FortiAuthenticator Interoperability Guide

Carl Windsor

Revision History

Date	Revision Number	Change Description
Aug 18th 2011	Revision 1	Initial revision.
3rd April 2012	Revision 2	Update to FortiAuthenticator 1.0 MR3. Added FortiMail, FortiWeb, Citrix Access Gateway
20th June 2012	Revision 3	Update to include challenge-response authentication method for FortiGate and Cisco IOS

FortiAuthenticator Interoperability Guide

Revision 3

20 June 2012

Contents

About this Guide

Purpose of this document

This document has been produced to aid the configuration of the FortiAuthenticator Secure Authentication system with Fortinet solutions and other third party products.

All testing was performed with:

- FortiAuthenticator 1.3
- FortiGate 4.0 MR3 PR1
- FortiWeb 4.0 MR3 PR6
- FortiClient Connect 4.0 MR3
- FortiManager 4.0 MR3
- Ubuntu 11.04
- OpenSSH version 5.8p1
- Apache version 2.2.17
- Citrix Access Gateway 5.0

Document Conventions

When you read this manual, you will see that certain words are represented in different fonts, typefaces, sizes and weights. This highlighting is systematic; text is represented in a particular style to indicate its importance or meaning e.g.

the same style to indicate their inclusion in a specific category. The types of words that are represented this way include the following:

Processes which are to be followed such as browsing to the correct section of a web site are highlighted in italics and steps separated by arrows e.g.

Browse to *User → User Group*

Text displayed on screen which may include configuration or be the result of executing a command is displayed in `Courier New font` e.g.

```
Port 1 IP: 192.168.1.99
Port 1 Netmask: 255.255.255.0
Default Gateway: 192.168.1.1
```

Paths and file locations are shown *in* **`Italic Courier New`** e.g

Edit the file `/etc/ssh/sshd_config`

CLI Commands which are to be executed by the user are shown in **`Italic Bold Courier New font`** e.g

Open the CLI and type ***`exe factory reset`***

GUI Commands which are to be executed by the user are shown in ***Italic Bold Arial font*** e.g

Under *Configure SSL-VPN Users*, click ***Add***.

Variables which should be replaced with the correct text such as passwords are displayed as a descriptor in `Courier New font` within angled brackets e.g.

```
Username:  <username>
Password:  <password><Token PIN>
```

Links are highlighted in underlined blue text e.g.

https://192.168.1.99

Additional attention is brought to specific point by the use of interest using the following breakout box format:

Note

This feature is only supported in version 1.3 onwards.

Caution

Do not add any local user to this policy under Available Users. If you do this, RADIUS Authentication will fail.

Warning

The execution of this command may result in data loss.

Basic Configuration of the FortiAuthenticator

The Basic configuration of the FortiAuthenticator is shown below. Any deviations or change which are required from this configuration will be detailed in the relevant section.

For more detail on he setup and configuration of the FortiAuthenticator see the Administration Guide at http://docs.fortinet.com/auth.html.

Basic Networking

On first boot, the FortiAuthenticator is configured to the default settings:

```
Port 1 IP: 192.168.1.99
Port 1 Netmask: 255.255.255.0
Default Gateway: 192.168.1.1
```

These setting can be modified by configuring a PC to an address on the same subnet and accessing the Web GUI via https://192.168.1.99/, alternatively you can use the CLI method below.

Configuration Using the CLI

Basic configuration of the interface IP and gateway address can be done using the Command
Line Interface (CLI).

- Connect the Management Computer to the FortiAuthenticator unit using the supplied Console Cable
- Using a suitable terminal emulation program connect to the unit with the following settings:
  - `Baud Rate: 9600`
  - `Data Bits: 8`
  - `Parity: None`
  - `Stop Bits: 1`
  - `Flow Control: None`
- Log in to the FortiAuthenticator unit using the default credentials below:
  - `Username:` **`admin`**
  - `Password:` **`<blank>`**
- Configure the network settings as required, for example:
  - ***`set port1-ip 10.1.1.99/24`***
  - ***`set default-gw 10.1.1.1`***

