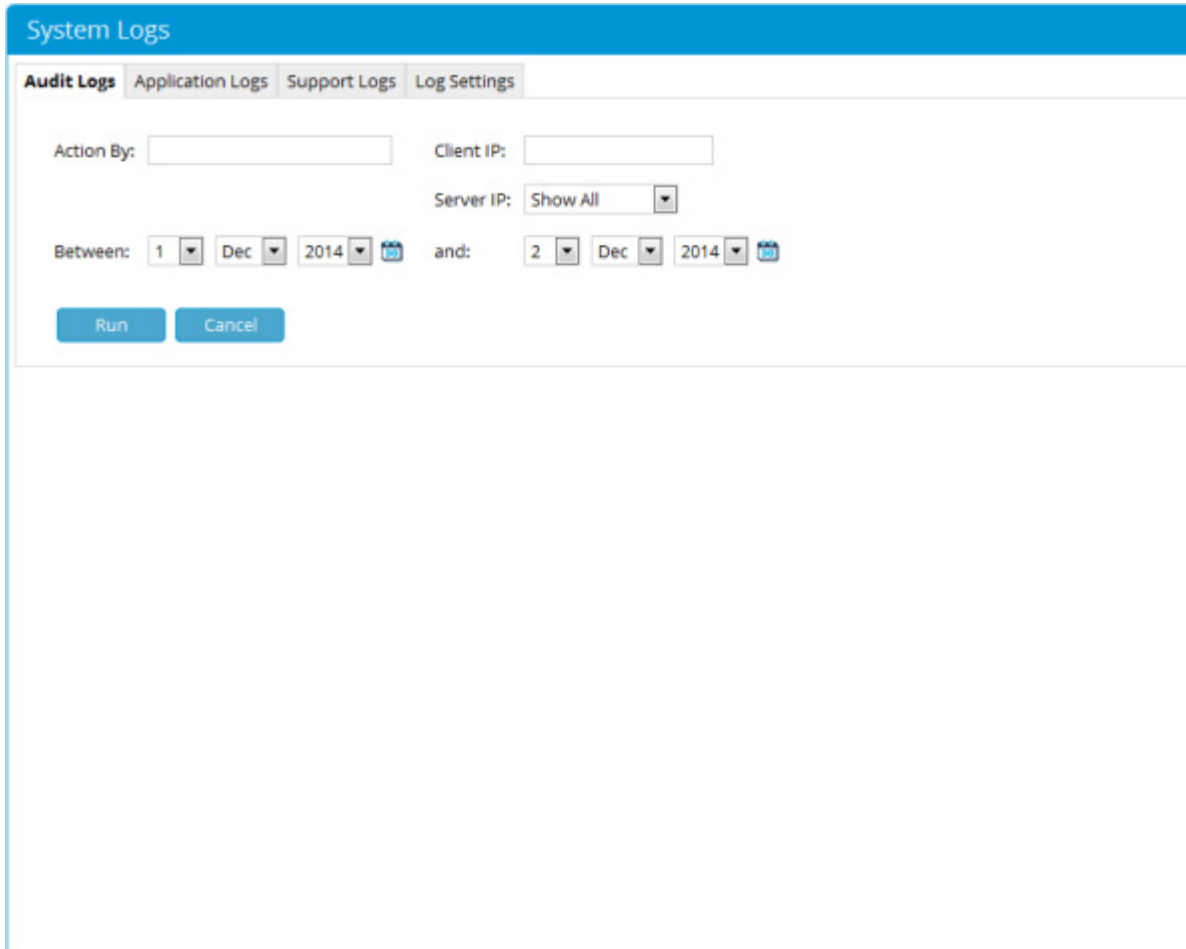
**Note:** It is important to create and constantly maintain logging levels. Refer to Log Settings for details.

# Audit Logs

---

Audit logs create a record of administrator and sponsor actions and can be created using four different methods.

1. To access the audit log functions from the administration interface, select **Reports & Logs > System Logs** as shown below and click the **Audit Logs** tab.



The screenshot displays the 'System Logs' interface. At the top, there is a blue header with the text 'System Logs'. Below the header, there are four tabs: 'Audit Logs' (which is selected and highlighted in blue), 'Application Logs', 'Support Logs', and 'Log Settings'. The main area contains search filters for 'Action By', 'Client IP', and 'Server IP'. The 'Action By' and 'Client IP' fields are empty text boxes. The 'Server IP' field is a dropdown menu currently set to 'Show All'. Below these fields, there is a date range selector labeled 'Between:' followed by three dropdown menus for day, month, and year (set to '1', 'Dec', and '2014' respectively), followed by an 'and:' label and another set of three dropdown menus for day, month, and year (set to '2', 'Dec', and '2014' respectively). At the bottom of the filter section, there are two buttons: 'Run' and 'Cancel'.

2. Audit log reports can be run using four different categories:
  - **Action by**—Displays logs using admin/sponsor user name as its search criteria.
  - **Client IP**—Displays logs using Client IP address as its search criteria.
  - **Server IP**—Displays logs using Server IP as its search criteria.

You can run log reports for a single category, multiple categories, or all categories at the same time.

3. Select a time duration for your search criteria using the date pickers provided, then click the **Run** button.

# Application Logs

Application Logs shows the application log containing application debugs.

1. To access the Application Logs function from the administration interface, select **Reports & Logs > System Logs** and click the **Application Logs** tab as shown below.

The screenshot displays the 'System Logs' interface. At the top, there are tabs for 'Audit Logs', 'Application Logs' (which is selected), 'Support Logs', and 'Log Settings'. Below the tabs, there are search filters: 'Action By:' with an empty text box, 'Client IP:' with an empty text box, and 'Between:' with date pickers for '1 Dec 2014' and '2 Dec 2014'. There are 'Run' and 'Cancel' buttons below the filters. The main area contains a table of log entries. The table has three columns: 'Sponsor/Admin User', 'Action', and 'Date/Time'. The table shows 10 entries, with the first one being 'admin' and 'Login successful [admin]' at '02-Dec-2014 12:44:52'. The table also includes pagination controls at the bottom right, showing 'Page 1 of 9' and 'Go' buttons.

Sponsor/Admin User ▲▼	Action ▲▼	Date/Time ▲▼
admin	Login successful [admin]	02-Dec-2014 12:44:52
admin	Configuration settings saved	02-Dec-2014 12:28:12
admin	Test URL returned [6] [Could not resolve host: scep; Unknown error; URL: http://scep]	02-Dec-2014 12:21:54
admin	Login successful [admin]	02-Dec-2014 12:19:13
admin	Client language template ( 2 ) updated	02-Dec-2014 12:07:18
admin	Client Language template ( Meru Template ) added, with component values as Default template	02-Dec-2014 12:06:21
admin	Client network configuration [Client Access] saved	02-Dec-2014 11:50:15
admin	Client network configuration [Client Access] saved	02-Dec-2014 11:49:33
admin	Client network configuration [Client Access] saved	02-Dec-2014 11:48:39
admin	Client network configuration [Client Access] saved	02-Dec-2014 11:47:53

2. Application Log reports can be run using different categories:
  - **Action By**—Displays logs using admin/sponsor user name as its search criteria.
  - **Client IP**—Displays logs using Client IP address as its search criteria.

You can run log reports for a single category, multiple categories, or all categories at the same time.

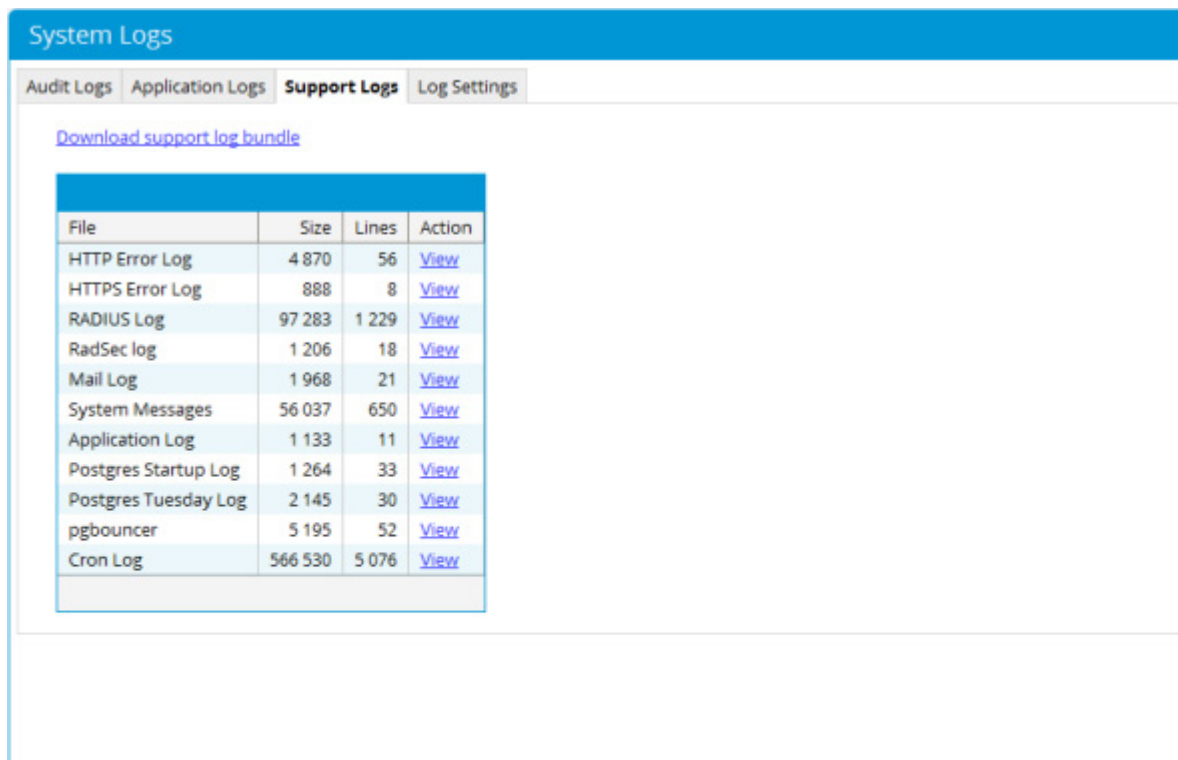
3. Select a time duration for your search criteria using the date pickers provided then click the **Run** button.

## Support Logs

---

Support Logs provide an area that stores:

- HTTP error logs
  - RADIUS logs
  - Mail logs
  - Twin (Replication logs only applicable if running replication between FortiConnects)
  - Debug logs
  - Audit logs
  - Application logs
  - An XML file
1. To access the Support Logs function from the administration interface, select **Reports & Logs > System Logs** and click the **Support Logs** tab as shown below



System Logs

Audit Logs Application Logs **Support Logs** Log Settings

[Download support log bundle](#)

File	Size	Lines	Action
HTTP Error Log	4 870	56	<a href="#">View</a>
HTTPS Error Log	888	8	<a href="#">View</a>
RADIUS Log	97 283	1 229	<a href="#">View</a>
RadSec log	1 206	18	<a href="#">View</a>
Mail Log	1 968	21	<a href="#">View</a>
System Messages	56 037	650	<a href="#">View</a>
Application Log	1 133	11	<a href="#">View</a>
Postgres Startup Log	1 264	33	<a href="#">View</a>
Postgres Tuesday Log	2 145	30	<a href="#">View</a>
pgbouncer	5 195	52	<a href="#">View</a>
Cron Log	566 530	5 076	<a href="#">View</a>

2. You can view or download the logs listed by clicking the underlined **Action** links.

**Note:** The Support Logs page only displays the latest details of each available log. However, clicking View or Download retrieves and displays ALL logs for that category.

## Log Settings

---

The Log Settings page allows an administrator to set the level of logging and administer syslog settings.

1. To access the Log Settings page from the administration interface, select **Reports & Logs > System Logs** and click the **Log Settings** tab as shown below.

**System Logs**

Audit Logs Application Logs Support Logs **Log Settings**

**Logging Levels**

General:	Errors and Notices Only
Sponsor Authentication:	Errors and Notices Only
Admin Authentication:	Errors and Notices Only
Account Creation:	Errors and Notices Only
Account Management:	Errors and Notices Only
Admin Operations:	Errors and Notices Only
RADIUS User Authentication:	Errors and Notices Only
Guest Portals:	Errors and Notices Only

**Syslog Settings**

Send Application Log Events to Remote Server:	(none)
Send System Log Events to Remote Server:	(none)
Syslog Server:	
Syslog Protocol:	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
Syslog Port:	514

Save Cancel

2. **Logging Levels** allow an administrator to choose the level of logging for multiple criteria:
  - **General**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
  - **Sponsor Authentication**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
  - **Admin Authentication**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
  - **Account Creation**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
  - **Account Management**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
  - **Admin Operations**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
  - **Radius User Authentication**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
  - **Guest Portals**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
3. **Syslog Settings** allows an administrator to determine what log events are sent to a predefined syslog server.
  - **Send Application Log Events to Remote Server**—This determines what type of application errors are logged and sent to the server. The administrator can decide on none, Audit, Errors or Audit and Errors.
  - **Send System Log Events to Remote Server**—This determines what type of system errors are logged and sent to the server. The administrator can decide on Emergency, Emergency and Alerts, Emergency Alerts and Critical, or Emergency Alerts Critical and Errors.
  - **Syslog Server**—Enter the DNS or IP Address of the syslog server to which the logs to be sent.
  - **Syslog Protocol**—Choose between UDP and TCP protocols.
  - **Syslog Port**—Define a port for your syslog server.
4. Click the **Save** button to save your settings.

**Note:** To test basic syslog functionality, go to the Log Settings page and click Save. This sends a test message to the syslog server with priority info (6).

**Note:** IdentityNetworks recommends disabling debugging immediately after use so as not to potentially disrupt any other FortiConnect functionality.

## RADIUS Authentications

---

To run a report on successful or failed RADIUS Authentications, go to **Reports & Logs > System Logs**

and click on **RADIUS Authentications** as shown below.

**RADIUS Authentications**

Enable RADIUS Authentication reporting:

Between: 2 Dec 2014

and: 3 Dec 2014

00:00

00:00

Username:

Client IP Address:

Client MAC Address:

NAS IP Address:

Status: Failed Authentications

Run

Username ▲▼	Status	IP Address ▲▼	MAC Address ▲▼	Time ▲▼	NAS IP Address ▲▼
No Records Found					

25 per page Go

1. Choose your search criteria using the fields available :-
  - **Between** - Choose the start date and time for your search.
  - **and** - Choose the end date and time for your search.
  - **Username** - Enter the Username of the account you wish to search against.
  - **Client IP Address** - Enter the Client IP Address you wish to search against.
  - **Client MAC Address** - Enter the Client MAC Address you wish to search against.
  - **NAS IP Address** - Enter the NAS IP Address you wish to search against.
  - **Status** - From the drop down menu select whether you wish to search for Failed Authentications, Successful Authentications or All Authentications.
2. Click on **Run** to start your report.



# User Accounts

FortiConnect can also perform a detailed search on User Accounts

To run this report follow the instructions below.

1. To access the User Accounts reporting function from the administration interface, select **Reports & Logs > User Accounts** and click the **Advanced Search** tab as shown below

## User Accounts

Active Time Between 25-Nov-2014 And 02-Dec-2014 << Advanced Search

Sponsor Group: All ▾ Active Time Between: 25 ▾ Nov ▾ 2014 ▾ 📅

Created By:  And: 2 ▾ Dec ▾ 2014 ▾ 📅

Guest Portal:  Timezone: All ▾

Username:  IP Address:

MAC Address:  Usage Profile:

First Name:  Account Group:

Last Name:  Event Code:

Company:  Email:

Mobile Number:  Inactive:

Active:  Expired:

Suspended:  Pending Approval:

Rejected:

Display Report Download PDF Download Excel Download ODS Download ODT

Created By ▲▼	Username ▲▼	Password	MAC Address ▲▼	First Name ▲▼	Last Name ▲▼	Email ▲▼	Company ▲▼
No Records Found							

2. Using the search filters, enter any information relevant to your search.
  - **Sponsor Group** - Use the drop down menu to select which Sponsor Group you wish to search under.
  - **Active Time Between** - Enter a start and end time to search under.
  - **Created By** - Search using Created By as your search criteria.

- **Guest Portal** - Search using Guest Portal as your search criteria.
  - **Username** - Search using Username as your search criteria.
  - **MAC Address** - Search using MAC Address as your search criteria.
  - **First Name** - Search using First Name as your search criteria.
  - **Last Name** - Search using Last Name as your search criteria.
  - **Company** - Search using Company as your search criteria.
  - **Mobile Number** - Search using Mobile Number as your search criteria.
  - **Timezone** - Search using a specific Timezone as your search criteria.
  - **IP Address** - Search using IP Address as your search criteria.
  - **Usage Profile** - Search using Usage Profile as your search criteria.
  - **Time Profile**- Search using Time Profile as your search criteria.
  - **Guest Role** - Search using Guest Role as your search criteria.
  - **Event Code** - Search using Event Code as your search criteria.
  - **Email** - Search using Email as your search criteria.
3. Check the appropriate check box for the account status -
- Active
  - Inactive
  - Suspended
  - Rejected
  - Expired
  - Pending Approval
4. Now decide how you want your report format -
- Display Report - Display report on screen
  - Download PDF - Downloads report as a PDF file
  - Download Excel - Download report as an excel spreadsheet
  - Download ODS - Download report as an ODS file
  - Download ODT - Download report as an ODT file

## RADIUS Accounting

---

FortiConnect can also perform a detailed search on RADIUS Accounting

1. To access the RADIUS Accounting reporting function from the administration interface, select **Reports & Logs > RADIUS Accounting** and click the **Advanced Search** button as shown below.

## RADIUS Accounting

Between 25-Nov-2014 And 03-Dec-2014 << Advanced Search

Between: 25 Nov 2014 And: 2 Dec 2014

Username:  NAS IP Address:

Calling Station ID:  User IP Address:

Called Station ID:

Display Report Download PDF Download Excel Download ODS Download ODT

Username ▲▼	Session ID ▲▼	Unique ID ▲▼	NAS IP Address ▲▼	Framed IP ▲▼	Start Time ▲▼	Stop Time ▲▼
-------------	---------------	--------------	-------------------	--------------	---------------	--------------

No Records Found

- Using the search filters, enter any information relevant to your search.
  - Between** - Enter a start date for your search
  - and** -Enter and end date for your search
  - Username** - Enter a username to search against
  - Calling Station ID** - Enter a calling station ID to search against
  - Called Station ID** - Enter a called station ID to search against
  - NAS IP Address** - Enter a NAS IP Address to search against
  - User IP Address** - Enter a user IP address to search against
- Now decide how you want your report format -
  - Display Report - Display report on screen
  - Download PDF - Downloads report as a PDF file
  - Download Excel - Download report as an excel spreadsheet
  - Download ODS - Download report as an ODS file
  - Download ODT - Download report as an ODT file


# System Performance


---

FortiConnect Identity can also perform a detailed report on System Performance.

1. To access the System Performance reporting function from the administration interface, select **Reports & Logs > System Performance** as shown below.

## System Performance

Between:    

and:    

Run

Download CSV

Showing 1-25 of 57

Time ▲▼	%user	%nice	%system	%iowait	%steal	%idle
02-Dec-2014 14:10	2.43	0.00	8.35	1.19	0.00	88.03
02-Dec-2014 14:00	1.14	0.00	8.38	1.02	0.00	89.47
02-Dec-2014 13:50	0.89	0.00	7.00	0.56	0.00	91.55
02-Dec-2014 13:40	1.03	0.00	7.56	0.57	0.00	90.83
02-Dec-2014 13:30	1.34	0.00	7.84	1.25	0.00	89.57
02-Dec-2014 13:20	1.26	0.00	7.52	0.57	0.00	90.65
02-Dec-2014 13:10	1.45	0.00	8.26	0.89	0.00	89.41
02-Dec-2014 13:00	1.23	0.00	9.44	0.88	0.00	88.45
02-Dec-2014 12:50	2.09	0.00	11.86	6.65	0.00	79.40
02-Dec-2014 12:40	0.88	0.00	7.44	0.76	0.00	90.91
02-Dec-2014 12:30	1.30	0.00	8.38	1.22	0.00	89.10
02-Dec-2014 12:20	1.28	0.00	7.66	1.02	0.00	90.04
02-Dec-2014 12:10	1.33	0.00	7.24	0.77	0.00	90.66
02-Dec-2014 12:00	1.30	0.00	7.06	0.50	0.00	91.14
02-Dec-2014 11:50	1.33	0.00	7.16	0.90	0.00	90.61
02-Dec-2014 11:40	1.13	0.00	6.94	0.52	0.00	91.40
02-Dec-2014 11:30	1.05	0.00	6.93	0.36	0.00	91.66
02-Dec-2014 11:20	1.29	0.00	7.17	0.62	0.00	90.92
02-Dec-2014 11:10	1.32	0.00	7.17	0.47	0.00	91.04
02-Dec-2014 11:00	1.86	0.00	9.31	0.76	0.00	88.07
02-Dec-2014 10:50	1.12	0.00	8.70	0.54	0.00	89.64
02-Dec-2014 10:40	1.61	0.00	7.81	0.87	0.00	89.71

2. Using the **Date Picker**, select the relevant dates to search between and click on **Run**.
3. Your report should appear below.
4. Click on the **Download CSV** button to download the report in a CSV format,

# PCI Compliance

This is a report to verify that all the settings required to be **PCI 2.0 compliant** are enabled.