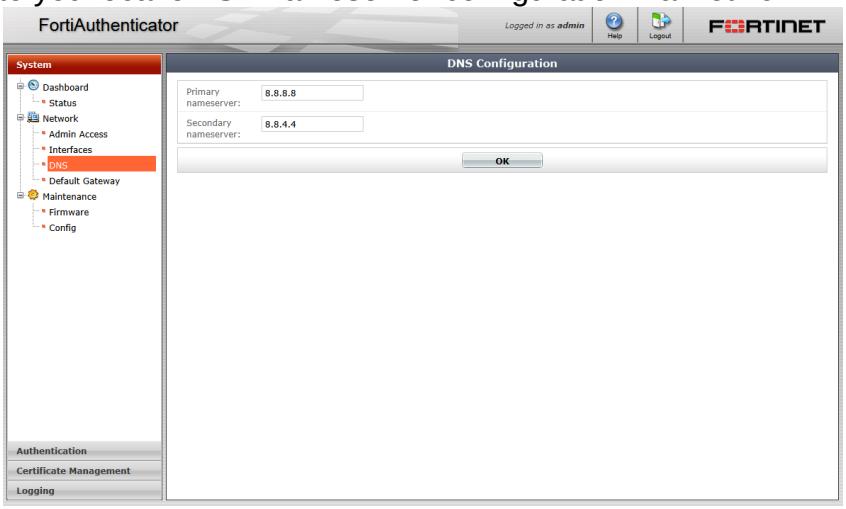
This will give you access to the GUI via the specified IP address, in this case https://10.1.1.99

System Settings

Once the basic networking has been configured, further configuration can be performed via the GUI.

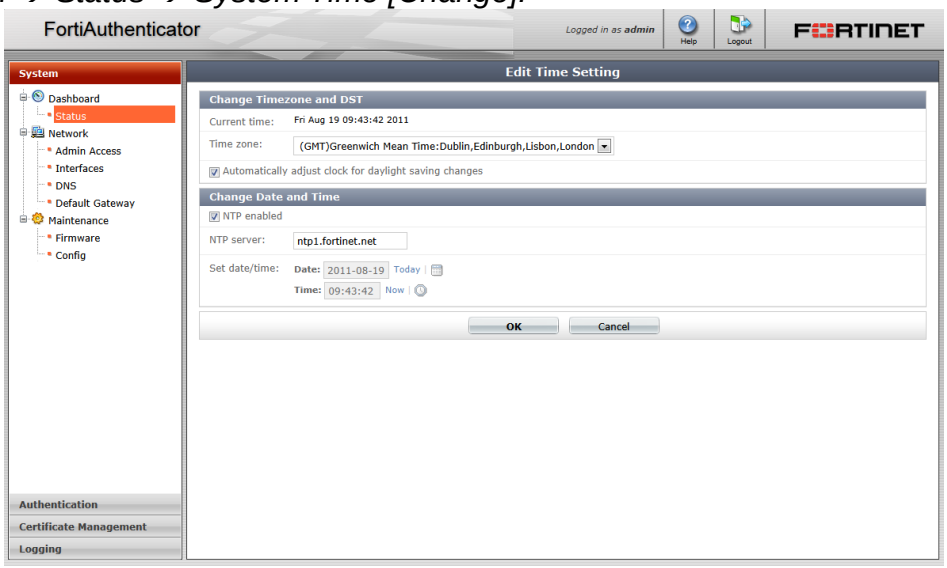
DNS

To enable resolution of the FortiGuard network and other systems such as NTP servers, set your DNS to you local or ISP nameserver configuration via *Network → DNS*.



Time Synchronization

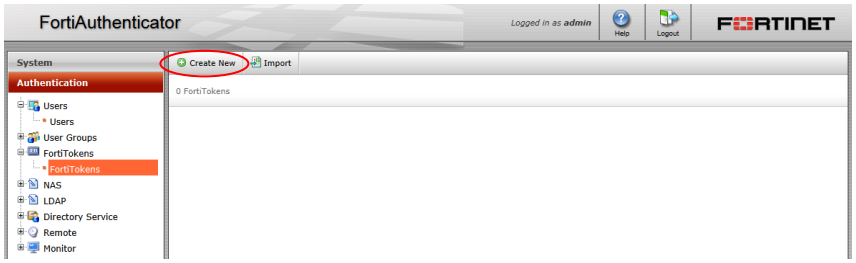
FortiToken two-factor authentication uses a time based algorithm to generate Token PINs for use in the authentication process. It is therefore essential that the time is accurate on the FortiAuthenticator system and NTP time synchronisation is recommended. Change your settings to a local NTP server for accurate timing via *Dashboard → Status → System Time [Change].*



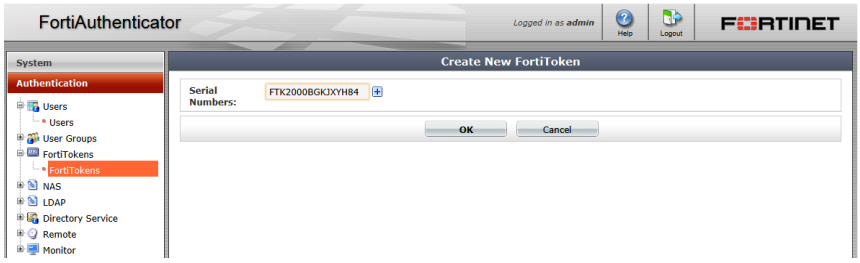
Create a test token

To test two-factor authentication a FortiToken will be required. The token serial can be found on the reverse of the token. Note that for security reasons a token can only be automatically registered from the FortiGuard network a single time. Should you require to re-register it a subsequent time, you should contact Fortinet support.

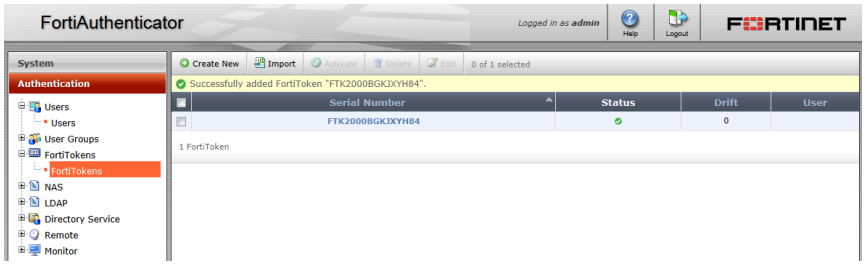
To register a token go to *Authentication → FortiTokens* and select ***Create New***.



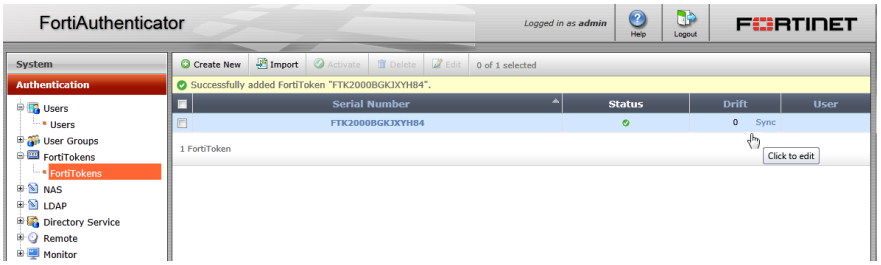
For single tokens, enter the token serial in the Serial Numbers dialogue box. To register multiple tokens, select the ⊞



Once registered the token should show as status active in the *Authentication → FortiTokens* page.



When new, all tokens are set to a drift of 0 which is a measure of how close the time on the token and time on the FortiAuthenticator match. When new, this should be 0. If you are unable to authenticate at any time, this may be due to clock drift. To force a token drift synchronisation, hover the mouse over the drift section for the token and a sync option will be opened.



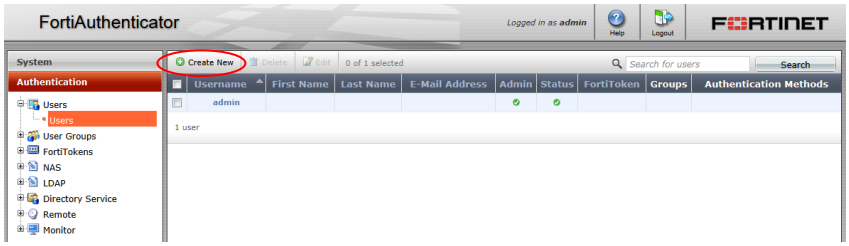
You will be prompted to enter 2 consecutive PINs from the token. Ensure you have not just used the number for an authentication attempt; if so, wait until the next number refreshed. Once synchronised wait until the next refresh before attempting to authenticate (token PINs are for one-time use, regardless of what they are used for).