It shows the status, and provides help/links to actions required to remediate any issues.

1. To access the System Performance reporting function from the administration interface, select **Reports & Logs > PCI 2.0 Compliance** as shown below.

PCI 2.0. Compliance Report

This report displays the current state of PCI 2.0 compliance for the existing IDM configuration.

PCI DSS Requirement ▲▼	Component ▲▼	State	Details / Action
01. Maintain Firewall Configuration To Protect Cardholder Data	Open Port: 1812 & 1813	✓	Required by RADIUS service
01. Maintain Firewall Configuration To Protect Cardholder Data	Open Port: 1645 & 1646	✓	Required by RADIUS service
01. Maintain Firewall Configuration To Protect Cardholder Data	Open Port: 443 & 8443	✓	Required by web server for HTTPS traffic
01. Maintain Firewall Configuration To Protect Cardholder Data	Open Port: 22	✓	Required by secure shell (SSH)
01. Maintain Firewall Configuration To Protect Cardholder Data	Open Port: 31415	✓	Required by replication services

Showing 1-5 of 42 5 per page Go

Page 1 of 9 Go

2. Columns detailed in this report are :-
  - **PCI DSS Requirement** - PCI requirement
  - **Component** - Component effected
  - **State** - A green tick shows this is captured, a red cross states that its required for compliance
  - **Details / Action** - Details of requirement and any actions needed to make it compliant

# Packet Capture

FortiConnect allows the admin user to record packet data from an IP address / network range for all network traffic or packets to specific ports.

The packet capture tool generates log files which can be downloaded & viewed using a packet viewing utility such as Wireshark.

Only the last 10 generated capture logs are shown in the log table.

1. From the FortiConnect Administration Database browse to **Server --> Packet Capture** as shown below.

**Packet Capture**

**Capture Settings**

Network Range:  /  All Traffic:

ICMP:	<input type="checkbox"/>	UDP 1645 (RADIUS auth):	<input type="checkbox"/>
TCP 80 (HTTP):	<input type="checkbox"/>	UDP 1646 (RADIUS acct):	<input type="checkbox"/>
TCP 8080 (HTTP):	<input type="checkbox"/>	UDP 1812 (RADIUS auth):	<input type="checkbox"/>
TCP 443 (HTTPS):	<input type="checkbox"/>	UDP 1813 (RADIUS acct):	<input type="checkbox"/>
TCP 8443 (HTTPS):	<input type="checkbox"/>	UDP 3799 (RADIUS COA):	<input type="checkbox"/>
TCP 389 (LDAP):	<input type="checkbox"/>	TCP 22 (SSH / SCP / SFTP):	<input type="checkbox"/>
TCP 636 (LDAPS):	<input type="checkbox"/>	TCP 20 / 21 (FTP):	<input type="checkbox"/>
TCP 88 (Kerberos):	<input type="checkbox"/>	UDP 123 (NTP):	<input type="checkbox"/>
UDP 88 (Kerberos):	<input type="checkbox"/>	UDP 161 (SNMP):	<input type="checkbox"/>
TCP 749 (Kerberos):	<input type="checkbox"/>	UDP 162 (SNMP Traps):	<input type="checkbox"/>
TCP 750 (Kerberos):	<input type="checkbox"/>	UDP 53 (DNS):	<input type="checkbox"/>
TCP 25 (SMTP):	<input type="checkbox"/>	TCP 53 (DNS):	<input type="checkbox"/>
TCP 31415 (Replication):	<input type="checkbox"/>		

**Capture Logs**


The last 10 capture logs generated are shown.







File	Size (kb)
No log files found	

2. Enter the Network Range you wish to capture traffic to, or place a check in the **All Traffic** check box to capture all traffic.
3. If you do not wish to capture all traffic, you may place a check in the check boxes provided to capture the relevant traffic.

4. Click on the **Start** button.
5. Once the logs have been completed you will see them listed as per below.

## Capture Logs

 The last 10 capture logs generated are shown.

File	Size (kb)	
2011-09-12T14:58:23-07:00.pcap	268.98	 
2011-09-12T14:58:04-07:00.pcap	178.34	 
2011-09-12T14:57:47-07:00.pcap	1.63	 

6. Download the logs by clicking on the **download** icon.
7. You can delete any logs by clicking on the **bin** icon.

# Automatic Updates

---

As Smart Connect clients are updated and released more quickly than FortiConnect releases Automatic Updates is a feature used to update certain parts of FortiConnect to support those new clients.

Enable Automatic Updates to allow FortiConnect to securely download browser detection rules and Smart Connect updates.

This enables the system to identify the latest browser versions & client platforms without needing to update the main FortiConnect software.

Updates can be scheduled as a batch job to run on a daily, weekly or monthly basis at a given time.

Updates are retrieved from a cloud based CDN. Proxy settings (with / without basic authentication) can be used if needed for external network access.



1. From the FortiConnect Administration interface go to **Server --> Automatic Updates** as shown below.

**Automatic Updates**

Enable Automatic Updates to allow Meru Connect to securely download browser detection rules and Smart Connect updates. This enables the system to identify the latest browser versions & client platforms without needing to update the main Meru Connect software.

Enable Automatic Updates:

---

**Schedule**

Frequency:

Day of the week:

Day of the month:

Time:

---

**HTTP Proxy**

Enable Proxy:

Server:

Port:

Authentication:

Username:

Password:  Confirm:

2. Check the **Enable Automatic Updates** check box to enable Automatic Updates.
3. In the **Schedule** section, use the drop down box to select :-
  - Frequency - Choose from Daily, Weekly or Monthly updates.
  - Day of the Week - Choose which day of the week you wish to perform your update.
  - Day of the Month - If you have chosen Monthly updates, select which day of the month you wish to perform the update.
  - Time - Choose the time of the day you wish to perform the update.
4. Check the **Enable Proxy** check box to enter your proxy server details.
5. In the **Proxy** section, use the fields to enter your proxy server information :-
  - Server - Enter your server hostname or IP address.
  - Port - Enter the port number for your proxy server.
  - Authentication - Use the drop down menu to select the method of authentication for the proxy server.

- Username - Supply the username used to authenticate against the proxy server.
- Password - Enter the password for the proxy server and confirm it.

6. Click on **Save** once you have made your selections.

**Note:** Click on the **Update Now** button to perform an immediate update.

FortiConnect provides multiple Licensing options, the section below details how licensing works on your FortiConnect.

There are two kinds of license that are required for the FortiConnect Appliance

- Device License - This license is unique to a single FortiConnect Appliance (Hardware or Virtual Machine). The device license allows FortiConnect to run on the Appliance. You may install only a single Device License on an appliance.
- User Feature License - This license allows for concurrent usage on a per user basis. Multiple User Feature Licenses can be installed and they are additive.

## Authenticated Users

Users are referred to as accounts that are either a person or a device and have been authenticated onto the network either internally, for example against the local FortiConnect database or with PMS (Property Management System) accounts, or externally by using AD, or a Social Media login.

FortiConnect allows the system to have the same amount of concurrent Users attached to the User network as user licenses.

There are no limits on the amount of authenticated accounts that can be created, only a connected User will consume a license.

## How licenses are consumed

- Each connected User account (as recorded by RADIUS accounting) consumes a single User license.
- Each connected device account unrelated to a User account consumes a single User license.
- Multiple devices registered by a single User account consume a single User license.

# Licensing

---

To view or upload a license from the administration interface:

1. Select **Server > Licensing** as shown below.

## Licensing

### System Information

Serial Number: VMware-56 4d b3 0c ac 5e ee 10-9c d3 f8 4f a6 de 56 f5

System ID: ce74-4745-a4d3-8fa7-a693-30df-6e91-0ca2-7344-9166

### Licence Summary


For information on licensing go to <http://www.merunetworks.com/license>

Feature	Settings	Expiry
Meru Connect	Enabled	31-Jan-2015
Users	Concurrent Users: 100 / In Use: 0	31-Jan-2015

### Upload new License

License File:  No file chosen

### Installed License Files

Features	Created	File
Meru Connect: Expiry: 31-Jan-2015 Users: 100	01-Dec-2014	

2. Click the **Choose File** button under the **Upload new License** section and select the license file.
3. Click the **Upload** button to upload a new license file.

If a license is currently installed the information will be displayed at the top of the page :

- **Serial Number** - Serial Number for the FortiConnect
  - **System ID** - System ID for the License granted.
4. Under Licence Summary it displays -
    - **Feature** - Which feature of FortiConnect is being used.
    - **Settings** - Whether the feature is enabled and how many active licenses are in use.
    - **Expiry** - Expiry date of feature.

**Note:** If you have uploaded an evaluation license, the FortiConnect License Status will indicate the license expiration date.

5. Under **Installed License Files**, you have the ability to download licenses and delete license files if you have multiple license files installed.

## **Replication and Licensing on FortiConnect**

When FortiConnects are replicated across a network, a license is installed on and shared between each system.

If one of the FortiConnect systems is disconnected from the network the remaining FortiConnect would continue to use the total license count of both systems. When connectivity is restored license sharing will resume automatically.



# Sponsor Documentation

This chapter provides user documentation for sponsor users who create UserUser accounts. It contains the following sections:

- Introduction to FortiConnect
- Connecting to the FortiConnect
- Change Default Settings
- Guest User Accounts
- Multiple Guest Accounts
- Event Codes
- Reporting on Guest Users
- Device Accounts
- Multiple Device Accounts
- Sponsor Reporting

## Introduction to FortiConnect

---


The FortiConnect allows you to create temporary network access accounts for your Users, visitors, contractors or anyone who needs temporary network access. You can easily create User or device accounts by browsing to the FortiConnect web interface, logging in with your corporate credentials, and entering the details of the User or device. FortiConnect creates the temporary account and allows you to provide the account details to the User via printout, email or SMS text message. In addition to creating User and device accounts, you can also view and amend the accounts to which you have access, or run reporting on accounts for auditing purposes.

## Connecting to the FortiConnect

---

All connections to the FortiConnect are through a web interface. To connect to the FortiConnect, open a web browser and enter the address into the URL or address field, as provided by your network administrator.

1. Enter the IP address of the FortiConnect into the URL of your web browser, for example, `http://<IP Address of FortiConnect>`.
2. In the FortiConnect login page below, enter your Username and Password, and click the Login button. Use the login credentials specified by your network administrator.



**FORTINET**

# FortiConnect Administration

Version: 17.0.0, Build 0007 (GA)

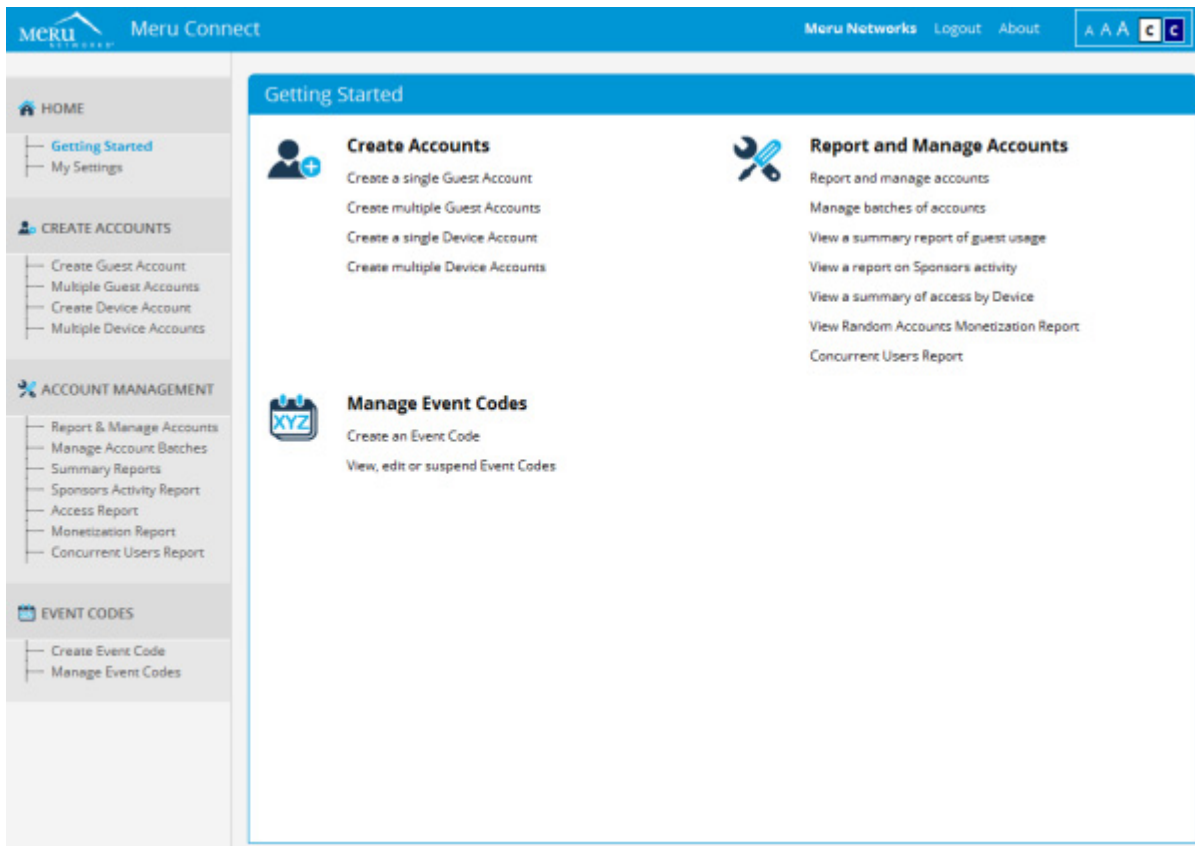
**Username:**

**Password:**

Login

3. When you first log in, the Getting Started page is displayed as shown in below.





4. From this page, you can navigate to **Home > My Settings** to:

- Change Default Settings.
- Change Password.

## Change Default Settings

---

You can change your password, or customize default settings like the language template, time zone, telephone country code, and default login page from the My Settings page.

1. Navigate to **Home > My Settings**

2. Click the **Preferences** tab as shown below, to modify the following Preferences:

- **Language Template**—If your administrator has added additional templates, you can select a language template from this dropdown menu to change the language of the application interface or the User printout/email/SMS notification.
- **Default Timezone**—This timezone is the default selected in the list on the account creation pages.

- **Default Telephone Country Code**—Specify the default for the telephone country code.
- This is used when sending the User details by SMS, or for recording the User’s phone number.
- **Default Guest Role**—Specify the default User role you want to use for creating accounts.
- **Default Device Role** - Specify the default device role you want to use for creating accounts.
- **First Name** - Sponsors first name
- **Last Name** - Sponsors last name
- **Email Address**—Enter your email address here. This is required if you want to receive a copy of the User’s account details by email.
- **Receive Email Confirmation**—Check this checkbox if you want the FortiConnect to send you a copy of the User’s account details by email, when you click the ‘Send Email Notification’ button to notify the users of their User account details.
- **Default Login Page**—Using the dropdown menu, select the page that you want the FortiConnect to display immediately after you login.
- **Use High Contrast UI** - Click the check box to use a high contrast user interface.
- **Base Font Size** - From the drop down menu choose between Normal, Bigger or Biggest for a choice of font sizes.

The screenshot shows the 'My Settings' interface with the 'Preferences' tab selected. The settings are as follows:

- Language Template: English (Default)
- Default Timezone: America/Los\_Angeles
- Default Telephone Country Code: +1
- Default User Group: Default Account Group
- Default Device Group: Default Account Group
- First Name: Meru
- Last Name: Networks
- Email Address: merunetworks@meru.com
- Receive Email Confirmation:
- Default Login Page: Getting Started
- Use High Contrast UI:
- Base Font Size: Normal

At the bottom of the form are two buttons: 'Save' and 'Cancel'.

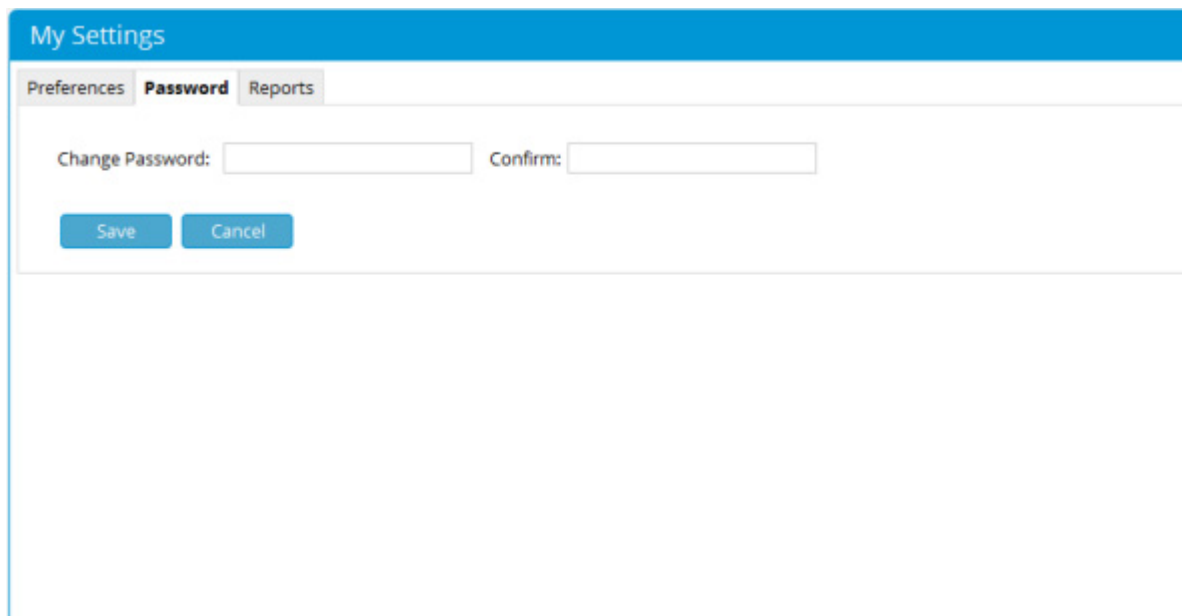
3. Click the **Save** button to save your default settings.

# Change Password

---

The Change Password option is enabled if your account is locally defined on the FortiConnect by your administrator. If you authenticated with a username/password from an external server such as Active Directory, you cannot view this option.

1. Navigate to **Home > My Settings**.
2. Click the **Password** tab as shown below.



The screenshot shows a web interface for 'My Settings'. At the top, there is a blue header bar with the text 'My Settings'. Below the header, there are three tabs: 'Preferences', 'Password', and 'Reports'. The 'Password' tab is selected and highlighted. Underneath the tabs, there are two input fields: 'Change Password:' followed by a text box, and 'Confirm:' followed by another text box. Below these fields, there are two buttons: 'Save' and 'Cancel'.

3. Enter your new password in the **Change Password** and **Confirm** fields.
4. Click the **Save** button to save your new password.

## Report Settings

---

You can select and deselect options you want to view in the Manage Accounts page or when exporting details from the Manage Accounts page.

1. Navigate to **Home > My Settings**

2. Click the **Reports** tab as shown below.

My Settings

Preferences Password **Reports**

	Report	Download
Created By:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Username:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MAC Address:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Password:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
First Name:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Last Name:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Email:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Company:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Status:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mobile Phone Number:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Start Time:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
End Time:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Timezone:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Account Group:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Usage Profile:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
option1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
option2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
option3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
option4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
option5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Event Code:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Time Remaining:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Price:	<input type="checkbox"/>	<input type="checkbox"/>

Save Cancel

3. Check or uncheck the check boxes based on the options to be displayed in the Manage Accounts page on downloading a report.
4. Click the **Save** button when finished.

# Creating Guest User Accounts

---

If you are assigned the appropriate permissions, you can create temporary user accounts.

1. Log into the FortiConnect as described in [Connecting to the FortiConnect](#).
2. Navigate to **Create Accounts > Create Guest Account**.
3. The Create Guest Account page appears as shown below.

**Note:** The screenshot below shows the default template for creating a Guest User Account. Your administrator has the option to add or remove other fields.

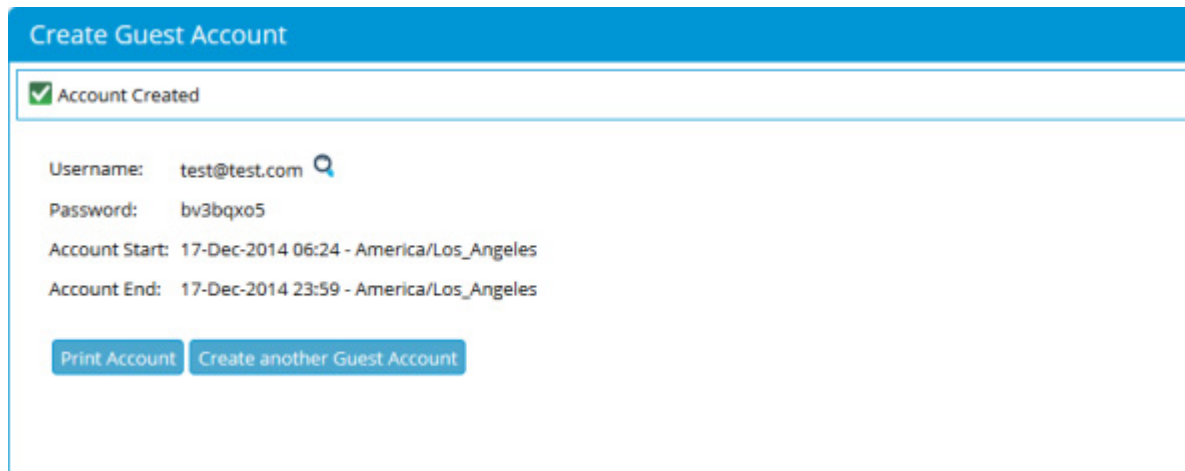
The screenshot shows the 'Create Guest Account' form with the following fields and values:

- First Name:
- Last Name:
- Company:
- Email Address:
- Mobile Phone Number: +1
- Timezone: America/Los\_Angeles
- Account Start: 2 Dec 2014 14:28
- Account End: 2 Dec 2014 23:59

Buttons: Add User, Cancel

4. Enter the **First Name** of your User. Enter the **Last Name** of your User.
5. Enter the **Company** or **organization** of your User. Enter the **Email Address** of your User.
6. Enter the **Mobile Phone Number** of your User.
7. Select the **Profile** from the dropdown menu. This dropdown appears automatically if your administrator has defined Usage Profiles and more than one profile is available.
8. Choose the **Timezone** relevant to the time and date.

9. From the **Account Start** field, choose the Time and Date from which you want the account to be valid.
10. From the **Account End** field, choose the Time and Date at which you want the account to end.
11. If the administrator for FortiConnect has configured any additional required account attributes, specify the appropriate information for those settings in this form.
12. Click the **Add User** button. The account is created and the details are displayed as shown below.



The screenshot displays a web interface titled "Create Guest Account". At the top, a blue header bar contains the title. Below the header, a green checkmark icon is followed by the text "Account Created". The main content area lists the following account details:

- Username: test@test.com
- Password: bv3bqxo5
- Account Start: 17-Dec-2014 06:24 - America/Los\_Angeles
- Account End: 17-Dec-2014 23:59 - America/Los\_Angeles

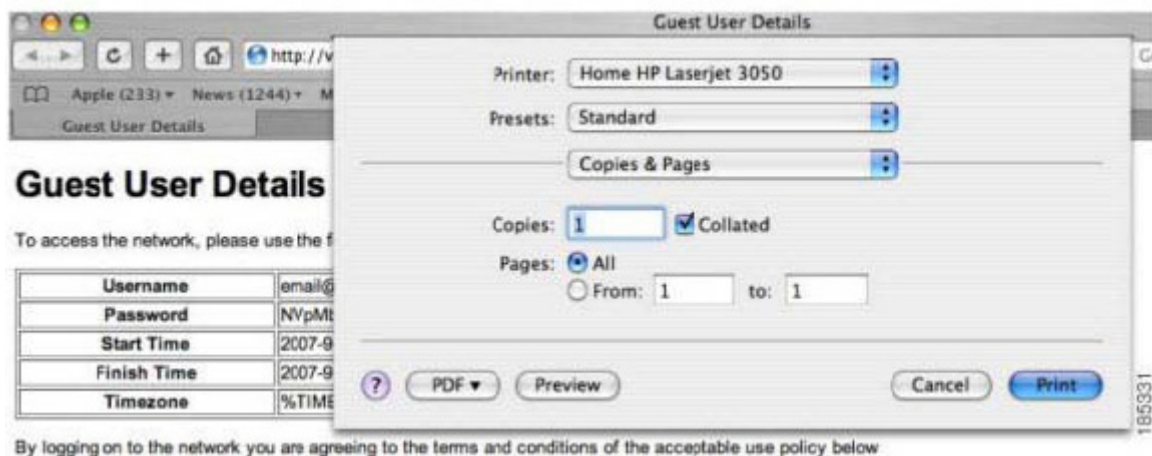
At the bottom of the form, there are two blue buttons: "Print Account" and "Create another Guest Account".

13. Depending on your permissions, you can perform one or all of the following actions on the same page where the new account details are displayed:
  - Clicking the **Print Account** button allows you to print the account details to your printer to hand to the User. These details commonly include User access instructions and usage policies. See [Print Account Details](#).
  - Clicking the **Email Account** button sends the account details to the email address you entered for the User. See [Email Account Details](#).
  - Clicking the **Send SMS Message** button sends the account details to the User's mobile phone via SMS text message. See [Text Message Account Details \(SMS\)](#).
14. You can also create another account immediately by clicking the **Create another Guest account** button.

# Print Account Details

---

1. Click the **Print Account** button from the Create Guest Account page shown below.



2. A new Printer window opens and you can print out the user details.

**Note:** After a User account is created, you can also access this feature by navigating to **Account Management > Manage Guests**. Find the required User account from the list displayed, then click on the printer icon, labelled print account details, adjacent to the User account on the far right of the screen

# Email Account Details

---

1. Click the **Email Account** button from the Create Guest Account page.
2. The FortiConnect sends an email to the email address specified when you created the account.

**Note:** After a User account is created, you can also access this feature by navigating to **Account Management > Manage Guests**. Find the required User account from the list displayed, then click on the envelope icon, labelled e-mail account details, adjacent to the User account on the far right of the screen.

# Text Message Account Details (SMS)

---

1. Click the **Send SMS Message** button from the Create Guest Account page.
2. The FortiConnect sends a text message to the phone number specified in the account creation.

**Note:** After a User account is created, you can also access this feature by navigating to Account Management > Manage Guests. Find the required User account from the list displayed, then click on the mobile phone icon, labelled Send SMS Message, adjacent to the User account on the far right of the screen.

## Multiple Guest Accounts

---

The FortiConnect allows you to create multiple accounts at the same time. The options available to you are configured by your administrator. They include:

- Creating Multiple Accounts from Text Entry
- Creating Multiple Accounts from CSV File
- Creating Multiple Random Accounts

You can create multiple accounts by pasting the details into the interface, importing a Comma Separated Values (CSV) file, or creating random accounts to be assigned to users (with the details recorded on paper) for input at a later time.

## Creating Multiple Guest Accounts from Text Entry

---

1. Navigate to **Create Accounts > Multiple Guest Accounts** and click on the **Multiple Guest Accounts** tab as shown below.





## Multiple Guest Accounts

Multiple Guest Accounts Random Guest Accounts

Choose File No file chosen

Import

[Download Template](#)

	First Name	Last Name	Company	Country Code	Mobile Phone Number	Email Address
				+1		

Timezone: America/Los\_Angeles

Account Start: 2 Dec 2014

14 33

Account End: 2 Dec 2014

23 59

Create Accounts

Cancel

- Download the CSV file by clicking the **Download Template** link and save this file locally.
- Fill out the fields in the CSV Template file using a program such as Microsoft Excel:
  - First Name** - The User's first name.
  - Last Name** - The User's last name
  - Company** - The User's company
  - Email Address** - The User's email address
  - Country Code** - The country code of the mobile phone number, for example 1 for the US, 44 for the UK.
  - Mobile Phone Number** - The User's mobile phone number.
  - Note - Do not enter hyphens in the number.
  - Other details** - Other details may be configured by your administrator and the names and descriptions are decided by them.
- Save the CSV Template file in CSV format.
- Click the **Browse** button to select your edited CSV file.
- Select the Profile from the dropdown menu. This dropdown appears automatically if your administrator has defined Usage Profiles and more than one profile is available.

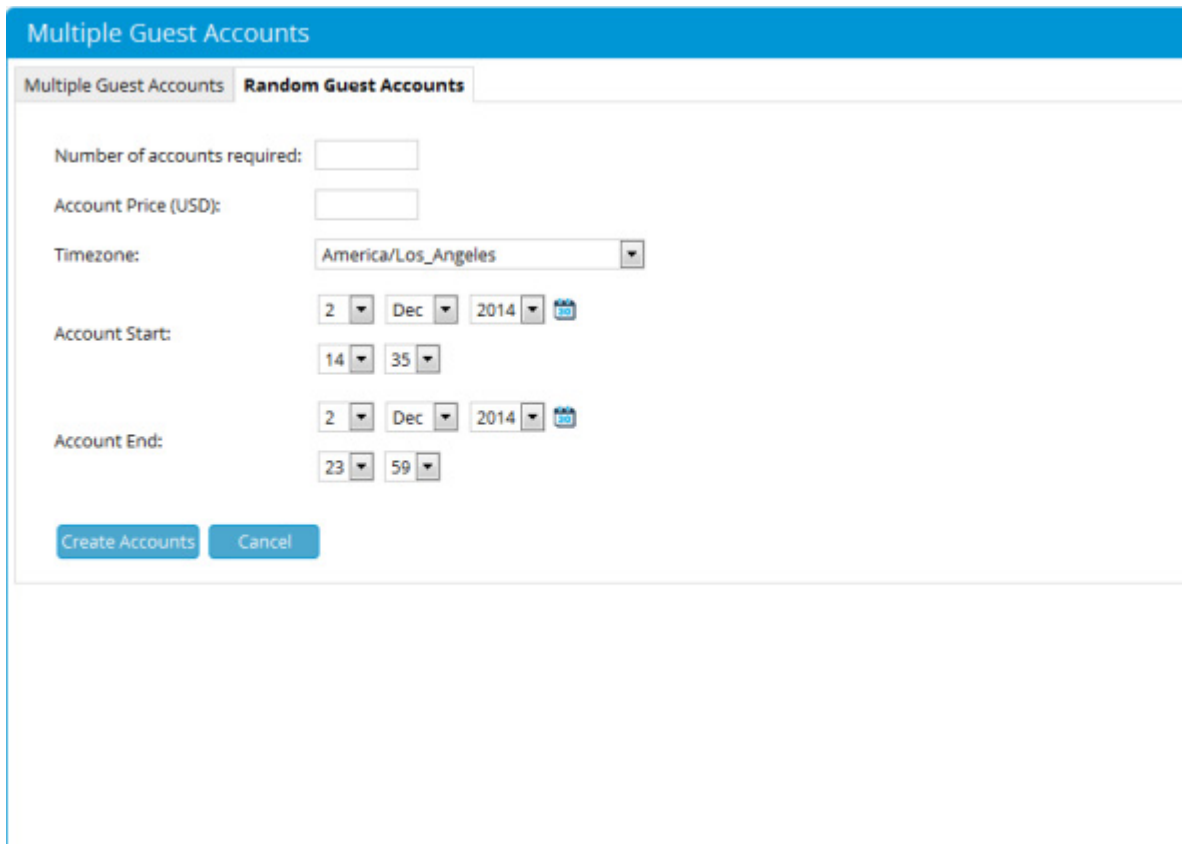
7. Select the relevant **Timezone** for the account.
8. Choose the **Account Start** time, and then the **Account End** time.
9. Click the **Import** button.

## Creating Multiple Random Guest Accounts

---

You can create random accounts when you need to hand out details to visitors, but do not have access to a computer at the time you need to create and provide the accounts to Users. This feature allows you to create accounts in advance and record the details on paper, and store them in the system for correlation at a later time.

1. Navigate to **Create Accounts > Multiple Guest Accounts** as shown below. and click on the **Random Guest Accounts** Tab.



The screenshot shows a web interface for creating multiple guest accounts. At the top, there is a blue header with the text "Multiple Guest Accounts". Below the header, there are two tabs: "Multiple Guest Accounts" and "Random Guest Accounts", with the latter being selected. The form contains the following fields and controls:

- Number of accounts required:** An empty text input field.
- Account Price (USD):** An empty text input field.
- Timezone:** A dropdown menu currently showing "America/Los\_Angeles".
- Account Start:** A date selector with three dropdowns for day (2), month (Dec), and year (2014), and a calendar icon.
- Account End:** A date selector with three dropdowns for day (23), month (Dec), and year (2014), and a calendar icon.
- Buttons:** Two buttons at the bottom: "Create Accounts" (highlighted in blue) and "Cancel".

2. Enter the number of accounts that you want to generate.
3. Select the **Profile** from the dropdown menu. This dropdown appears automatically if your administrator has defined Usage Profiles and more than one profile is available.

- Select the relevant **Timezone** for the account.
- Choose the **Account Start** time, and then the **Account End** time.
- Click the **Submit** button. The random accounts are created and displayed as shown below.

Multiple Account Details

Print All Download CSV

Showing 1-10 of 50 10 per page Go

Username ▲▼	Password ▲▼	MAC Address ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<a href="#">2k92HJqu</a>	ik8vx7f5l				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">2Wj8NooZ</a>	y59sidhb				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">3loQal4wr</a>	w49qzxoq				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">3WYvM6xf</a>	l4wni9fn				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">52LtvVdo</a>	j5wuqjd4				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">5K8vFZb</a>	wo3fbv7k				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">6cY0DpsY</a>	jjmun57y				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">6FFff4r</a>	qx8wkBoc				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">6UQ7kWp</a>	xyme6bx8				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">7ONadnH8</a>	y6idt6ye				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	

Page 1 of 5 Go

## Printing/Email/SMS Multiple Guest Accounts

When you have created accounts using one of the multiple account creation methods, the screen for the users details is slightly different than the one shown when a single User account is created. You can Email and SMS all accounts to each individual User after creation. You can also print the details for each individual account, or download the accounts file in CSV format.

- Navigate to **Account Management > Manage Account Batches** as shown below.

## Manage Account Batches

Username:

MAC Address:

Run

Cancel

Download CSV

Showing 1-1 of 1 10 per page Go

Batch ▲▼	Created By ▲▼	Created ▲▼	Accounts ▲▼	Total Value ▲▼
<a href="#">1417559865</a>	meru networks	02-Dec-2014 14:37	50	500.00 (USD)

Page 1 of 1 Go

- Determine the batch of accounts you have created by the Time/Date Created column or by checking the Created By column. Click the bulk account ID link you have created to view the **Multiple Account Details** page as shown below.

- When creating account batches, both for user and device accounts, the sponsor will be required to enter the batch name to place the accounts. If the sponsor specifies the name of an existing batch, the accounts will be added to that batch, if the sponsor specifies a new name, a new batch will be created with the accounts.

### Multiple Device Accounts

Browse... No file selected.  [Download Template](#)

	MAC Address	First Name	Last Name	Country Code	Mobile Phone Number	Email Address
				+1		

Batch Name:

Device Group:

Usage Profile:

Timezone:






























Account Start:

Account End:

## Multiple Account Details

Print All Suspend All Download CSV

Showing 1-10 of 50 10 per page Go

Username ▲▼	Password ▲▼	MAC Address ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<a href="#">2k0PHUqu</a>	k8vxff5l				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">2Wj8NooZ</a>	y59sidhb				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">3loQaLfw</a>	v49qzxoq				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">3WyyM6xf</a>	l4wni9fn				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">52LtvVdo</a>	j5wuqjd4				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">5K8vF2h</a>	wo3fbv7k				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">6cY0DgSV</a>	ljmun57y				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">6FFiff4r</a>	qx8wkc8oc				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">6UQ7jkWp</a>	xyme6bx8				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">7QHadnH8</a>	y6ldt6ye				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  

Page 1 of 5 Go

#### 4. From this page you can:

- **Print All** –Click to print out the account details created for each User.
- **Email All** –Click to email the account details created to each User.
- **SMS All** –Click to SMS the account details created to all User.
- **Suspend All** –Click to suspend all the bulk accounts you have created.
- **Download CSV**–Click to download a CSV file of the bulk accounts created.
- **Suspend an account**–Click the hazard icon.
- **Edit an account**–Click the pencil icon to edit the individual account selected.
- **View an account in detail**–Click the notepad icon to view the individual account details.
- **Print account details**–Click the printer icon to print the individual account details.

**Note:** When creating accounts with preset details (by either importing text or creating a CSV file), you can print, email, or transmit via SMS the User account details. However, when you create random accounts, you can only use the print option.

# Viewing Multiple Account Groups

---

When creating bulk accounts, you can view batches of accounts that were created at the same time using one of the following three methods:

- Viewing Multiple Account Groups
- Finding Multiple Account Groups by Username
- Finding Multiple Account Groups on the Active Accounts Report

## Viewing Multiple Account Groups

---




This option allows you to select the batch of accounts that you created.

1. Navigate to **Account Management > Manage Account Batches**.
2. Click the underlined link of the Bulk account ID you have created to bring up the **Multiple Account Details**.




## Multiple Account Details

[Print All](#)[Suspend All](#)[Download CSV](#)Showing 1-10 of 50 10 per page 

Username ▲▼	Password ▲▼	MAC Address ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<a href="#">2k0PHUqu</a>	k8vxff5l				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">2Wj8NxxZ</a>	y59sidhb				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">3lcQal6w</a>	v49qzxoq				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">3WyyM6xf</a>	l4wnl9fn				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">52LtvVdo</a>	j5wuqjd4				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">5K8vFIZh</a>	wo3fbv7k				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">6cY0QgkV</a>	jimun57y				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">6FFiff4r</a>	qx8wkb9oc				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">6UQ7jkWp</a>	xyme6bx8				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<a href="#">7QNadnH8</a>	y6idt6ye				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  

3. Click the underlined link of the account ID you have created to bring up the account details as shown below

## Guest Account Details

Username:	6cY0DgKV 
Password:	jimun57y
Status:	Active
Account Start:	02-Dec-2014 14:35 - America/Los_Angeles
Account End:	02-Dec-2014 23:59 - America/Los_Angeles
First Name:	Not available
Last Name:	Not available
Company:	Not available
Email Address:	Not available
Mobile Phone Number:	Not available
Usage Profile:	default
Account Group:	Default Account Group
Account Price (USD)	10.00

[Print Account](#)

[Suspend](#)

[Reset Password](#)

## Finding Multiple Account Groups by Username

---

This option allows you to find the batch of accounts by entering one username of the batch.

1. Navigate to **Account Management > Manage Account Batches**.
2. Enter a username that belongs to a batch of accounts in the Username field and click the **Submit** button.

If found, the batch of accounts, that were created in the same operation as the username submitted, is displayed.

## Finding Bulk Account Groups on the Active Accounts Report

---

This option allows you to find the batch of accounts from the Active Accounts Report page.

1. Navigate to **Account Management > Manage Account Batches**.
2. Click the underlined link of the Bulk account ID you have created to go to the **Manage Accounts** page for the bulk-created accounts. You can edit individual accounts in this page by clicking on the pencil icon next to the account you wish to edit.

Multiple Account Details

Print All Suspend All Download CSV

Showing 1-10 of 50 10 per page Go

Username ▲▼	Password ▲▼	MAC Address ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<a href="#">2k0PHUqu</a>	k8vxff5l				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">2WJ8NxxZ</a>	y59sidhb				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">3loQal6w</a>	v49qzxoq				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">3WyyM6Xf</a>	l4wnl9fn				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">52LtvVdo</a>	j5wuqjd4				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">5K8vEIZh</a>	wo3fbv7k				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">6c00gkV</a>	jimun57y				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">6FFiff4r</a>	qx8wk8oc				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<a href="#">6UQ7jkWp</a>	xyme6bx8				Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	

## Managing Guest Accounts

You can view all accounts that have been created at any time using the **Manage Guests** page.































1. From the Main page select **Account Management > Report and Manage Accounts**.
2. On the Manage Accounts page, you can view the list of accounts that have been created as shown below. The fields displayed on this page can be customized using Report Settings.

## Report & Manage Accounts

Created By: meru Status: Inactive,Active,Pending Approval: Active Time between 02-Nov-2014 01:00 and 02-Jan-2015 00:00 [Advanced Search >>](#)

[Run](#) [Save as Default](#) [Reset to Default](#) [Download CSV](#)

Showing 1-10 of 51 10 per page Go

<input type="checkbox"/>	Created By ▲▼	Username ▲▼	MAC Address ▲▼	Password ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<input type="checkbox"/>	meru networks	<a href="#">meru@meru.com</a>		5aj@gehq	User	One	Active	02-Dec-2014 14:28 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">BJCG2NH7</a>		tm9wpm6			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">na3Z9Qet</a>		ggk2ra3b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">n9PYU3r4</a>		jk6vrl3t			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">Fcapk23ef</a>		9exl5lci			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">5k8vrl2h</a>		wo3fbv7k			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">y5Xa8Q1f</a>		zq3prwo3			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">KUm49msj</a>		9lbulu4d			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">w7Tg2v4tp</a>		anlwo9b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">6JQ7j6Wp</a>		xyme6bx8			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  

Page 1 of 6 Go

# Editing Guest Accounts

If you create an account for a User and you need to extend their account access, you can change the expiry date and time of the account.