Create test user

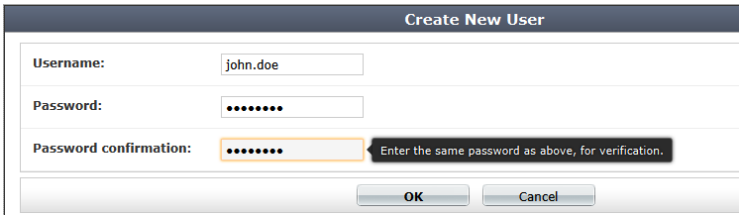
For the purpose of this interoperability test, a single user will be created:

john.doe -Test user with RADIUS based username / password and FortiToken

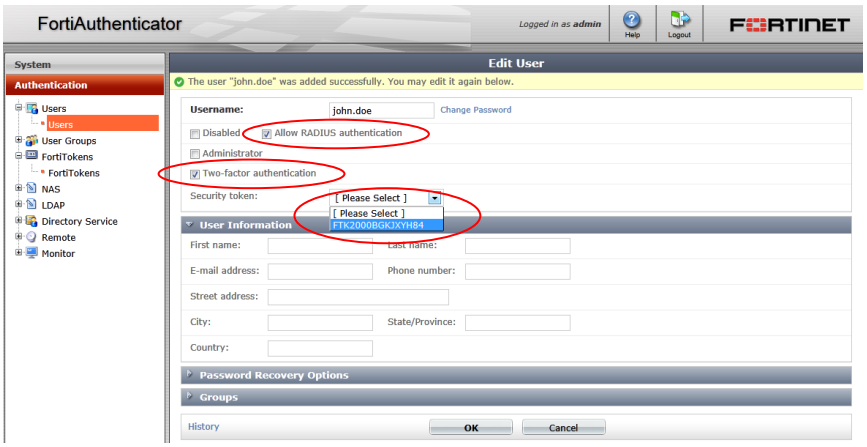
In *Authentication* → *Users* select *Create New*



In the resulting dialogue, enter a username and password for this test user account

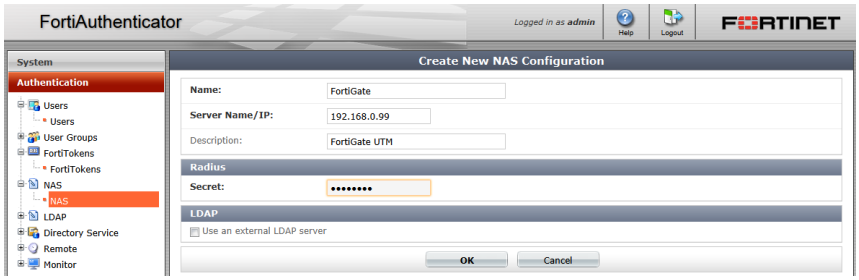


Once created you will be provided with additional options to edit for the user. For the purpose of this document, all that is needed is to *Allow RADIUS authentication* and *enable Two-factor authentication* by ticking the radio buttons and select the token serial you have just created from the drop down menu.



Configure a NAS

Before any device can connect to the FortiAuthenticator via RADIUS or LDAP, it must be configured as a NAS (Network Access Server). Until this is done, the FortiAuthenticator will ignore all authentication requests for security reasons. In *Authentication → NAS* select *Create New* and on the resulting page, enter the details of the device you wish to authenticate.



Enter the a unique name for the device and the IP from which it will be connecting. Note that this is the IP address of the device itself, not the IP that the users will be authenticating from.

In the secret section, enter a secret password which will be used by both ends of the RADIUS connection to secure the authentication process.

You will have to repeat this process for every device you wish to authenticate against the FortiAuthenticator.