1. From the Main page select **Account Management > Report and Manage Accounts**.
2. In the **Manage Guests** page you can view a list of the accounts that you can edit as shown below.

## Report & Manage Accounts

Created By: meru networks; Status: Inactive,Active,Pending Approval; Active Time between 02-Nov-2014 01:00 and 02-Jan-2015 00:00

[Advanced Search >>](#)























[Run](#)

[Save as Default](#)

[Reset to Default](#)

[Download CSV](#)

Showing 1-10 of 51 10 per page [Go](#)

<input type="checkbox"/>	Created By ▲▼	Username ▲▼	MAC Address ▲▼	Password ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<input type="checkbox"/>	meru networks	<a href="#">meru@meru.com</a>		Saj@gehg	User	One	Active	02-Dec-2014 14:28 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">BjCG0NH7</a>		tmf9wpm6			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">nx3Z9Qet</a>		ggk2ra3b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">rPPYU3r4</a>		jk6vr3t			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">Eqpk23ef</a>		9xv15ki			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">2K8vFRz</a>		wo3bv7k			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">y5Xa9QTI</a>		zq3prwo3			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">Kj,m49mjU</a>		9lbulu4d			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">w7Tg7u4hp</a>		anl8wo9b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">6UQ7k0xp</a>		xyme6bxll			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  

Page 1 of 6 [Go](#)

[Suspend All](#)

3. Click the **pencil** icon next to the account you want to change to go to the Edit User Accounts page Guest Self Service as shown below.

## Edit User Account

Username: meru@meru.com

First Name:

Last Name:

Company:

Email Address:

Mobile Phone Number:

Re-apply usage profile:

4. Change the Account details.
5. Click the **Save Changes** button to update the account with the new details.

# AP Usage Summary

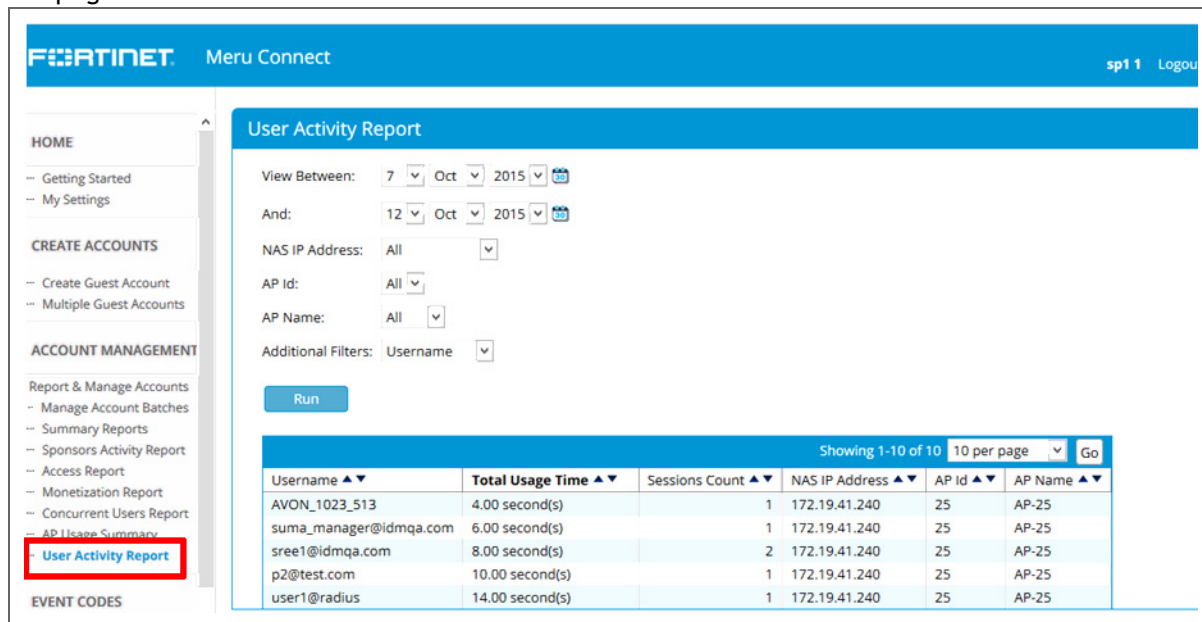
Shows total unique users, total usage time and sessions count based on AP Name and NAS IP Address. From the main page select **Account Management > AP Usage Summary** to bring up the AP Usage Summary report page as shown below.

The screenshot displays the 'AP Usage Summary' report page. On the left is a navigation menu with sections: HOME, GETTING STARTED (Getting Started, My Settings), CREATE ACCOUNTS (Create Guest Account, Multiple Guest Accounts), and ACCOUNT MANAGEMENT (Report & Manage Accounts, Manage Account Batches, Summary Reports, Sponsors Activity Report, Access Report, Monetization Report, Concurrent Users Report, **AP Usage Summary**, User Activity Report). The main content area has a blue header 'AP Usage Summary'. Below it are filters: 'View Between: 11 Jan 2015' and 'Anc: 12 Oct 2015', followed by a 'Run' button. A table shows usage data for AP 25. The table has columns: AP Name, NAS IP Address, Total Unique Users, Total Usage Time, and Sessions Count. The data row shows AP 25 with NAS IP 172.19.41.240, 12 unique users, 1 hour(s), 42 minute(s) usage time, and 23 sessions. The page shows 1-1 of 1 results, 10 per page, and is Page 1 of 1.

AP Name ▲▼	NAS IP Address ▲▼	Total Unique Users ▲▼	Total Usage Time ▲▼	Sessions Count ▲▼
<a href="#">AP 25</a>	172.19.41.240	12	1 hour(s), 42 minute(s)	23

# User Activity Report

Shows total usage time, sessions count for each User based on AP Name, AP ID and NAS IP Address. From the main page select **Account Management > User Activity Report** to bring up the User Activity Report page as shown below.



The screenshot shows the Meru Connect interface. The top navigation bar includes the logo, 'Meru Connect', and 'sp1 1 Logou'. The left sidebar contains a menu with categories: HOME, CREATE ACCOUNTS, ACCOUNT MANAGEMENT, and EVENT CODES. Under ACCOUNT MANAGEMENT, 'User Activity Report' is highlighted with a red box. The main content area is titled 'User Activity Report' and contains a form with the following fields:

- View Between: 7 Oct 2015
- And: 12 Oct 2015
- NAS IP Address: All
- AP ID: All
- AP Name: All
- Additional Filters: Username

A 'Run' button is located below the form. Below the form is a table showing the results of the report. The table has the following columns: Username, Total Usage Time, Sessions Count, NAS IP Address, AP Id, and AP Name. The table shows 6 rows of data.

Username	Total Usage Time	Sessions Count	NAS IP Address	AP Id	AP Name
AVON_1023_513	4.00 second(s)	1	172.19.41.240	25	AP-25
suma_manager@idmqa.com	6.00 second(s)	1	172.19.41.240	25	AP-25
sree1@idmqa.com	8.00 second(s)	2	172.19.41.240	25	AP-25
p2@test.com	10.00 second(s)	1	172.19.41.240	25	AP-25
user1@radius	14.00 second(s)	1	172.19.41.240	25	AP-25

## Advanced Search

1. If your Account Management page returns a large number of users, you can perform an advanced search by clicking the **Advanced Search** button as shown below.



## Report & Manage Accounts

Created By: meru networks; Status: Inactive.Active.Pending Approval; Active Time between 02-Nov-2014 00:00 and 02-Jan-2015 00:00 << Advanced Search

Sponsor Group:	All	Active Time Between:	2 Nov 2014
Created By:	meru networks		00 00
Guest Portal:		And:	2 Jan 2015
Username:			00 00
MAC Address:		Timezone:	All
First Name:		IP Address:	
Last Name:		Usage Profile:	
Company:		Account Group:	
Email:		Event Code:	
Mobile Phone Number:			
Inactive:	<input checked="" type="checkbox"/>		
Active:	<input checked="" type="checkbox"/>		
Expired:	<input type="checkbox"/>		
Suspended:	<input type="checkbox"/>		
Pending Approval:	<input checked="" type="checkbox"/>		
Rejected:	<input type="checkbox"/>		

Run

Save as Default

Reset to Default

Download CSV

2. In the Advanced Search page that is displayed, you can enter the following criteria to make your search:

- **Sponsor Group** - From the drop down menu select a sponsor group to search in.
- **Created by**—Sponsor who created the account.
- **Guest Portal** - Search for a User on a specific portal they authenticated on.
- **Username** - Search for a User by their allocated username.
- **MAC Address** - Search using a specific MAC Address.
- **First Name**—First Name of User.
- **Last Name**—Last name of User.
- **Company**—Company or Organization of User.
- **Email**—Email address of User.
- **Mobile Phone Number** - Mobile number of User.
- **Active Time Between**—Start Time from which the search to start.
- **And** —End Time at which the search to end.
- **Timezone**—From the dropdown menu select a timezone to be searched.
- **IP Address**—IP Address of User workstation.
- **Usage Profile** - Search by Usage Profile
- **Time Profile** - Search by a specific Time Profile.

- **Guest Role** - Search by a specific Guest Role.
  - **Event Code** - Search by a specific Event Code.
  - **Inactive**—Select this option to include search for Inactive accounts.
  - **Active**—Select this option to include search for Active accounts.
  - **Expired**—Select this option to include search for Expired accounts.
  - **Suspended**—Select this option to include search for Suspended accounts.
  - **Pending Approval** - Used when creating Event Codes, this will list accounts pending approval by Sponsor.
  - **Rejected** -Used when creating Event Codes, this will list accounts rejected by Sponsor.
3. Click the **Run** button to search based on the given criteria. If your search criteria matches any accounts in the database, they are displayed.
  4. Click the **Save as Default** option to save your current search as a default search.
  5. Click on the **Reset to Default** option if you have made other searches and wish to revert back to your saved default search.
  6. Click on **Download as CSV** if you wish to download your search as a CSV file.

## Suspending Guest Accounts

---

You can terminate an account so that a User can no longer login. To do this, you need to contact your network administrator to make sure that the user has been removed from the network. Depending on the access method, this may happen automatically. Suspending does not delete the account, but marks the account as suspended so that it cannot be used anymore.



**Note:** Account suspension will only work if the controller in use supports 'Change of Authorization'.

1. Select **Account Management > Report and Manage Accounts** as shown below.

## Report & Manage Accounts

Created By: meru networks; Status: Inactive,Active,Pending Approval; Active Time between 02-Nov-2014 00:00 and 02-Jan-2015 00:00

[Advanced Search >>](#)































[Run](#)

[Save as Default](#)

[Reset to Default](#)

[Download CSV](#)

Showing 1-10 of 51 10 per page Go

<input type="checkbox"/>	Created By ▲▼	Username ▲▼	MAC Address ▲▼	Password ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<input type="checkbox"/>	meru networks	<a href="#">meru@meru.com</a>		5aj8gehg	User	One	Active	02-Dec-2014 14:28 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">8JCG6NH7</a>		tm09wpm6			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">nc379Qe4</a>		gpk2ra3b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">rPPYU3rd</a>		jk6vr33t			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">Fqpk23af</a>		9ex5ldi			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">5K8vF2h</a>		wo3fbv7k			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">y5Xe9QTF</a>		zq3prwo3			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">Klmaf9mU</a>		9lbulu4d			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">w77g7uHp</a>		an8wo9b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  
<input type="checkbox"/>	meru networks	<a href="#">6UQ7kWp</a>		xyme6bx8			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	  

Page 1 of 6 Go

[Suspend All](#)

2. Click the **suspend** icon next to the account you want to terminate. The account is removed from the list and the User will not be able to login anymore.
3. To Suspend more than once account, place a check in the check box of each account you wish to suspend and then click on the **Suspend All** button to suspend the selected accounts.

**Note:** You can revive the account at a later date by performing an advanced search for suspended accounts and clicking on the revive account icon.

## Charging and Refunding Transactions on Purchased Guest Accounts

If a User has purchased an account through a Guest Portal using the Payment Provider option, you can now charge or refund that Users payment if necessary.

# 1. Go to Account Management --> Report and Manage Guests

Report & Manage Accounts

Status: Inactive,Active,Pending Approval: Active Time between 17-Nov-2014 00:00 and 17-Jan-2015 00:00 [Advanced Search >>](#)

[Run](#) [Save as Default](#) [Reset to Default](#) [Download CSV](#)

Showing 1-5 of 5 10 per page [Go](#)

Created By	Username	MAC Address	Password	First Name	Last Name	Status	Start Time	End Time	
local	sp6b68b6c		sp6b7eum			Active	17-Dec-2014 06:18 America/Los_Angeles	17-Dec-2014 23:59 America/Los_Angeles	
local		sp6b6cc11:22:33		test	device	Active	17-Dec-2014 06:31 America/Los_Angeles	17-Dec-2014 23:59 America/Los_Angeles	
identitynetworks.com	dfuser1			DFuser1	Last Name	Active	17-Dec-2014 11:54 Europe/London	17-Dec-2014 23:54 Europe/London	
identitynetworks.com	dfuser2			DFuser2		Active	17-Dec-2014 12:07 Europe/London	18-Dec-2014 00:07 Europe/London	
login	test@test.com2		Bsp6RH8H	aanjum		Active			

[Suspend All](#)

# 2. Click on the Currency Unit Icon as shown on the far right, and this will display the screen below.

Charge/Refund & Payments Report: test@test.com2

Showing 1-4 of 4 10 per page [Go](#)

Transaction ID	Customer	Guest Portal	Payment Account	Access Plan	(USD) Amount	Date
2225724394	aanjum	login	Auth	plan1	2.00 = 2 + 0 @0%	17-Dec-2014 06:29:17
Added By: local					5.00	17-Dec-2014 06:37:01
Added By: local					5.00	17-Dec-2014 08:54:55
Added By: local					-2.00	17-Dec-2014 08:54:58

Transaction Type:  Charge  
 Refund

Amount:  (USD)

Reason:

Note: Manually added transactions are only recorded for the guest, they are not charged/refunded on the payment system. This must be done manually in the relevant payment systems interface.

[Add](#) [Cancel](#) [Send Purchase Receipt](#)

# 3. This displays the Transaction ID and the history related to it. To refund a payment :

- **Transaction Type** - Click on the Charge or Refund option depending on which you wish to do.
- **Amount** - Enter the amount you wish to charge or refund.
- **Reason** - Enter a reason for the charge or refund.
- Click **Add** to add the charge the User or refund the User.

# Creating Event Codes

---

FortiConnect has the ability to allow a sponsor to create Event Codes which would allow Users to create their own accounts when they were invited to an Event and the code generated by the Sponsor was given to them. The Users would be subject to the timeout of that Code depending on how long an Event was created for, be it a morning seminar or a week long conference.

Event Codes can be created in the Sponsor interface and then issued to Users who will then access the Hotspot created for that Event and self register.

If you have the correct permissions to set up Event Codes, you will see the the options to Create and Manage Event codes at your **Getting Started** screen :-

# Creating Event Codes

---

To create an Event Code goto **Event Codes --> Create Event Codes**.

## Create Event Code

**Details**

Code Name:

Description:

Accounts can be created between:

And:

Timezone:

Account Limit:  Maximum Created Accounts  Maximum number of accounts that can be created for this event  
 Maximum Active Accounts  Maximum number of accounts that can be active at any one time

**Note:** You will only see this option if your Administrator has given you the relevant permissions

1. Enter the following information in the fields provided
  - **Code Name** - Enter the Name of the Code that will be provided to your Users.
  - **Description** - Enter a Description of the Event
  - **Accounts can be created between** - From the drop down menus and date pickers, select the start and end dates you wish Users to be able to create their own accounts.
  - **Timezone** - Enter the Timezone that event will occur in.
  - **Account Limit - Maximum Created Accounts** - Enter the maximum number of accounts that can be created for the Event.
  - **Account Limit - Maximum Active Accounts** - Enter the maximum number of accounts that can be active at anyone time for the Event.
2. Click on **Create Event Code** when complete.
3. Once this has been completed you will see an extra tab appear, **Time Restrictions**, you can use this screen to restrict Users from creating their accounts between certain times.
4. Click on the **Time Restrictions** tab as shown below.

**Edit Event Code**

Details **Time Restrictions**

Guests cannot create their accounts using this event code during these periods

No current restrictions for this event code

Monday

5. Enter the restrictions you wish to impose using the drop down tabs provided and click on **Add** after each one.

You are now ready to issue your Event Code to Users so that they can Self Register when ready

## Managing Event Codes

---

Click on **Manage Event Codes** in the Event Codes section.




1. From the **Manage Events Code** page you can tailor and run a report using the fields provided as shown below.

Manage Event Codes

Created By:  Active Time Between: 2 Nov 2014

Code Name:  And: 1 Jan 2015

Showing 1-1 of 1 10 per page Go

Created By ▲▼	Code Name ▲▼	Status ▲▼	Accounts can be created between ▲▼	And ▲▼	Account Group ▲▼	Usage Profile ▲▼	
meru networks	<a href="#">Event_One</a>	Active	02-Dec-2014 14:54 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	Default Account Group	default	  

Page 1 of 1 Go




- This will list all the event codes that have been created and then can be managed accordingly -
  - Click on the **suspend** icon to suspend the Event.

Manage Event Codes

Created By:  Active Time Between: 2 Nov 2014

Code Name:  And: 1 Jan 2015

Showing 1-1 of 1 10 per page Go

Created By ▲▼	Code Name ▲▼	Status ▲▼	Accounts can be created between ▲▼	And ▲▼	Account Group ▲▼	Usage Profile ▲▼	
meru networks	<a href="#">Event_One</a>	Active	02-Dec-2014 14:54 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	Default Account Group	default	  

Page 1 of 1 Go

The page at 192.168.137.20 says:

Are you sure you want to suspend this event code?

- Click on the **edit** icon to edit the details of the Event.





## Edit Event Code

### Details Time Restrictions

Code Name:

Description:

Accounts can be created between:    

And:    

Timezone:

Account Limit:  Maximum Created Accounts  Maximum number of accounts that can be created for this event

Maximum Active Accounts  Maximum number of accounts that can be active at any one time

Edit any changes and click on **Edit Event Code** to confirm.

- Click on the **view accounts** icon to view the Users that have created their own accounts for the Event so far.

## Report & Manage Accounts

Event Code: Event One: Active Time between 02-Dec-2014 14:54 and 02-Dec-2014 23:59

Sponsor Group:	All	Active Time Between:	2	Dec	2014
Created By:			14	54	
Guest Portal:		And:	2	Dec	2014
Username:			23	59	
MAC Address:		Timezone:	All		
First Name:		IP Address:			
Last Name:		Usage Profile:			
Company:		Account Group:			
Email:		Event Code:	Event One		
Mobile Phone Number:					
Inactive:	<input type="checkbox"/>				
Active:	<input type="checkbox"/>				
Expired:	<input type="checkbox"/>				
Suspended:	<input type="checkbox"/>				
Pending Approval:	<input type="checkbox"/>				
Rejected:	<input type="checkbox"/>				

Run

Save as Default

Reset to Default

Download CSV

10 per page

Go

<input type="checkbox"/>	Created By	Username	MAC Address	Password	First Name	Last Name	Status	Start Time	End Time
--------------------------	------------	----------	-------------	----------	------------	-----------	--------	------------	----------

No Records Found

To perform an advanced search click on the Advanced Search Button as shown below under **Account Management-->Report & Manage Accounts**.

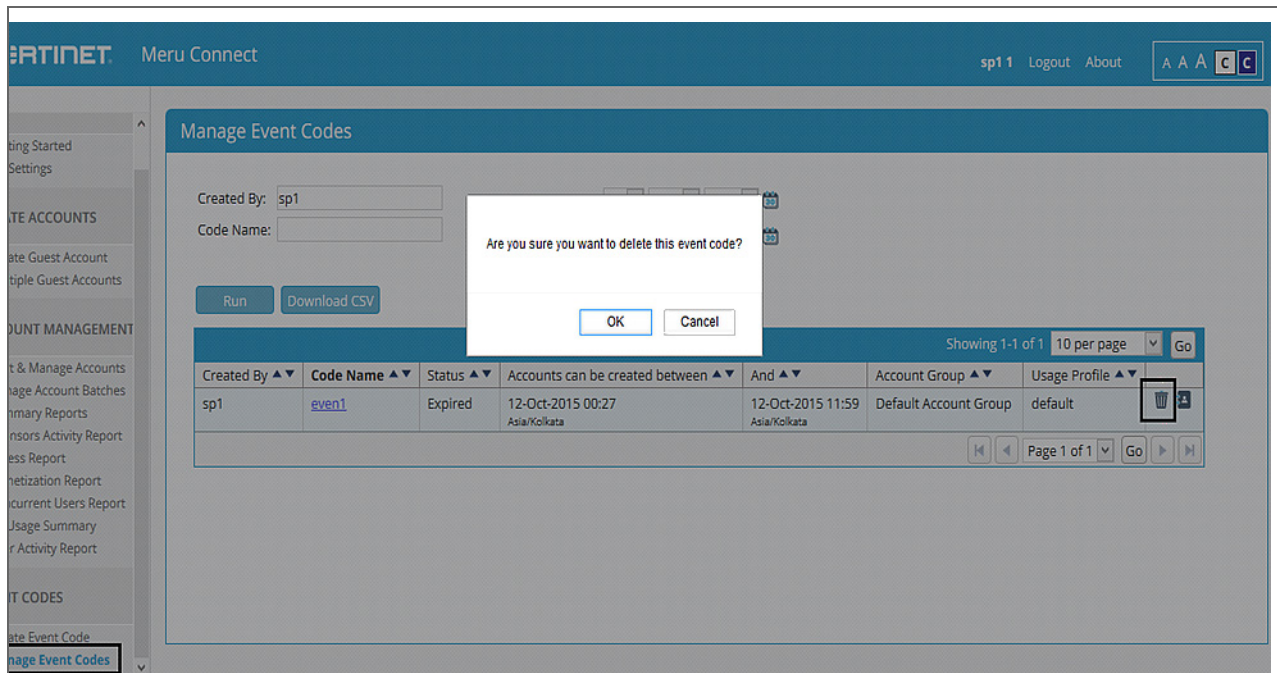
Searches can be made using the relevant search criteria entered into the correct search fields.

## Delete expired event codes

A sponsor can delete an expired event code from the **Manage event codes** page. Sponsor should have "Manage Event Codes" permission to delete expired event code.

**Step 1** Select **Event Codes > Manage Event Codes**.

**Step 2** Click **Delete** icon next to the event code to delete the event code




## Viewing Active Accounts and Resending Details

FortiConnect provides an Active Accounts page that allows you to view the active accounts that you created or accounts that you have permissions to view. This page allows you to view, print, email or text message (SMS) the account access details to Users if they have lost or forgotten them.

1. Select **Account Management > Report & Manage Guests** to display a list of active accounts.
2. Click the username of the User to which you wish to resend details as shown below.

## Guest Account Details

Username: test@test.com2   
Password: Bsp6RH8H  
Status: Active  
Maximum Duration: 1 hour(s), 0 minute(s)  
First Name: aanjum  
Last Name: Not available  
Company: Not available  
Email Address: test@test.com  
Mobile Phone Number: +44 00000000000  
Usage Profile: 1 Hour  
Account Group: Default Account Group

[Print Account](#)

[Email Account](#)

[Send SMS Message](#)

[Suspend](#)

[Send Purchase Receipt](#)

[Reset Password](#)

From this page you can click the relevant buttons:

- **Print Account**—Prints the account.
- **Email Account**—Sends email the account to the User.
- **Send SMS Message**—Sends an SMS message of the account details to the User.
- **Suspend** —Suspend the User account.
- **Send Purchase Receipt** - Resend a Purchase receipt to a purchased account.

# Reporting on Guest Users

---

If you have the appropriate permissions, you can generate full reporting on User user accounts. You can run reports to view who created User accounts, when they were created, and access details for the Users themselves, such login time, logout time, and IP address used.

1. From the Main page, select **Account Management > Report & Manage Guests** to display a list of active accounts as shown below.
2. Select the user for which you wish to view reporting, and click the **notepad** icon to view the detailed report for that user.
3. Click the **Accounting Log** tab as shown below for the RADIUS accounting information for that User including:
  - **Total Download** - Total Download Usage in KB
  - **Total Upload** - Total Upload Usage in KB
  - **Total Time Online**
  - **NAS IP Address**—NAS IP address the User user was specified.
  - **Users IP Address**—IP Address assigned to the User.
  - **Logged In**—Time at which the User logged in.
  - **Logged Out**—Time at which the User logged out.
  - **Duration**—Duration of time the User remained logged in the account.
  - **Download KB** - Total amount of data downloaded by User.
  - **Upload KB** - Total amount of data uploaded by User.
  - **Chargeable User ID** - The Chargeable User ID attached to the account
  - **Operator Name** - Operator Name of the account
  - **AP ID** - AP ID account came via
  - **AP Name** - AP Name account came via

Report & Manage Accounts: meru@meru.com

Accounting Log | Audit Log | Activity Log | User Certificates

Total download: 0 KB  
 Total upload: 0 KB  
 Total time online: 0.00 second(s)

Download CSV

10 per page Go

NAS IP Address ▲▼	User's IP Address: ▲▼	Calling Station Id ▲▼	Logged In ▲▼	Logged Out ▲▼	Duration	Download KB ▲▼	Upload KB ▲▼	Chargeable User Id ▲▼	Operator Name ▲▼	AP Id ▲▼	AP Name ▲▼
No Records Found											

4. Click the **Audit Log** tab as shown below to view the audit entries for that User account including:
  - **Sponsor**—Sponsor ID.
  - **Action**—Audit entry action.
  - **Date/Time**—Date and Time of audit entry action.

Report & Manage Accounts: meru@meru.com

Accounting Log | **Audit Log** | Activity Log | User Certificates

Download CSV

Showing 1-1 of 1 10 per page Go

Sponsor ▲▼	Action ▲▼	Date/Time ▲▼
meru networks	Guest account created [username=meru@meru.com] [id=2003]	02-Dec-2014 14:31:47

Page 1 of 1 Go

5. Click the **Activity Log** tab as shown below to view the activities performed by the User for that account, including firewall information if your administrator has allowed that functionality.

Report & Manage Accounts: Fqpk23ef

Accounting Log Audit Log **Activity Log** User Certificates

Activity Data last loaded 02-Dec-2014 16:02:44 Refresh

Network Device IP:

Message Contains:

Use regular expressions:

Between: 2 Nov 2014 And: 2 Dec 2014  
 16 02 16 02

Run Download CSV

10 per page Go

Date/Time	Device	Message
No Records Found		

Search criteria include:

- **Network Device IP**—IP address of any network device you wish to search.
- **Message Contains**—Enter any text you wish to search for within the logs.
- **Use regular expression**—Check this checkbox to search for the specified text that matches with regular expression. You can use Perl compatible regular expressions in the search.
- **Between**—Enter Date and Time from which you want to start your search.
- **And**—Enter Date and Time at which you want to end your search.

6. Click the **Run** button once you have completed selecting your criteria. Once the search is completed, you can click the **Download** button to save your results to a file.

Returned information includes:

- **Date/Time field**—Displays the date and time of the User's actions.
- **Device**—The device on which the User's actions took place.
- **Message**—Displays the User's actions.

# Creating Device Accounts

---

If you are assigned the appropriate permissions, you can create temporary device accounts.

1. Log into the FortiConnect as described in [Connecting to the FortiConnect](#).
2. Navigate to **Create Accounts > Create Device Account**.
3. The Create Device Account page appears as shown in Figure devaccpage.

**Note:** The screenshot below shows the default template for creating a Device Account. Your administrator has the option to add or remove other fields.

The screenshot shows the 'Create Device Account' form with the following fields and values:

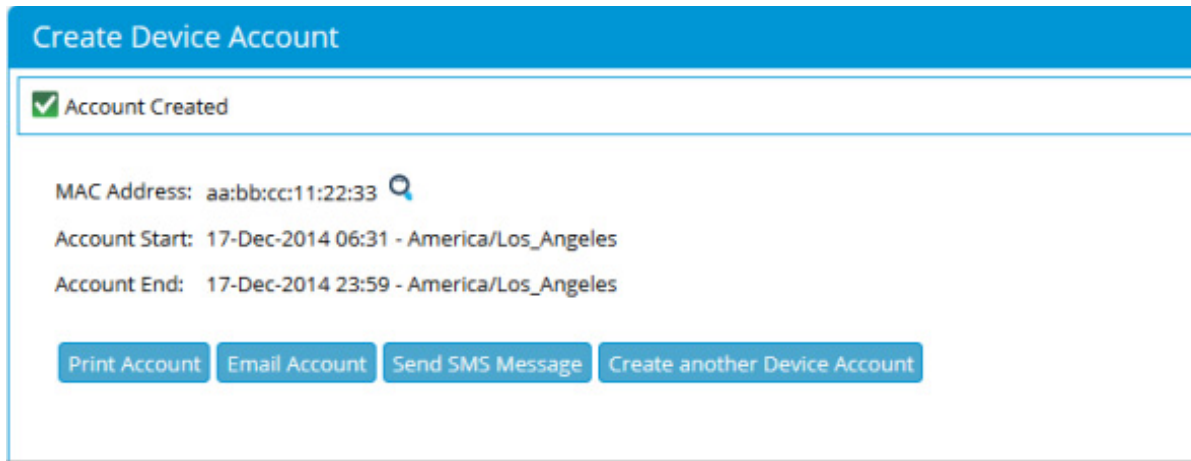
- MAC Address:
- First Name:
- Last Name:
- Company:
- Email Address:
- Mobile Phone Number: +1
- Timezone: America/Los\_Angeles
- Account Start: 2 Dec 2014 16:04
- Account End: 2 Dec 2014 23:59

Buttons: Add Device, Cancel

4. Enter the **MAC Address** of the device then follow the steps below to enter the details of the User requesting the device be added onto the network.
5. Enter the **First Name** of your User.
6. Enter the **Last Name** of your User.
7. Enter the **Company** or **organization** of your User. Enter the **Email Address** of your User.
8. Enter the **Mobile Phone Number** of your User.
9. Select the **Guest Role** from the dropdown menu. This dropdown appears automatically if your administrator has defined User roles and more than one role is available.



10. Choose the **Timezone** relevant to the time and date.
11. From the **Account Start** field, choose the Time and Date from which you want the account to be valid.
12. From the **Account End** field, choose the Time and Date at which you want the account to end.
13. If the administrator for FortiConnect has configured any additional required account attributes, specify the appropriate information for those settings in this form.
14. Click the **Add Device** button. The account is created and the details are displayed as shown below.



**Create Device Account**

✓ Account Created

MAC Address: aa:bb:cc:11:22:33 🔍

Account Start: 17-Dec-2014 06:31 - America/Los\_Angeles

Account End: 17-Dec-2014 23:59 - America/Los\_Angeles

Print Account   Email Account   Send SMS Message   Create another Device Account

15. Depending on your permissions, you can perform one or all of the following actions on the same page where the new account details are displayed:
  - Clicking the **Print Account** button allows you to print the account details to your printer to hand to the User. These details commonly include User access instructions and usage policies. See [Print Account Details](#).
16. You can also create another account immediately by clicking the **Create another Device account** button.

## Multiple Device Accounts

---

The FortiConnect allows you to create multiple device accounts at the same time. The options available to you are configured by your administrator. They include:

- Creating Multiple Device Accounts from Text Entry
- Creating Multiple Device Accounts from CSV File

You can create multiple accounts by pasting the details into the interface or importing a Comma Separated Values (CSV) file.

# Creating Multiple Device Accounts from Text Entry

---

1. Navigate to **Create Accounts--> Multiple Device Accounts** as shown below

Multiple Device Accounts

Choose File No file chosen Import Download Template

MAC Address	First Name	Last Name	Company	Country Code	Mobile Phone Number	Email Address
				+1		

Timezone: America/Los\_Angeles

Account Start: 2 Dec 2014

Account End: 23 Dec 2014

Create Accounts Cancel

2. Enter the details in the grid fields as required with a cell separating the values.
3. Select the **Guest Role** from the dropdown menu. This dropdown appears automatically if your administrator has defined User roles and more than one role is available.
4. Select the relevant **Timezone** for the account.
5. Choose the **Account Start time**, and then the **Account End time**.
6. Click the **Create Accounts** button.

# Creating Multiple Device Accounts from CSV File

---

1. Navigate to **Create Accounts > Multiple Device Accounts** as shown below.

	MAC Address	First Name	Last Name

2. Download the CSV file by clicking the **Download Template** link and save this file locally.
3. Fill out the fields in the CSV Template file using a program such as Microsoft Excel:
  - **MAC Address** - The device MAC Address.
  - **First Name** – The User’s first name requesting the device be added.
  - **Last Name** – The User’s last name requesting the device be added.
  - **Company** – The User’s company requesting the device be added.
  - **Email Address** – The User’s email address requesting the device be added.
  - **Country Code** - The country code of the mobile phone number, for example 1 for the US, 44 for the UK.
  - **Mobile Phone Number** – The User’s mobile phone number requesting the device be added.  
**NOTE: Do not enter hyphens in the number.**
  - **Other details** - Other details may be configured by your administrator and the names and descriptions are decided by them.
4. Save the CSV Template file in CSV format.
5. Click the **Browse** button to select your edited CSV file.

6. Select the **Guest Role** from the dropdown menu. This dropdown appears automatically if your administrator has defined Usage Profiles and more than one profile is available.
7. Select the relevant **Timezone** for the account.
8. Choose the **Account Start** time, and then the **Account End** time.
9. Click the **Import** button.

## Managing Device Accounts

You can view all accounts that have been created at any time.









































1. From the Main page select **Account Management > Report and Manage Accounts**.
2. On the Manage Devices page, you can view the list of accounts that have been created as shown below. The fields displayed on this page can be customized using Report Settings.

Report & Manage Accounts

Created By: meru Status: Inactive.Active.Pending Approval Active Time between 02-Nov-2014 00:00 and 02-Jan-2015 00:00 [Advanced Search >>](#)

Run Save as Default Reset to Default Download CSV

Showing 1-10 of 52 10 per page Go

<input type="checkbox"/>	Created By ▲▼	Username ▲▼	MAC Address ▲▼	Password ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<input type="checkbox"/>	meru		1e2d81ad211921		test	test	Active	02-Dec-2014 16:04 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	meru@meru.com		5aj8g9hg	User	One	Active	02-Dec-2014 14:28 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	RJCGNH7		tm9wpm6			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	nx3Z90et		gpk2ra3b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	rFPYU3r4		jk0vrf3t			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	Eopk23ef		9exd5ci			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	5k8vf12h		wo3fbv7k			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	y5xw9Q1f		zq3prwo3			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	KLm49mJ		9lbulu4d			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	w7TgDu4n		ani8wo9b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   

Page 1 of 6 Go

## Editing Device Accounts

If you create an account for a device and you need to extend its account access, you can change the expiry date and time of the account.









































1. From the Main page select Account Management > Report and Manage Accounts.

Report & Manage Accounts

Created By: meru; Status: Inactive,Active,Pending Approval; Active Time between 02-Nov-2014 00:00 and 02-Jan-2015 00:00 [Advanced Search >>](#)

[Run](#) [Save as Default](#) [Reset to Default](#) [Download CSV](#)

Showing 1-10 of 52 10 per page [Go](#)

<input type="checkbox"/>	Created By ▲▼	Username ▲▼	MAC Address ▲▼	Password ▲▼	First Name ▲▼	Last Name ▲▼	Status ▲▼	Start Time ▲▼	End Time ▲▼	
<input type="checkbox"/>	meru		<a href="#">1e2d41a1211d1</a>		test	test	Active	02-Dec-2014 16:04 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	<a href="#">meru@meru.com</a>		Saj@gehg	User	One	Active	02-Dec-2014 14:28 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	<a href="#">BjCG2NH7</a>		tm9wpm6			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	<a href="#">nx379Qet</a>		gpk2ra3b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	<a href="#">rPPVJ3rd</a>		jk6vrl3t			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	<a href="#">Fqpk23ef</a>		9exl5lc			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	<a href="#">5k0vf12h</a>		wo3fbv7k			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	<a href="#">y5w49Q1f</a>		zq3prwo3			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	<a href="#">Klm49mL</a>		9lbu4d			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   
<input type="checkbox"/>	meru networks	<a href="#">w7Tg7uHp</a>		anlwo9b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	   

Page 1 of 6 [Go](#)

2. Click the pencil icon next to the account you want to change to go to the Edit Device Account page as shown below.

## Edit Device Account

MAC Address:	1e:2d:1a:12:11:21
First Name:	<input type="text" value="test"/>
Last Name:	<input type="text" value="test"/>
Company:	<input type="text" value="test"/>
Email Address:	<input type="text" value="test@test.com"/>
Mobile Phone Number:	+1 <input type="text" value="122434325235"/>
Re-apply usage profile:	<input type="text" value="No change (default)"/>

Save Changes

Cancel

3. Change the Account details.
4. Click the **Save Changes** button to update the account with the new details.

## Advanced Device Search

---

1. If your Account Management page returns a large number of devices, you can perform an advanced search by clicking the **Advanced Search button** as shown below.

## Report & Manage Accounts

Created By: meru Status: Inactive,Active,Pending Approval: Active Time between 02-Nov-2014 00:00 and 02-Jan-2015 00:00 << Advanced Search

Sponsor Group:	All	Active Time Between:	2 Nov 2014
Created By:	meru		00 00
Guest Portal:		And:	2 Jan 2015
Username:			00 00
MAC Address:		Timezone:	All
First Name:		IP Address:	
Last Name:		Usage Profile:	
Company:		Account Group:	
Email:		Event Code:	
Mobile Phone Number:			
Inactive:	<input checked="" type="checkbox"/>		
Active:	<input checked="" type="checkbox"/>		
Expired:	<input type="checkbox"/>		
Suspended:	<input type="checkbox"/>		
Pending Approval:	<input checked="" type="checkbox"/>		
Rejected:	<input type="checkbox"/>		

Run Save as Default Reset to Default Download CSV

- In the Advanced Search page that is displayed, you can enter the **following** criteria to make your search:
  - Created by**—Sponsor who created the account.
  - MAC Address** - MAC Address of device
  - First Name**—First Name of User.
  - Last Name**—Last name of User.
  - Company**—Company or Organization of User device.
  - Email**—Email address of User device.
  - Start Time Between**—Start Time from which the search to start.
  - End Time Between**—End Time at which the search to end.
  - Timezone**—From the dropdown menu select a timezone to be searched.
  - Inactive**—Select this option to include search for Inactive accounts.
  - Active**—Select this option to include search for Active accounts.
  - Expired**—Select this option to include search for Expired accounts.
  - Suspended**—Select this option to include search for Suspended accounts.
- Click the **Run** button to search based on the given criteria. If your search criteria matches any accounts in the database, they are displayed.
- Click the **Save as Default** option to save your current search as a default search.

- Click on the **Reset to Default** option if you have made other searches and wish to revert back to your saved default search.
- Click on **Download as CSV** if you wish to download your search as a CSV file.

**Note:** Remember that not all device search criteria will be relevant to that of a User search.

## Suspending Device Accounts

You can terminate an account so that a device can no longer login. Depending on the access method, this may happen automatically. Suspending does not delete the account, but marks the account as suspended so that it cannot be used anymore.



**Note:** Account disconnection will only work if the controller in use supports 'Change of Authorization', suspension of accounts will always work.

- Select **Account Management > Manage Devices** as shown below.

Report & Manage Accounts

Selected guest account(s) suspended

Created By: meru; Status: Inactive,Active,Pending Approval; Active Time between 02-Nov-2014 00:00 and 02-Jan-2015 00:00 [Advanced Search >>](#)

[Run](#)
[Save as Default](#)
[Reset to Default](#)
[Download CSV](#)

Showing 1-10 of 50										
	Created By	Username	MAC Address	Password	First Name	Last Name	Status	Start Time	End Time	
<input type="checkbox"/>	meru networks	<a href="#">BjCG2Nc7</a>		tmi9wpm6			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<input type="checkbox"/>	meru networks	<a href="#">nx3Z9Qst</a>		ggk2ra3b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<input type="checkbox"/>	meru networks	<a href="#">rPPYU3t4</a>		jk6vr3t			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<input type="checkbox"/>	meru networks	<a href="#">Fqpk33ef</a>		9ex0lci			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<input type="checkbox"/>	meru networks	<a href="#">5K8vF2h</a>		wo3fbv7k			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<input type="checkbox"/>	meru networks	<a href="#">y5Xe9QIf</a>		zq3prwo3			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<input type="checkbox"/>	meru networks	<a href="#">Kl.m49msJ</a>		9lbulu4d			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<input type="checkbox"/>	meru networks	<a href="#">w7Tg7uHp</a>		an8wo9b			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<input type="checkbox"/>	meru networks	<a href="#">6UQ7JKWp</a>		xyrne6bx8			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	
<input type="checkbox"/>	meru networks	<a href="#">lqchm3eJ</a>		gade9gq4			Active	02-Dec-2014 14:35 America/Los_Angeles	02-Dec-2014 23:59 America/Los_Angeles	

Page 1 of 5

[Suspend All](#)



2. Check the check box of the accounts you wish to suspend then Click the **Suspend All** button. The account is removed from the list and the device will not be able to login anymore.