FortiGate

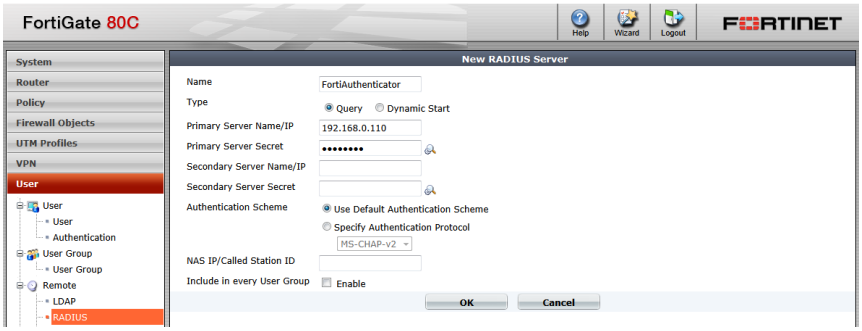
Caution

Before proceeding, ensure that you have followed the steps detailed in Chapter 2. Pay particularly attention to Section 2.2.5:- Configure a NAS and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

The FortiGate appliance is the Gateway to your network therefore securing remote access, whether to the box itself (administration or to the network behind it (VPN) is critical. FortiOS versions 4.0 MR3 and above support two factor authentication using FortiToken, however to perform two factor authentication to multiple FortiGate or to versions 4.0 MR2 and lower, you will want to use FortiAuthenticator to enable strong authentication.

Create Remote RADIUS Connection

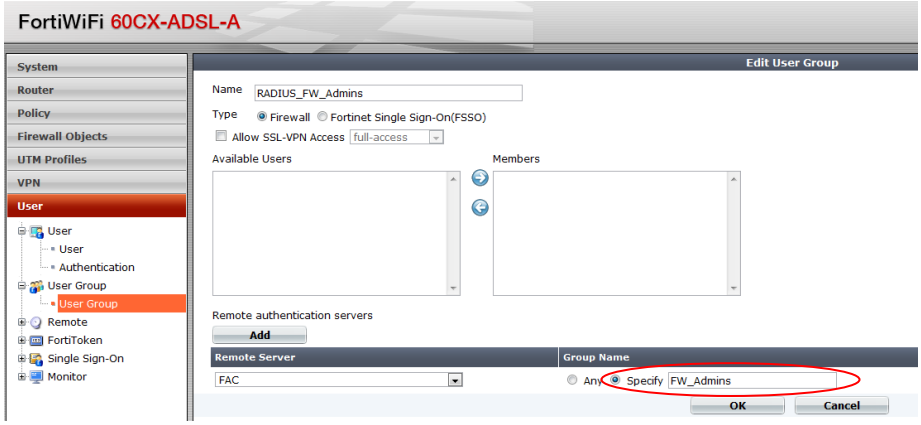
A RADIUS association is required for all FortiGate configurations described below so configure the system to point at the FortiAuthenticator. In *User → Remote → RADIUS* select Create New and configure the details of the FortiAuthenticator. Enter the shared secret which you created previously.



Authenticating Administration Users

Create User Group

In *User → User Group*, select *Create New*. Create a group called *RADIUS_Admins* of *type firewall* and under *Remote Authentication Servers*, click *Add*. Select *FortiAuthenticator* from the drop down list and click *OK* to save.



Caution

Do not add any local user to this policy under Available Users. If you do this, RADIUS Authentication will fail.

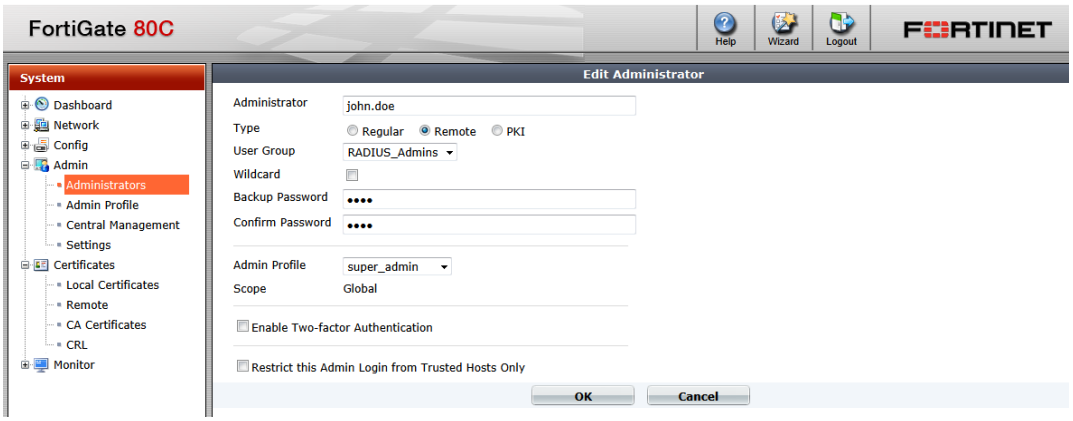
FortiAuthenticator 1.0 MR3 or higher supports sending the group membership as an AVP for example, when users configured in the FortiAuthenticator Group FW_Admins authenticate, the AVP Fortinet-Group-Name=FW_Admins will be sent in the Authentication Accept packet. This can be used to Authorize the user onto the FortiGate by setting only to accept members of that group as shown above.