## Mobile Device User Interface

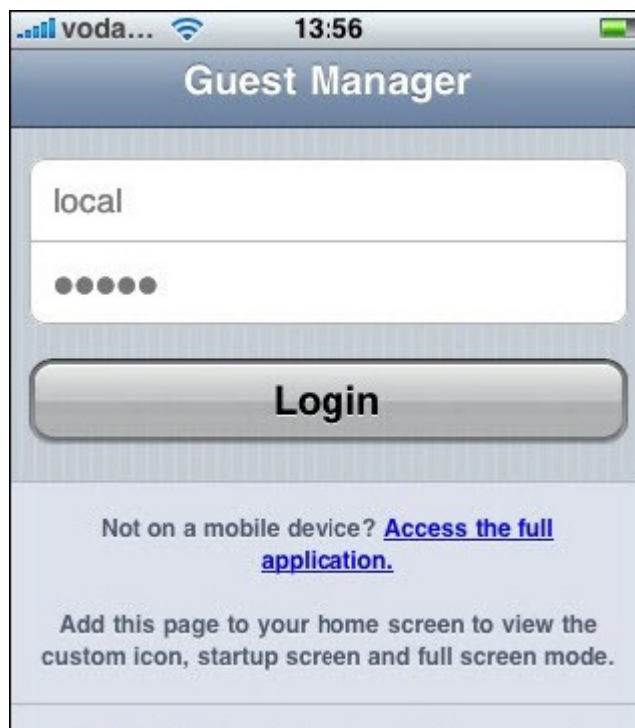
---

Sponsors can create Users using a mobile device as long as the sponsor has the correct administrative permissions to create accounts.

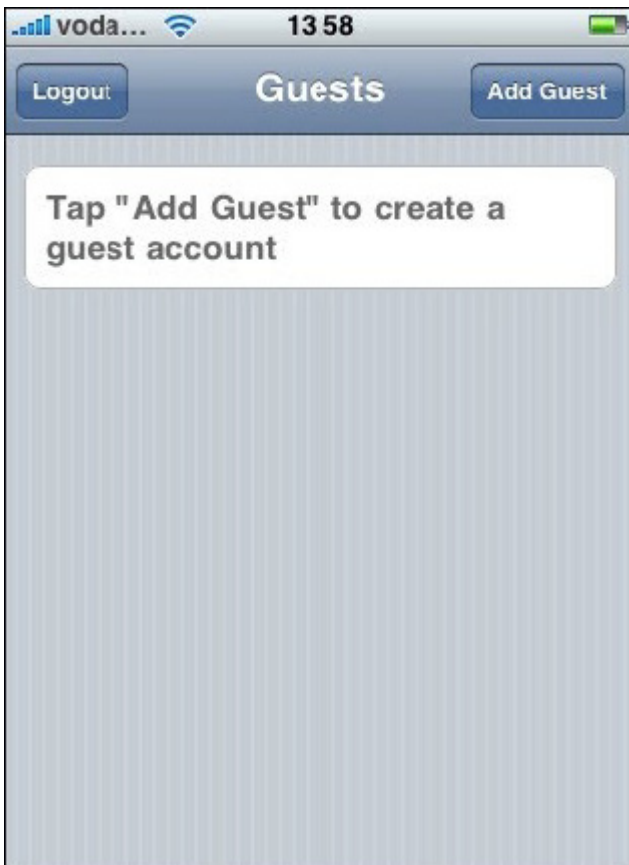
**Note:** Compatible with I-Phones, Android and Blackberrys. Although some older browsers on these devices may not support the Mobile User Interface.

**Note:** Screenshots below are of the I-Phone and may differ on other Mobile Devices

1. Using your Mobile device, navigate to your FortiConnect Management browser as shown below.



2. Enter your **Username** and **Password** in the fields provided and tap on the **Login** button, this should bring up the Mobile UI home page as shown below.



3. Tap on the **Add Guest** button to create a User account and enter the information required in the fields provided as shown below.

The screenshot shows an iPhone interface for adding a guest. At the top, the status bar displays 'voda...', signal strength, Wi-Fi, and the time '13:58'. Below this is a blue header bar with a 'Back' button on the left and the title 'Add Guest' in the center. The main content area contains a series of white input fields with rounded corners and light gray borders. The fields are labeled: 'First Name', 'Last Name', 'Company', 'Email Address', '+1 Mobile Phone Number', a dropdown menu with 'default' selected and a right-pointing chevron, and 'Ends today at 07:00' with a right-pointing chevron. At the bottom of the form is a large, rounded rectangular button with a gradient and the text 'Add' in bold black font.

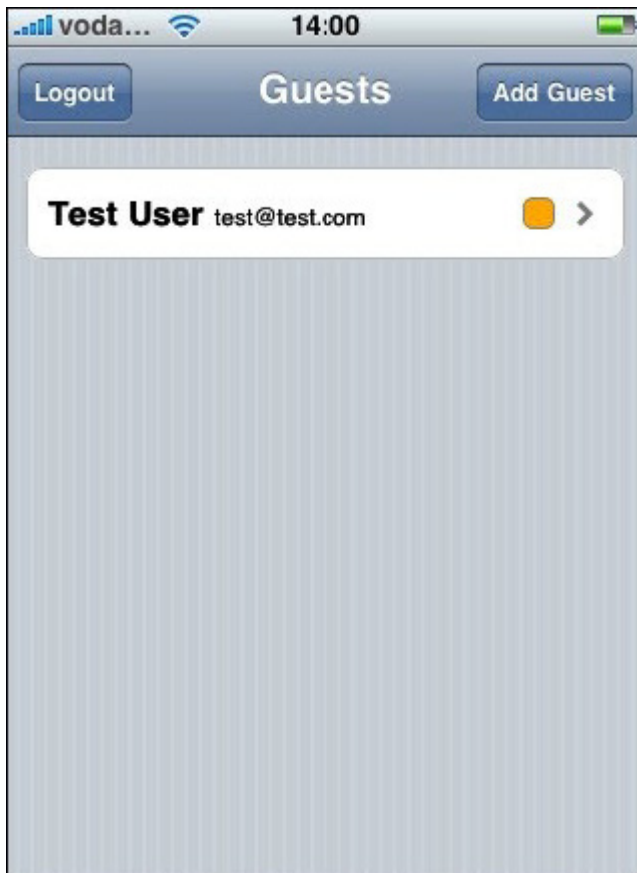
4. In the fields provided enter the following :-
- First Name - First Name of the User user
  - Last Name - Last Name of the User user
  - Company - Company name of the User user
  - Email Address - Email Address of the User user
  - Mobile Phone Number - Users mobile phone number
  - Group - Default by standard, but tap the > icon to see more groups if applicable.
  - End time - Tap the > icon to select a time you with the users access to end by.

Tap on the **Add** button once complete.

5. Once you have selected **Add** the user details will show as per below.



6. Tap on the **Back** button to return back to your Mobile UI home screen.



7. To check the status of any of the Users you have created on your Mobile UI home screen tap on the > icon next to the User.



Once you have finished with your Mobile UI, tap the **Logout** button on the Mobile UI home page to logout.

## Concurrent Users Report

---

A Sponsor may also be able to run a report on Users that are concurrently connected to the Network at any one time and see license usage and licenses used over a specific period.

1. From the Sponsor User Interface, go to **Account Management-->Concurrent Users Report** as shown below.

## Concurrent Users Report

View Between: 25 Nov 2014

And: 2 Dec 2014

Username:

MAC Address:

Created By:   
Enter either the sponsor's username or the user's domain name

Show Connected Only:

Run

Created By ▲▼	Username ▲▼	MAC Address ▲▼	Logged In ▲▼	Logged Out ▲▼	IP Address ▲▼	NAS IP Address ▲▼
No Records Found						

2. Select which dates you wish to run the report from and to using the **View Between** date picker.
  - **License Type** - To run a report on a specific license type use the drop down menu to select.
  - **Username** - To run a report on a specific User enter the username of the User. Leave blank to search for all.
  - **MAC Address** - To run a report on a MAC address enter the MAC address details here.
  - **Created by** - To run a report on Users created by a specific sponsor enter the sponsors username, leave blank to search for all.
  - **Show Connected Only** - Place a check in the check box to show connected Users only
3. Once the report has run, a list of connected Users will appear.
  - Click the **Link** icon to disconnect the active User from the Network.
  - Click the **suspend** icon to suspend the Users account.

### Concurrent Guests Report

View Between: 10 Dec 2014

And: 17 Dec 2014

Username:

MAC Address:

Created By:

Enter either the sponsor's username or the user's domain name

Show Connected Only:

**Run**

Created By ▲▼	Username ▲▼	MAC Address ▲▼	Logged In ▲▼	Logged Out ▲▼	IP Address ▲▼	NAS IP Address ▲▼	
identitynetworks.com	dfuser1	a0f4:50:5f:7eaf	17-Dec-2014 05:48		10.1.210.109	10.1.210.45	
identitynetworks.com	DFUser1 Last Name	00:1c:bf:04:97:6b	17-Dec-2014 04:41	17-Dec-2014 04:57	10.1.210.104	10.1.210.45	
identitynetworks.com	dfuser1	00:1c:bf:04:97:6b	17-Dec-2014 04:40	17-Dec-2014 04:41	10.1.210.104	10.1.210.45	
identitynetworks.com	dfuser2	30:85:a9:62:64:cf	17-Dec-2014 04:38		10.1.210.105	10.1.210.45	
identitynetworks.com	DFUser2	c8:85:50:89:34:b8	17-Dec-2014 04:37		10.1.210.103	10.1.210.45	
identitynetworks.com	DFUser2	c8:85:50:89:34:b8	17-Dec-2014 04:31	17-Dec-2014 04:35		10.1.210.45	
identitynetworks.com	DFUser2	c8:85:50:89:34:b8	17-Dec-2014 04:28	17-Dec-2014 04:31		10.1.210.45	
identitynetworks.com	dfuser1	00:25:d3:bf:f3:2a	17-Dec-2014 04:28	17-Dec-2014 04:34	10.1.210.106	10.1.210.45	
identitynetworks.com	dfuser1	38:aa:3c:45:75:c8	17-Dec-2014 04:23	17-Dec-2014 04:35	10.1.210.108	10.1.210.45	
identitynetworks.com	DFUser2	c8:85:50:89:34:b8	17-Dec-2014 04:19	17-Dec-2014 04:28	10.1.210.103	10.1.210.45	

Showing 1-10 of 34 10 per page Go

Page 1 of 4 Go

4. The report will also detail the License Type and Overall License Usage below.

## Sponsor Reporting

Sponsors can view reports under the Account Management section to view the summary, activity and access details for their own account and other sponsor accounts.

## Summary Reports

1. From the main page select **Account Management > Summary Reports** to bring up the summary reports page as shown below.



## Summary Reports

View Summary Between: 2 Nov 2014 And: 2 Dec 2014

Total Guest Accounts Created: **52**  
Total Authenticated Guests: **0**  
Total Cumulative Connect Time: **0.00 second(s)**

2. Select a search criteria using the date pickers provided and click the **Submit** button.
3. The screen displays:
  - Total Guest Accounts Created.
  - Total Authenticated Guests.
  - Total Cumulative Connect Time.

## Sponsors Activity Report

---

1. From the main page, select **Account Management > Sponsors Activity Report** to display the Sponsors Activity Report page as shown below.

**Sponsors Activity Report**

Guest accounts created between: 2 Nov 2014

And: 2 Dec 2014

Only show sponsors who have created more than 0 accounts

**Run**

Showing 1-2 of 2 10 per page Go

Username ▲▼	Accounts Created ▲▼	Email ▲▼
meru	1	meru@meru.co.uk
meru networks	51	merunetworks@meru.com

meru networks (51) meru (1)

**Top 10 Sponsors**

Total Logins Created: 52

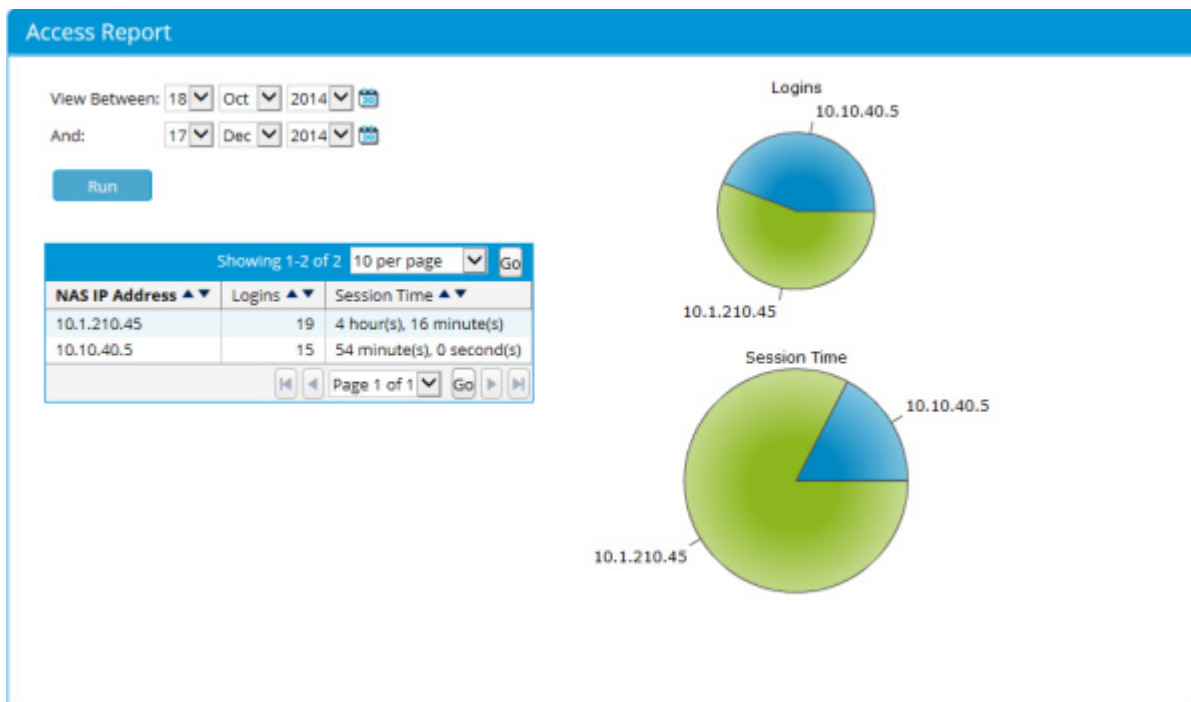
2. Select a search criteria using the date pickers provided. You can also select a minimum number of Users created by sponsor.
3. When completed, click the **Run** button. The screen displays:
  - **Username**—Username of sponsor.
  - **Total Accounts Created**—Accounts created by sponsor.
  - **Email**—Email address of sponsor.

A pie chart of the top ten sponsors, who created the accounts, is also displayed.

## Access Reports

---

1. Navigate to **Account Management > Access Report** to go to the Access Report page as shown below.



2. Select a search criteria using the date pickers provided and click the **Run** button.
3. The screen displays the number of logins made by the enforcement device (IP Address) and its session time.

## Monetization Report

---

In some environments, credit card based purchases are not widely used and they are much more interested in using access codes with currency denominations attached to them.

Currency Denominations can be set up within the Admin interface, when this is set, it will allow a sponsor to create a number of random User accounts assigned to a time profile, and then export them to a CSV file to print off and then create an offline coupon or scratch card to distribute to the User.

Once the batches have been created and distributed, we can report on them using the report below.

From the Sponsor Portal go to **Account Management --> Monetization Report** as shown below

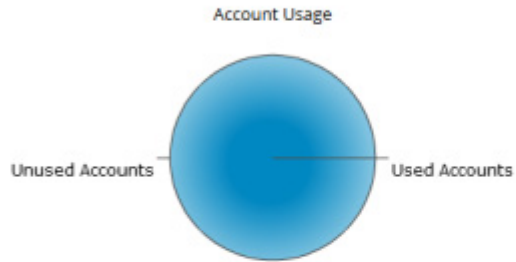
## Monetization Report

Guest accounts created between: 17 Nov 2014

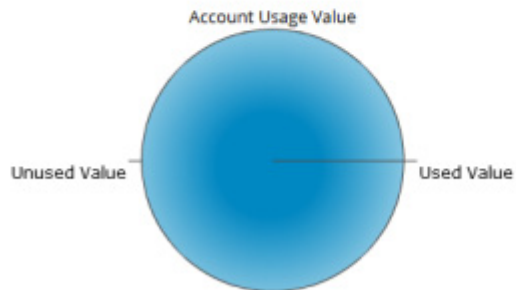
And: 17 Dec 2014

Run

Number of accounts used: **0**  
Number of unused accounts: **2**  
Total number of accounts created: **2**



Value of accounts used: **0 (USD)**  
Value of unused accounts: **40 (USD)**  
Total value of accounts created: **40(USD)**



This appendix discusses API support for the FortiConnect. It describes the following:

- Overview
- Authentication Requirements
- Time Format
- API Operations
- Status Codes
- Error Codes
- Valid Timezones

## Overview

---

FortiConnect provides an API that allows you to perform certain operations using HTTP or HTTPS via POST or GET operations. The FortiConnect API is accessed via <https://serveripaddress/sponsor/api/GuestAccount.php> or <http://serveripaddress//sponsor/api/GuestAccount.php>.

To use this API, note the following:

- Competency with a programming language (e.g. C, Java, Perl, PHP) is required and you must install the relevant software on the machine that runs these programs to call this API.
- Fortinet does not support debugging of custom programs using the API. It only supports running API calls.

## Authentication Requirements

---

Access over HTTP or HTTPS for the API is based upon the SSL settings for the web

Administration interface as defined in [Accessing the FortiConnect Using HTTP or HTTPS](#).

A valid username and password is also required to authenticate as a sponsor against the following components:

- Local database
- Active directory server as defined in admin settings
- LDAP server as defined in admin settings
- RADIUS as defined in admin settings

For example, the following call uses the username “sponsor” with password “mypass”:

<http://1.1.1.1/sponsor/api/GuestAccount.php?username=sponsor&password=mypass&method=createCarter&email=test@fortinet.com&role=DEFAULT&company=fortinet&mobileNumber=12345484345&startTime=20100210T10%3A45%3A00&endTime=20100211T13%3A15%3A00&timezone=Europe%2FLondon&timeProfile=default>

**Note:** All fields must be URL encoded, e.g. date/time fields have been encoded so the colon has been replaced with %3A

## Time Formats

---

All dates/times must be specified in a particular ISO 8601 format: YYYYMMDDTHH:MM:SS where:

- YYYY is the 4-digit year
- MM is the 2-digit month
- DD is the 2-digit day of the month
- T is a literal T
- HH is the 2-digit hour (24 hour format)
- MM is the 2-digit minute
- SS is the 2-digit second

e.g. 20100304T08:45:30 is 4 March 2010, 08:45:30

See [http://en.wikipedia.org/wiki/ISO\\_8601](http://en.wikipedia.org/wiki/ISO_8601) for details.

## API Operations

---

You can use the API by passing the details either through a POST or GET operation to the Identity Manager API.

The following example shows a GET operation to obtain the version of the API and Identity Manager.

`https://1.1.1.1/sponsor/api/GuestAccount.php?`

`username=sponsor&password=mypass&method=getVersion`

All data is returned as XML.

# XML Response

---

All responses are provided in the following XML format:

```
<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  ....
</response>
```

In the case of an error, the code and message elements are set with the error code and error text. Internal errors also return a <details> element that contains developer information to help address the issue.

## create

---

The create method creates a guest user account in accordance with the sponsor's permissions.

### Required In Parameters

- method (required): create
- username (required): Sponsor account username
- password (required): Sponsor account password
- firstName (based on policy): Guest user first name
- surname (based on policy): Guest user surname
- email (based on policy): Guest user email address
- accountGroup - name of account group (string)
- company (based on policy): Guest user company name

- phonecode (based on policy): Telephone code for the Guest user mobile telephone (e.g. +44)
- mobilenumber (based on policy): Mobile telephone number for the Guest user
- timezone (required): The timezone in which the guest account is created (as detailed in Valid Timezones, page A-13)
- option1 (based on policy): Optional data field 1
- option2 (based on policy): Optional data field 2
- option3 (based on policy): Optional data field 3
- option4 (based on policy): Optional data field 4
- option5 (based on policy): Optional data field 5
- startTime (required): The time the account is due to start
- endTime (required): The time the account should end
- timeProfile (required): The time profile to use when creating the account

## Example

1. The following example creates an account with the following guest details:

- First Name: John
- Surname: Carter
- Email: johncart@fortinet.com
- Role: DEFAULT (as created in the user role interface)
- Company: Fortinet
- Mobile Number (cellphone): 12345 48434532
- Phone Code: 123
- Start Time: 29th November 2008 (midnight)
- EndTime: 30th November 2008 (midnight)
- Timezone: Europe/London
- Time Profile: StartEnd (as created in the time profile user interface)

2. Call the API as follows:

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=create&firstName=John&surname=Carter&email=johnc40fortinet.com&role=DEFAULT&company=fortinet&mobileNumber=12345+48434532&phoneCode=-11-29&endTime=2008-11-30&timezone=Europe%2FLondon&timeProfile=StartEnd>

3. If successful, a response is returned:

```
<?xml version="1.0"?>
```

```
<response>
```

```
  <status>
```



```
<code>0</code>
<message>Success</message>
</status>
<account/>
<account>
  <id>815</id>
  <firstName>John</firstName>
  <surname>Carter</surname>
  <company>Fortinet</company>
  <email>johncart@fortinet.com</email>
  <mobileNumber>12345 48434532</mobileNumber>
  <phoneCode>123</phoneCode>
  <option1/>
  <option2/>
  <option3/>
  <option4/>
  <option5/>
  <username>JohnCarter10</username>
  <password>!B,4N!32(F1{VJ2</password>
  <status>1</status>
  <bulkId/>
  <timezone>Europe/London</timezone>
  <startTimeT>2008-11-29T00:00:00+00:00</startTimeT>
  <endTimeT>2008-11-30T00:00:00+00:00</endTimeT>
  <role/>
  <createdTime/>
  <modifiedUsername>1</modifiedUsername>
  <timeProfile>
    <id>2</id>
```

```
<name>StartEnd</name>
<description/>
<duration>0</duration>
<accountType>1</accountType>
<durationUnit>Days</durationUnit>
<durationInUnits>0</durationInUnits>
<restriction>
  <id>43</id>
  <weekDay>1</weekDay>
  <startTime>00:00</startTime>
  <endTime>08:59</endTime>
</restriction>
<restriction>
  <id>45</id>
  <weekDay>3</weekDay>
  <startTime>00:00</startTime>
  <endTime>08:59</endTime>
</restriction>
<restriction>
  <id>50</id>
  <weekDay>3</weekDay>
  <startTime>17:00</startTime>
  <endTime>23:59</endTime>
</restriction>
<restriction>
  <id>51</id>
  <weekDay>4</weekDay>
  <startTime>17:00</startTime>
  <endTime>23:59</endTime>
```

```
</restriction>
<restriction>
  <id>47</id>
  <weekDay>5</weekDay>
  <startTime>00:00</startTime>
  <endTime>08:59</endTime>
</restriction>
<restriction>
  <id>54</id>
  <weekDay>7</weekDay>
  <startTime>00:00</startTime>
  <endTime>23:59</endTime>
</restriction>
</timeProfile>
</account>
</response>
```

## edit

---

The edit method edits an existing user account in accordance with sponsor's permissions.

You may edit any of the fields associated with an existing account with the following exceptions:

- start time
- role
- time profile
- time zone

To edit an account, you must supply the account ID as returned by the create method.

## Required In Parameters

- method (required): edit

- id (required): The database ID of the account to be edited
- username (required): Sponsor account username
- password (required): Sponsor account password
- firstName (optional): Guest user first name
- surname (optional): Guest user surname
- email (optional): Guest user email address
- group (optional): The role in which the guest user is created
- company (optional): Guest user company name
- phonecode (optional): Telephone code for the Guest user mobile telephone (e.g. +44)
- cellnumber (optional): Cell telephone number for the Guest user
- timezone (optional): The timezone in which the guest account is created (as detailed in Valid Timezones)
- option1 (optional): Optional data field 1
- option2 (optional): Optional data field 2
- option3 (optional): Optional data field 3
- option4 (optional): Optional data field 4
- option5 (optional): Optional data field 5
- startTime (optional): The time the account is due to start
- endTime (optional): The time the account should end
- timeProfile (optional): The time profiler to use when creating the account

## Example

The following example changes the mobile phone (cell phone) number for the account with ID 794:

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=edit&id=794&mobileNumber=12345678>

The full account detail is returned as with the getDetails method.

```
<?xml version="1.0"?>
```

```
<response>
```

```
  <status>
```

```
    <code>0</code>
```

```
    <message>Success</message>
```

```
  </status>
```

```
</account/>
```

```
<account>
```

```
<id>794</id>
<firstName>John</firstName>
<surname>Carter</surname>
<company>Fortinet</company>
<email>johncart@fortinet.com</email>
<mobileNumber>12345678</mobileNumber>
<phoneCode>123</phoneCode>
<option1>1</option1>
<option2>1</option2>
<option3>1</option3>
<option4>1</option4>
<option5>1</option5>
<username>jcarter</username>
<password>Fortinet</password>
<status>1</status>
<bulkId/>
<timezone>Europe/London</timezone>
<startTimeT>2008-10-28T00:00:00+00:00</startTimeT>
<endTimeT>2008-10-29T00:00:00+00:00</endTimeT>
<role/>
<createdTime/>
<modifiedUsername/>
<usage>
  <startTime>2008-08-07T04:06:32+01:00</startTime>
  <endTime>2008-08-07T04:06:33+01:00</endTime>
  <ipAddress>4.5.6.7</ipAddress>
</usage>
<usage>
  <startTime>2008-10-02T22:00:00+01:00</startTime>
```

<endTime>2008-10-03T00:30:00+01:00</endTime>

<ipAddress>4.5.6.7</ipAddress>

</usage>

<timeProfile>

<id>2</id>

<name>StartEnd</name>

<description/>

<duration>0</duration>

<accountType>1</accountType>

<durationUnit>Days</durationUnit>

<durationInUnits>0</durationInUnits>

<restriction>

<id>43</id>

<weekDay>1</weekDay>

<startTime>00:00</startTime>

<endTime>08:59</endTime>

</restriction>

<restriction>

<id>45</id>

<weekDay>3</weekDay>

<startTime>00:00</startTime>

<endTime>08:59</endTime>

</restriction>

<restriction>

<id>50</id>

<weekDay>3</weekDay>

<startTime>17:00</startTime>

<endTime>23:59</endTime>

</restriction>

```
<restriction>
  <id>51</id>
  <weekDay>4</weekDay>
  <startTime>17:00</startTime>
  <endTime>23:59</endTime>
</restriction>
<restriction>
  <id>47</id>
  <weekDay>5</weekDay>
  <startTime>00:00</startTime>
  <endTime>08:59</endTime>
</restriction>
<restriction>
  <id>54</id>
  <weekDay>7</weekDay>
  <startTime>00:00</startTime>
  <endTime>23:59</endTime>
</restriction>
</timeProfile>
</account>
</response>
```

## suspend

---

The suspend method suspends a user account in accordance with sponsor's permissions.

### Required In Parameters

- method (required): suspend
- username (required): Sponsor account username

- password (required): Sponsor account password
- id (required): The database ID of the account to be suspended

## Example

The suspend method suspends the account and returns the same XML response as getDetails.

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=suspend&&id=815>

## delete

---

The delete method deletes a user account in accordance with sponsor's permissions.

## Required In Parameters

### Example

## getDetails

---

The getDetails API gets a user's account details in accordance with the sponsor's permissions.

## Required In Parameters

- method (required): getDetails
- username (required): Sponsor account username
- password (required): Sponsor account password
- id (one required): ID of the account to be retrieved

### Example

1. To get details for an existing account, use the getDetails API call, passing in the ID of the account as returned by the create method:

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=getDetails&id=815>



## 2. If successful the following response will be returned:

```
<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <account/>
  <account>
    <id>815</id>
    <firstName>John</firstName>
    <surname>Carter</surname>
    <company>Fortinet</company>
    <email>johncart@fortinet.com</email>
    <mobileNumber>12345 48434532</mobileNumber>
    <phoneCode>123</phoneCode>
    <option1>aaa</option1>
    <option2>bbb</option2>
    <option3/>
    <option4>ddd</option4>
    <option5>eee</option5>
    <username>jcarter</username>
    <password>*****</password>
  </account>
  <status>1</status>
  <bulkId/>
  <timezone>Europe/London</timezone>
  <startTimeT>2008-10-29T00:00:00+00:00</startTimeT>
  <endTimeT>2008-10-30T00:00:00+00:00</endTimeT>
  <role/>
```

```
<createdTime/>
<modifiedUsername/>
<usage>
  <startTime>2008-08-07T04:06:32+01:00</startTime>
  <endTime>2008-08-07T04:06:33+01:00</endTime>
  <ipAddress>4.5.6.7</ipAddress>
</usage>
<usage>
  <startTime>2008-10-02T22:00:00+01:00</startTime>
  <endTime>2008-10-03T00:30:00+01:00</endTime>
  <ipAddress>4.5.6.7</ipAddress>
</usage>
<timeProfile>
  <id>2</id>
  <name>StartEnd</name>
  <description/>
  <duration>0</duration>
  <accountType>1</accountType>
  <durationUnit>Days</durationUnit>
  <durationInUnits>0</durationInUnits>
  <restriction>
    <id>43</id>
    <weekDay>1</weekDay>
    <startTime>00:00</startTime>
    <endTime>08:59</endTime>
  </restriction>
  <restriction>
    <id>45</id>
    <weekDay>3</weekDay>
```

```
<startTime>00:00</startTime>
  <endTime>08:59</endTime>
</restriction>
<restriction>
  <id>50</id>
  <weekDay>3</weekDay>
  <startTime>17:00</startTime>
  <endTime>23:59</endTime>
</restriction>
<restriction>
  <id>51</id>
  <weekDay>4</weekDay>
  <startTime>17:00</startTime>
  <endTime>23:59</endTime>
</restriction>
<restriction>
  <id>47</id>
  <weekDay>5</weekDay>
  <startTime>00:00</startTime>
  <endTime>08:59</endTime>
</restriction>
<restriction>
  <id>54</id>
  <weekDay>7</weekDay>
  <startTime>00:00</startTime>
  <endTime>23:59</endTime>
</restriction>
</timeProfile>
</account>
```

</response>

## notifyEmail

---

The notifyEmail method sends an email message to the guest's email account. It returns the same XML as getDetails.

- Required In Parameters
- method (required): notifyEmail
- username (required): Sponsor account username
- password (required): Sponsor account password
- id (required): The database ID of the account to be emailed
- from (required): The email address from which to send the email
- to (required): the email address to send the email to

### Example

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=notifyEmail.&&&id=815>.

## notifySMS

---

The notifySms method sends an SMS message to the guest's mobile (cell) phone. It returns the same XML as getDetails.

### Required In Parameters

- method (required): notifySms
- username (required): Sponsor account username
- password (required): Sponsor account password
- id (required): The database ID of the account to be emailed

## Example

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=notifySms&&&id=815>.

# getVersion

---

The getVersion method shows the current API version.

## Required In Parameters

- method (required): getVersion
- username (required): Sponsor account username
- password (required): Sponsor account password

## Example

A call return a response of the form:

```
<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <appName>Cisco NAC Guest Server</appName>
  <version>2.0.2</version>
  <majorVersion>2</majorVersion>
  <minorVersion>0</minorVersion>
  <maintenanceVersion>2</maintenanceVersion>
</response>
```

# search

---

The search API returns guest account details for reporting purposes according to the sponsor's permissions and configuration, as per the Managing Guest Accounts of the sponsor interface.

## Required In Parameters

- username (required): sponsor account username
- password (required): sponsor account password
- method (required): search
- sponsor (optional): sponsor username
- guestUsername (optional): guest username
- firstName (optional): guest user first name
- surname (optional): guest user surname
- company (optional): guest user company name
- email (optional): guest user email address
- ipAddress (optional)
- startTime (optional): YYYY-MM-DD
- endTime (optional): YYYY-MM-DD
- timezone (optional): Timezone in which the account is create
- timeProfile (optional): time profile name
- accountGroup - name of account group (string)
- mobileNumber (optional): guest mobile number
- phoneCode (optional): guest mobile number country code
- guestPortal (optional): guest portal name used by the guest to self register his account
- option1 (optional):
- option2 (optional):
- option3 (optional):
- option4 (optional):
- option5 (optional):
- statusInactive (optional):
- statusActive (optional):
- statusExpired (optional):
- statusSuspended (optional):
- statusPending (optional):

- statusRejected (optional):

## Example

The required parameters are mandatory. The optional parameters serve to subset the data returned. If the start and end date are not specified, then accounts spanning the last 24 hours are returned.

The following example returns details of active guest accounts between 3rd March 2009 and 15th April 2009.

<http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local&method=search&startTime=2009-03-03&endTime=2009-04-15&statusActive=1>

If successful, the following response will be returned.

```
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <item>
    <id>2005</id>
    <firstName>Jim</firstName>
    <surname>Bean</surname>
    <company>Beans Brewery</company>
    <email>jim@bean.com</email>
    <username> jim@bean.com </username>
    <password>Es3TDdd3</password>
    <status>2</status>
    <mobileNumber>782394928</mobileNumber>
    <phoneCode>1</phoneCode>
    <timezone>America/Los_Angeles</timezone>
    <option1/>
    <option2/>
    <option3/>
    <option4/>
```

```
<option5/>
<startTime>2009-04-01T04:40:00+00:00</startTime>
<endTime>2009-04-06T06:59:00+00:00</endTime>
<role>Default</role>
<sponsorId>196</sponsorId>
<sponsor>sam</sponsor>
<timeProfileId>1</timeProfileId>
<timeProfile>default</timeProfile>
</item>
<item>
  ...further account details meeting the request criteria...
</item>
<item>
  ...further account details meeting the request criteria...
</item>
<item>
  ...further account details meeting the request criteria...
</item>
</response>
```

## approve

---

Approves a guest account

**Note:** The approve API is only available from Versions 10.11 and later. Required in parameters are:

- method (required) : approve
- id (required) : id for the guest account
- username (required) : username for the sponsor making the API call
- password (required) : password for the sponsor making the API call



# example

Approve example input method:

[http://10.53.0.244/sponsor/api/GuestAccount.php?](http://10.53.0.244/sponsor/api/GuestAccount.php?username=local&password=local&method=approve&id=1)

[username=local&password=local&method=approve&id=1](http://10.53.0.244/sponsor/api/GuestAccount.php?username=local&password=local&method=approve&id=1)

```
<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <account>
    <username>test@test.com</username>
    <password>a</password>
    <failedLoginAttempts>0</failedLoginAttempts>
    <modifiedUsername/>
    <lastMonitoredLogRefresh/>
    <duration/>
    <allowedWindow/>
    <approvalDecisionDate>2010-11-18T10:20:46-05:00</approvalDecisionDate>
    <eventCode>
      <id/>
      <sponsor/>
      <startTime/>
      <endTime/>
      <timezone/>
      <maxAccounts>0</maxAccounts>
      <code/>
      <status>1</status>
      <description/>
```

```
<timeProfile/>
  <guestRole/>
</eventCode>
<approvalRequestEmail/>
<nextApprovalNotification/>
<rejectReason/>
<id>1</id>
<firstName>test</firstName>
<surname>test</surname>
<company>test</company>
<email>test@test.com</email>
<mobileNumber/>
<phoneCode/>
<option1/>
<option2/>
<option3/>
<option4/>
<option5/>
<status>1</status>
<bulkId/>
<timezone>America/Lima</timezone>
<startTimeT>2010-11-18T10:18:00-05:00</startTimeT>
<endTimeT>2010-11-18T23:59:00-05:00</endTimeT>
<role>
  <id>3</id>
  <name>Default</name>
  <description>Default Role</description>
  <maxConcurrentConnections>0</maxConcurrentConnections>
  <maxFailedAuthAttempts>2</maxFailedAuthAttempts>
```

```
<allowPasswordChange/>
<requirePasswordChange/>
<passwordChangeInterval/>
</role>
<createdTime>2010-11-18T15:18:53+00:00</createdTime>
<hotspot/>
<restricted/>
<timeProfile>
  <id>1</id>
  <name>default</name>
  <description>Default time profile</description>
  <duration/>
  <timezone/>
  <accountType>1</accountType>
  <durationUnit>D</durationUnit>
  <durationInUnits>0</durationInUnits>
  <allowedWindow/>
  <windowUnit>D</windowUnit>
  <windowInUnits>0</windowInUnits>
</timeProfile>
</account>
</response>
```

## disableRememberMe

---

Disables remember me option of a guest till it is enabled again by the guest. Remember me can be disabled either using guest user id or Mac Address.

Required parameters

method (required): disableRememberMe

username (required): Sponsor account username

password (required): Sponsor account password

id (required): The database ID of the account to be suspended or MAC Address

## Example

The `disableRememberMe` method deletes the data used by remember me feature and forces guest user to explicitly login during his next visit.

API returns the same XML response as `getDetails`.

`http://x.x.x.x/sponsor/api/GuestAccount.php?username=local&password=local6&method=disableRememberMe&id=2815`

## reject

---

Rejects a guest account

**Note:** The reject API is only available from Versions 10.11 and later. Required in parameters are:

- method (required) : reject
- id (required) : id for the guest account
- username (required) : username for the sponsor making the API call password (required) : password for the sponsor making the API call

## Example

Reject example input:

`http://10.53.0.244/sponsor/api/GuestAccount.php?username=local&password=local&method=reject&id=1`

```
<?xml version="1.0"?>
```

```
<response>
```

```
  <status>
```

```
    <code>0</code>
```

```
    <message>Success</message>
```

```
  </status>
```

```
<account>
  <username>test@test.com</username>
  <password>a</password>
  <failedLoginAttempts>0</failedLoginAttempts>
  <modifiedUsername/>
  <lastMonitoredLogRefresh/>
  <duration/>
  <allowedWindow/>
<approvalDecisionDate>2010-11-18T10:22:52-05:00</approvalDecisionDate>
  <eventCode>
    <id/>
    <sponsor/>
    <startTime/>
    <endTime/>
    <timezone/>
    <maxAccounts>0</maxAccounts>
    <code/>
    <status>1</status>
    <description/>
    <timeProfile/>
    <guestRole/>
  </eventCode>
  <approvalRequestEmail/>
  <nextApprovalNotification/>
  <rejectReason/>
  <id>1</id>
  <firstName>test</firstName>
  <surname>test</surname>
  <company>test</company>
```

```
<email>test@test.com</email>
<mobileNumber/>
<phoneCode/>
<option1/>
<option2/>
<option3/>
<option4/>
<option5/>
<status>6</status>
<bulkId/>
<timezone>America/Lima</timezone>
<startTimeT>2010-11-18T10:18:00-05:00</startTimeT>
<endTimeT>2010-11-18T23:59:00-05:00</endTimeT>
<role>
  <id>3</id>
  <name>Default</name>
  <description>Default Role</description>
  <maxConcurrentConnections>0</maxConcurrentConnections>
  <maxFailedAuthAttempts>2</maxFailedAuthAttempts>
  <allowPasswordChange/>
  <requirePasswordChange/>
  <passwordChangeInterval/>
</role>
<createdTime>2010-11-18T15:18:53+00:00</createdTime>
<hotspot/>
<restricted/>
<timeProfile>
  <id>1</id>
  <name>default</name>
```

```
<description>Default time profile</description>
<duration/>
<timezone/>
<accountType>1</accountType>
<durationUnit>D</durationUnit>
<durationInUnits>0</durationInUnits>
<allowedWindow/>
<windowUnit>D</windowUnit>
<windowInUnits>0</windowInUnits>
</timeProfile>
</account>
</response>
```

## guestCreateParams

---

The guestCreateParams method ...

### Required In Parameters

### Example

## Device Account API

---

### createDevice

The createDevice method creates a device account in accordance with the sponsor's permissions.