Create Admin User

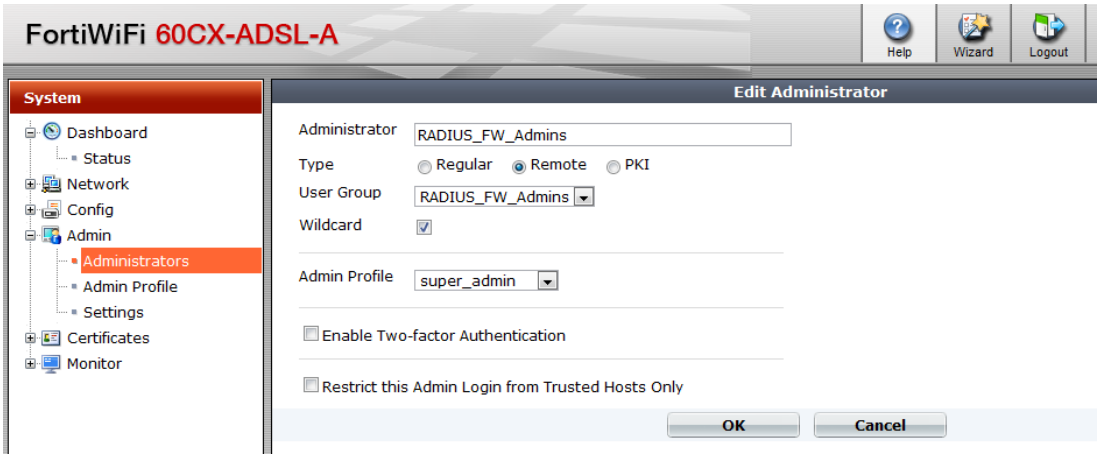
In *System* → *Admin* → *Administrators*, select *Create New*. In the resulting page, enter

`Administrator:`	***`john.doe`***
`Type:`	***`Remote`***
`User Group:`	***`RADIUS_Admins`***
`Admin Profile:`	***`super_admin`***

You will also need to enter a backup password which can be used in the event that the RADIUS authentication is unavailable e.g. do to connectivity issues.



There is also the ability to use wildcard accounts to avoid the need to specify each user locally. If this option is enabled, any user from the specified group (or from the whole RADIUS Server if a group is not specified) will be able to authenticate. If this is required, create a new administrator with a name with a descriptive name (it will not be used to authenticate). When the wildcard option is selected, any user configured on the FortiAuthenticator who is in an allowed group will be able to authenticate.



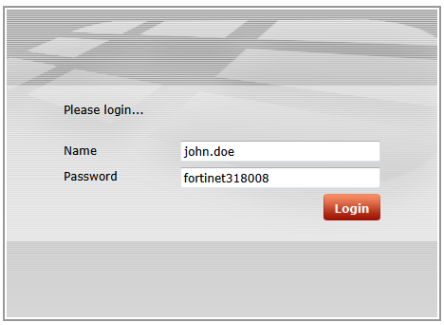
Caution

Do not select two-factor authentication at this point. The Two Factor Authentication is done externally, so the FortiGate does not need to know it is happening. This is why the FortiAuthenticator is capable of authenticating FortiOS 4.2 and below and third party systems which have no direct support for two-factor authentication.

Log out of the FortiGate and log back into the FortiGate Admin GUI with your new credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

```
Username: john.doe
Password: <password><Token PIN>
```

e.g. for a Password “fortinet” and one-time PIN of 318008, the login would become



However, obviously the password would be starred out.

Successful authentication will provide the user with access to the device and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
175	Fri Aug 19 14:12:51 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter **Debugging** to identify what is wrong.