### Required In Parameters

- method (required): createDevice
- username (required): Sponsor account username
- password (required): Sponsor account password
- macAddress
- (required): Sponsor account username
- firstName (based on policy): user first name
- surname (based on policy): user surname
- company (based on policy): Guest user company name
- email (based on policy): Guest user email address
- phonecode (based on policy): Telephone code for the Guest user mobile telephone (e.g. +44)
- mobilenumber (based on policy): Mobile telephone number for the Guest user
- accountGroup - name of account group (string)
- timeProfile (required): The time profile to use when creating the account
- timezone (required): Timezone in which the account is created (as per Valid Timezones, page A-13)
- startTime (required): The time the account is due to start
- endTime (required): The time the account should end
- option1 (based on policy): Optional data field 1
- option2 (based on policy): Optional data field 2
- option3 (based on policy): Optional data field 3
- option4 (based on policy): Optional data field 4
- option5 (based on policy): Optional data field 5

## Example

The following example creates a device account with the details below:

Mac Address: 12-12-78-3b-cd-25

First Name: samuel

Surname: samuel

Company: Fortinet

Email: samuel@Fortinet.com

Phone Code: 44

Mobile Number (cellphone):

07929379212

Role: Default



Time Profile: Default

Timezone: Europe/London

Start Time: 16th March 2012 (midnight)

EndTime: 16th April 2012 (midnight)

### Call the API as follows:

```
http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=
createDevice&macAddress=12-12-78-3b-cd-
255&firstName=samuel&surname=samuel&company=fortinet&email=sam@fortinet.co
m&phoneCode=44&mobileNumber=07929379212&role=Default&timeProfile=Default&t
imezone=Europe%2FLondon&startTime=2012-03-16&endTime=2012-04-16
```

### If successful, a response is returned in the form:

```
<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <account>
    <macAddress>12-12-78-3b-cd-25</macAddress>
    <startTime>2012-03-16T00:00:00+00:00</startTime>
    <endTime>2012-04-16T00:00:00+01:00</endTime>
    <id>1</id>
    <firstName>samuel</firstName>
    <surname>samuel</surname>
    <company>fortinet</company>
    <email>samuel@fortinet.com</email>
    <mobileNumber>07929379212</mobileNumber>
    <phoneCode>44</phoneCode>
```

```
<option1/>
<option2/>
<option3/>
<option4/>
<option5/>
<status>1</status>
<bulkId/>
<timezone>Europe/London</timezone>
<startTimeT>2012-03-16T00:00:00+00:00</startTimeT>
<endTimeT>2012-04-16T00:00:00+01:00</endTimeT>
<createdTime>2012-03-16T03:47:48-07:00</createdTime>
<restricted/>
<timeProfile>
  <id>1</id>
  <name>default</name>
  <description>Default time profile</description>
  <duration/>
  <timezone/>
  <accountType>1</accountType>
  <durationUnit>D</durationUnit>
  <durationInUnits>0</durationInUnits>
  <allowedWindow/>
  <windowUnit>D</windowUnit>
  <windowInUnits>0</windowInUnits>
</timeProfile>
</account>
</response>
```

# editDevice

The editDevice method edits an existing device account in accordance with sponsor's permissions. To edit an account, you must supply the account ID as returned by createDevice above.

## Required In Parameters

- method (required): editDevice
- username (required): Sponsor account username
- password (required): Sponsor account password
- id (required): The database ID of the device account to be edited
- firstName (optional): Guest user first name
- surname (optional): Guest user surname
- email (optional): Guest user email address
- group (optional): The role in which the guest user is created
- company (optional): Guest user company name
- phonecode (optional): Telephone code for the Guest user mobile telephone (e.g. +44)
- cellnumber (optional): Cell telephone number for the Guest user
- timezone (optional): The timezone in which the guest account is created (as per Valid Timezones)
- option1 (optional): Optional data field 1
- option2 (optional): Optional data field 2
- option3 (optional): Optional data field 3
- option4 (optional): Optional data field 4
- option5 (optional): Optional data field 5
- startTime (optional): The time the account is due to start
- endTime (optional): The time the account should end
- timeProfile (optional): The time profiler to use when creating the account

## Example

The following example changes mobile / cell phone number & end date for an account with ID 1:

```
http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=editDevice&id=1&mobileNumber=0794122222&endTime=2012-07-09
```

The full account detail are returned:-

```
<?xml version="1.0"?>
```

```
<response>
  <status>
    <code>0</code>
    <message>Success</message>
  </status>
  <account>
    <macAddress>12-12-78-3B-CD-23</macAddress>
    <startTime>2012-03-16T00:00:00+00:00</startTime>
    <endTime>2012-07-09T00:00:00-07:00</endTime>
    <id>1</id>
    <firstName>samuel</firstName>
    <surname>samuel</surname>
    <company>fortinet</company>
    <email>samuel@fortinet.com</email>
    <mobileNumber>07941222222</mobileNumber>
    <phoneCode>44</phoneCode>
    <option1/>
    <option2/>
    <option3/>
    <option4/>
    <option5/>
    <bulkId/>
    <timezone>Europe/London</timezone>
    <startTimeT>2012-03-16T00:00:00+00:00</startTimeT>
    <endTimeT>2012-07-09T00:00:00-07:00</endTimeT>
    <createdTime>2012-03-16T10:47:48+00:00</createdTime>
    <restricted/>
    <timeProfile>
      <id>1</id>
```

```
<name>default</name>
<description>Default time profile</description>
<duration/>
<timezone/>
<accountType>1</accountType>
<durationUnit>D</durationUnit>
<durationInUnits>0</durationInUnits>
<allowedWindow/>
<windowUnit>D</windowUnit>
<windowInUnits>0</windowInUnits>
<restrictions/>
</timeProfile>
</account>
</response>
```

## getDeviceDetails

The `getDeviceDetails` retrieves device account details in accordance with the sponsor's permissions.

### Required In Parameters

- `method` (required): `getDeviceDetails`
- `username` (required): Sponsor account username
- `password` (required): Sponsor account password
- `id` (required): ID of the account to be retrieved

### Example

To fetch details of an existing device account using the ID of the account as returned by `createDevice`:

```
http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=getDeviceDetails&id=1
```

The full account detail are returned:-

```
<?xml version="1.0"?>
<response>
  <status>
```

```
<code>0</code>
<message>Success</message>
</status>
<account>
  <macAddress>12-12-78-3B-CD-23</macAddress>
  <startTime>2012-03-16T00:00:00+00:00</startTime>
  <endTime>2012-07-09T08:00:00+01:00</endTime>
  <id>1</id>
  <firstName>samuel</firstName>
  <surname>samuel</surname>
  <company>fortinet</company>
  <email>samuel@fortinet.com</email>
  <mobileNumber>07941222222</mobileNumber>
  <phoneCode>44</phoneCode>
  <option1/>
  <option2/>
  <option3/>
  <option4/>
  <option5/>
  <status>2</status>
  <bulkId/>
  <timezone>Europe/London</timezone>
  <startTimeT>2012-03-16T00:00:00+00:00</startTimeT>
  <endTimeT>2012-07-09T08:00:00+01:00</endTimeT>
  <createdTime>2012-03-16T10:47:48+00:00</createdTime>
  <restricted/>
  <timeProfile>
    <id>1</id>
    <name>default</name>
```

```
<description>Default time profile</description>
<duration/>
<timezone/>
<accountType>1</accountType>
<durationUnit>D</durationUnit>
<durationInUnits>0</durationInUnits>
<allowedWindow/>
<windowUnit>D</windowUnit>
<windowInUnits>0</windowInUnits>
<restrictions/>
</timeProfile>
</account>
</response>
```

## suspendDevice

The suspendDevice method suspends a device account in accordance with sponsor's permissions.

### Required In Parameters

- method (required): suspendDevice
- username (required): Sponsor account username
- password (required): Sponsor account password
- id (required): ID of the device account to be suspended

### Example

The suspendDevice method suspends the account & returns the same XML response as getDeviceDetails.

```
http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=
suspendDevice&id=1
```

## deviceNotifyEmail

The deviceNotifyEmail method sends an email message to the device accounts email address & returns the same XML response as getDeviceDetails.

## Required In Parameters

- method (required): deviceNotifyEmail
- username (required): Sponsor account username
- password (required): Sponsor account password
- id (required): ID of the device account to be emailed

## Example

```
http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=deviceNotifyEmail.&id=1
```

## deviceNotifySms

The deviceNotifySms method sends an SMS message to the account mobile / cell phone & returns the same XML response as getDeviceDetails.

## Required In Parameters

- method (required): notifySms
- username (required): Sponsor account username
- password (required): Sponsor account password
- id (required): The ID of the account to be messaged via SMS

## Example

```
http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=deviceNotifySms&id=1
```

## searchDevices

The searchDevices API call returns device account details for reporting purposes according to the sponsor's permissions.

## Required In Parameters

- method (required): searchDevices
- username (required): Sponsor account username
- password (required): Sponsor account password
- id (required): The ID of the account to be messaged via SMS
- sponsor (optional): sponsor username
- macAddress (optional): guest username
- firstName (optional): account first name



- surname (optional): account surname
- company (optional): account company name
- email (optional): account email address
- ipAddress (optional)
- startTime (optional): YYYY-MM-DD
- endTime (optional): YYYY-MM-DD
- timezone (optional): Timezone in which the account is create
- timeProfile (optional): time profile name
- accountGroup - name of account group (string)
- mobileNumber (optional): guest mobile number
- phoneCode (optional): guest mobile number country code
- guestPortal (optional): guest portal name used by the guest to self register his account
- option1 (optional):
- option2 (optional):
- option3 (optional):
- option4 (optional):
- option5 (optional):
- statusInactive (optional):
- statusActive (optional):
- statusExpired (optional):
- statusSuspended (optional):

## Example

Optional parameters serve to subset the data returned. If the start and end date are not specified then only accounts spanning the last 24 hours are returned.

The following example returns details of active device accounts between 1<sup>st</sup> January 2012 and 31<sup>st</sup> December 2012.

```
http://x.x.x.x/sponsor/api/GuestAccount.php?username=xxx&password=xxx&method=searchDevices&startTime=2012-01-01&endTime=2012-12-31&statusActive=1
```

On success, the following response will be returned.

```
<?xml version="1.0"?>
<response>
  <status>
    <code>0</code>
    <message>Success</message>
```

</status>

<item>

<id>1</id>

<macaddress>12:12:78:3B:CD:23</macaddress>

<firstName>samuel</firstName>

<surname>samuel</surname>

<company>fortinet</company>

<email>samuel@fortinet.com</email>

<status>2</status>

<mobileNumber>07941222222</mobileNumber>

<phoneCode>44</phoneCode>

<timezone>Europe/London</timezone>

<option1/>

<option2/>

<option3/>

<option4/>

<option5/>

<startTime>2012-03-16T00:00:00+00:00</startTime>

<endTime>2012-07-09T07:00:00+00:00</endTime>

<role>Default</role>

<sponsorId>196</sponsorId>

<sponsor>Sam</sponsor>

<timeProfileId>1</timeProfileId>

<timeProfile>default</timeProfile>

</item>

<item>

<id>2</id>

<macaddress>BB:1C:7C:3B:CD:24</macaddress>

<firstName>John</firstName>

<surname>James</surname>  
<company>fortinet</company>  
<email>jj@fortinet.com</email>  
<status>2</status>  
<mobileNumber>07929379212</mobileNumber>  
<phoneCode>44</phoneCode>  
<timezone>Europe/London</timezone>  
<option1/>  
<option2/>  
<option3/>  
<option4/>  
<option5/>  
<startTime>2012-01-16T00:00:00+00:00</startTime>  
<endTime>2012-08-15T23:00:00+00:00</endTime>  
<role>Default</role>  
<sponsorId>192</sponsorId>  
<sponsor>Will</sponsor>  
<timeProfileId>1</timeProfileId>  
<timeProfile>default</timeProfile>

</item>

<item>

...further account details meeting the request criteria...

</item>

<item>

...further account details meeting the request criteria...

</item>

```
<item>
  ...further account details meeting the request criteria...
</item>
</response>
```

## getRadiusAccounting

---

The getRadiusAccounting retrieves the list of RADIUS accounting records.

### Required In Parameters

mac: MAC address of the device for which the accounting data is to be retrieved. Mandatorily, a string value is required.

### Example

## Status Codes

---

The account status is returned via XML and contains the following values:

- Status inactive = 1
- Status active = 2
- Status expired = 3
- Status suspended = 4

## Error Codes

---

The following error codes are returned in the <code> element of the response. Value - Description:

- Value 0—No error
- Value 1—Internal application error
- Value 100—Incorrect sponsor username and/or password

- Value101—Cannot access API via HTTPS (controlled by administrator)
- Value102—Cannot access API via HTTP (controlled by administrator)
- Value 1000—Some required fields are missing (listed in the message)
- Value1001—Sending SMS messages disabled by administrator
- Value1002—Sending Emails disabled by administrator
- Value1003—The passed account ID does not exist
- Value1004—Some fields are incorrect (listed in the message)
- Value 1005—Some fields cannot be changed using the edit method

## Valid Timezones

---

Africa/Abidjan Africa/Accra Africa/Addis\_Ababa Africa/Algiers Africa/Asmara Africa/Bamako  
 Africa/Bangui Africa/Banjul Africa/Bissau Africa/Blantyre Africa/Brazzaville Africa/Bujumbura  
 Africa/Cairo Africa/Casablanca Africa/Ceuta Africa/Conakry Africa/Dakar Africa/Dar\_es\_Salaam  
 Africa/Djibouti Africa/Douala Africa/El\_Aaiun Africa/Freetown Africa/Gaborone Africa/Harare  
 Africa/Johannesburg Africa/Kampala Africa/Khartoum Africa/Kigali Africa/Kinshasa Africa/Lagos  
 Africa/Libreville Africa/Lome Africa/Luanda Africa/Lubumbashi Africa/Lusaka Africa/Malabo  
 Africa/Maputo Africa/Maseru Africa/Mbabane Africa/Mogadishu Africa/Monrovia Africa/Nairobi  
 Africa/Ndjamena Africa/Niamey Africa/Nouakchott Africa/Ouagadougou Africa/Porto-Novo  
 Africa/Sao\_Tome Africa/Tripoli Africa/Tunis Africa/Windhoek America/Adak America/Anchorage  
 America/Anguilla America/Antigua America/Araguaina America/Argentina/Buenos\_Aires  
 America/Argentina/Catamarca America/Argentina/Cordoba America/Argentina/Jujuy  
 America/Argentina/La\_Rioja America/Argentina/Mendoza America/Argentina/Rio\_Gallegos  
 America/Argentina/San\_Juan America/Argentina/Tucuman America/Argentina/Ushuaia America/Aruba  
 America/Asuncion America/Atikokan America/Bahia America/Barbados America/Belem America/Belize  
 America/Blanc-Sablon America/Boa\_Vista America/Bogota America/Boise America/Cambridge\_Bay  
 America/Campo\_Grande America/Cancun America/Caracas America/Cayenne America/Cayman  
 America/Chicago America/Chihuahua America/Costa\_Rica America/Cuiaba America/Curacao  
 America/Danmarkshavn America/Dawson America/Dawson\_Creek America/Denver America/Detroit  
 America/Dominica America/Edmonton America/Eirunepe America/EL\_Salvador America/Fortaleza  
 America/Glace\_Bay America/Godthab America/Goose\_Bay America/Grand\_Turk America/Grenada  
 America/Guadeloupe America/Guatemala America/Guayaquil America/Guyana America/Halifax  
 America/Havana America/Hermosillo America/Indiana/Indianapolis America/Indiana/Knox  
 America/Indiana/Marengo America/Indiana/Petersburg America/Indiana/Tell\_City  
 America/Indiana/Vevay America/Indiana/Vincennes America/Indiana/Winamac America/Inuvik  
 America/Iqaluit America/Jamaica America/Juneau America/Kentucky/Louisville  
 America/Kentucky/Monticello America/La\_Paz America/Lima America/Los\_Angeles America/Maceio  
 America/Managua America/Manaus America/Martinique America/Mazatlan America/Menominee  
 America/Merida America/Mexico\_City America/Miquelon America/Moncton America/Monterrey  
 America/Montevideo America/Montreal America/Montserrat America/Nassau  
 America/New\_York America/Nipigon America/Nome America/Noronha America/North\_Dakota/Center  
 America/North\_Dakota/New\_Salem America/Panama America/Pangnirtung America/Paramaribo  
 America/Phoenix America/Port-au-Prince America/Port\_of\_Spain America/Porto\_Velho

America/Puerto\_Rico America/Rainy\_River America/Rankin\_Inlet America/Recife America/Regina  
America/Resolute America/Rio\_Branco America/Santiago America/Santo\_Domingo America/Sao\_Paulo  
America/Scoresbysund America/Shiprock America/St\_Johns America/St\_Kitts America/St\_Lucia  
America/St\_Thomas America/St\_Vincent America/Swift\_Current America/Tegucigalpa America/Thule  
America/Thunder\_Bay America/Tijuana America/Toronto America/Tortola America/Vancouver  
America/Whitehorse America/Winnipeg America/Yakutat America/Yellowknife Antarctica/Casey  
Antarctica/Davis Antarctica/DumontDURville Antarctica/Mawson Antarctica/McMurdo  
Antarctica/Palmer Antarctica/Rothera Antarctica/South\_Pole Antarctica/Syowa Antarctica/Vostok  
Arctic/Longyearbyen Asia/Aden Asia/Almaty Asia/Amman Asia/Anadyr Asia/Aqtau Asia/Aqtobe  
Asia/Ashgabat Asia/Baghdad Asia/Bahrain Asia/Baku Asia/Bangkok Asia/Beirut Asia/Bishkek  
Asia/Brunei Asia/Calcutta Asia/Choibalsan Asia/Chongqing Asia/Colombo Asia/Damascus Asia/Dhaka  
Asia/Dili Asia/Dubai Asia/Dushanbe Asia/Gaza Asia/Harbin Asia/Hong\_Kong Asia/Hovd Asia/Irkutsk  
Asia/Jakarta Asia/Jayapura Asia/Jerusalem Asia/Kabul Asia/Kamchatka Asia/Karachi Asia/Kashgar  
Asia/Katmandu Asia/Krasnoyarsk Asia/Kuala\_Lumpur Asia/Kuching Asia/Kuwait Asia/Macau  
Asia/Magadan Asia/Makassar Asia/Manila Asia/Muscat Asia/Nicosia Asia/Novosibirsk Asia/Omsk  
Asia/Oral Asia/Phnom\_Penh Asia/Pontianak Asia/Pyongyang Asia/Qatar Asia/Qyzylorda Asia/Rangoon  
Asia/Riyadh Asia/Saigon Asia/Sakhalin Asia/Samarkand Asia/Seoul Asia/Shanghai Asia/Singapore  
Asia/Taipei Asia/TashkentAsia/Tbilisi Asia/Tehran Asia/Thimphu Asia/Tokyo Asia/Ulaanbaatar  
Asia/Urumqi Asia/Vientiane Asia/Vladivostok Asia/Yakutsk Asia/Yekaterinburg Asia/Yerevan  
Atlantic/Azores Atlantic/Bermuda Atlantic/Canary Atlantic/Cape\_Verde Atlantic/Faroe  
Atlantic/Jan\_Mayen Atlantic/Madeira Atlantic/Reykjavik Atlantic/South\_Georgia Atlantic/Stanley  
Atlantic/St\_Helena Australia/Adelaide Australia/Brisbane Australia/Broken\_Hill Australia/Currie  
Australia/Darwin Australia/Eucla Australia/Hobart Australia/Lindeman Australia/Lord\_Howe  
Australia/Melbourne Australia/Perth Australia/Sydney Europe/Amsterdam Europe/Andorra  
Europe/Athens Europe/Belgrade Europe/Berlin Europe/Bratislava Europe/Brussels Europe/Bucharest  
Europe/Budapest Europe/Chisinau Europe/Copenhagen Europe/Dublin Europe/Gibraltar  
Europe/Guernsey Europe/Helsinki Europe/Isle\_of\_Man Europe/Istanbul Europe/Jersey  
Europe/Kaliningrad Europe/Kiev Europe/Lisbon Europe/Ljubljana Europe/London Europe/Luxembourg  
Europe/Madrid Europe/Malta Europe/Mariehamn Europe/Minsk Europe/Monaco Europe/Moscow  
Europe/Oslo Europe/Paris Europe/Podgorica Europe/Prague Europe/Riga Europe/Rome Europe/Samara  
Europe/San\_Marino Europe/Sarajevo Europe/Simferopol Europe/Skopje Europe/Sofia  
Europe/Stockholm Europe/Tallinn Europe/Tirane Europe/Uzhgorod Europe/Vaduz Europe/Vatican  
Europe/Vienna Europe/Vilnius Europe/Volgograd Europe/Warsaw Europe/Zagreb Europe/Zaporozhye  
Europe/Zurich Indian/Antananarivo Indian/Chagos Indian/Christmas Indian/Cocos Indian/Comoro  
Indian/Kerguelen Indian/Mahe Indian/Maldives Indian/Mauritius Indian/Mayotte Indian/Reunion  
Pacific/Apia Pacific/Auckland Pacific/Chatham Pacific/Easter Pacific/Efate Pacific/Enderbury  
Pacific/Fakaofu Pacific/Fiji Pacific/Funafuti Pacific/Galapagos Pacific/Gambier Pacific/Guadalcanal  
Pacific/Guam Pacific/Honolulu Pacific/Johnston Pacific/Kiritimati Pacific/Kosrae Pacific/Kwajalein  
Pacific/Majuro Pacific/Marquesas Pacific/Midway  
Pacific/Nauru Pacific/Niue Pacific/Norfolk Pacific/Noumea Pacific/Pago\_Pago Pacific/Palau  
Pacific/Pitcairn Pacific/Ponape Pacific/Port\_Moresby Pacific/Rarotonga Pacific/Saipan Pacific/Tahiti  
Pacific/Tarawa Pacific/Tongatapu Pacific/Truk Pacific/Wake Pacific/Wallis