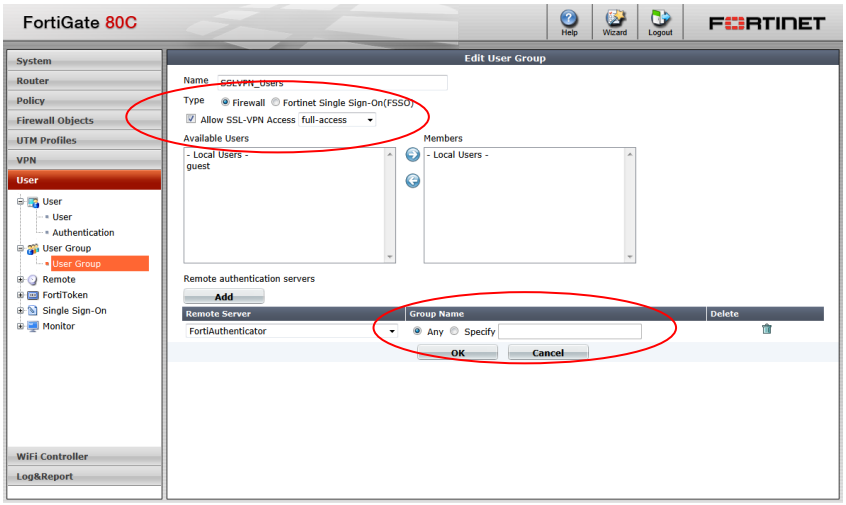
Authenticating SSL-VPN Users

Note

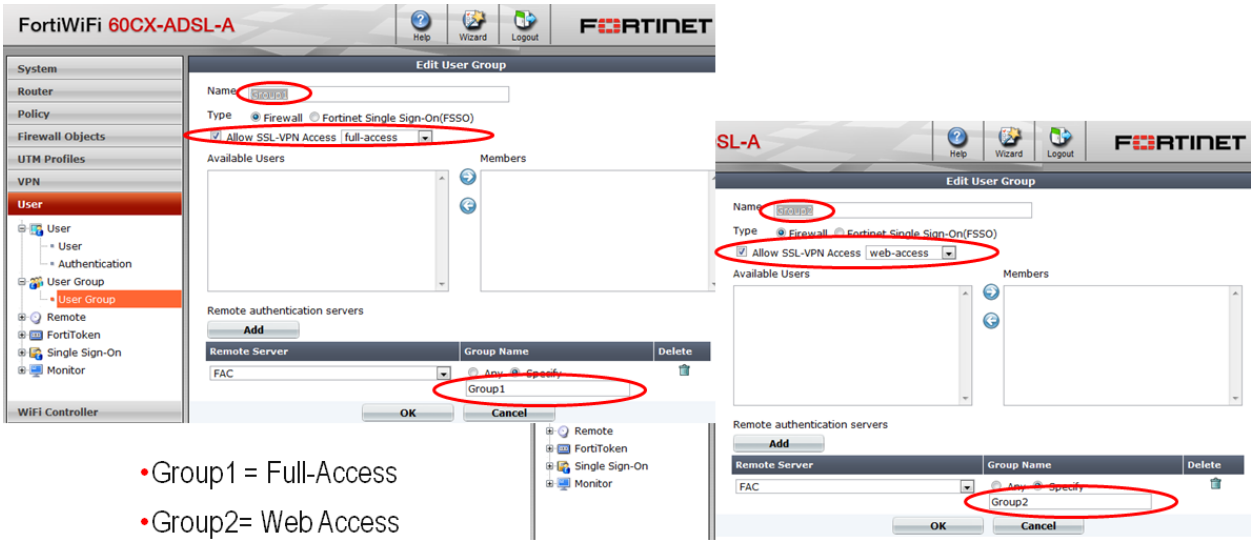
This guide does not detail how to configure the SSL-VPN, only how to enable secure authentication using FortiAuthenticator. For more information on configuring the SSL-VPN please see the SSL-VPN Guide for your specific firmware release here http://docs.fortinet.com/fgt.html.

Create User Group

In *User → User Group*, select *Create New*. Create a group called *SSLVPN_Users* of *type firewall* and enable “Allow SSL-VPN Access” with your selected access permissions. Under *Remote Authentication Servers*, click *Add*. Select *FortiAuthenticator* from the drop down list and click *OK* to save.



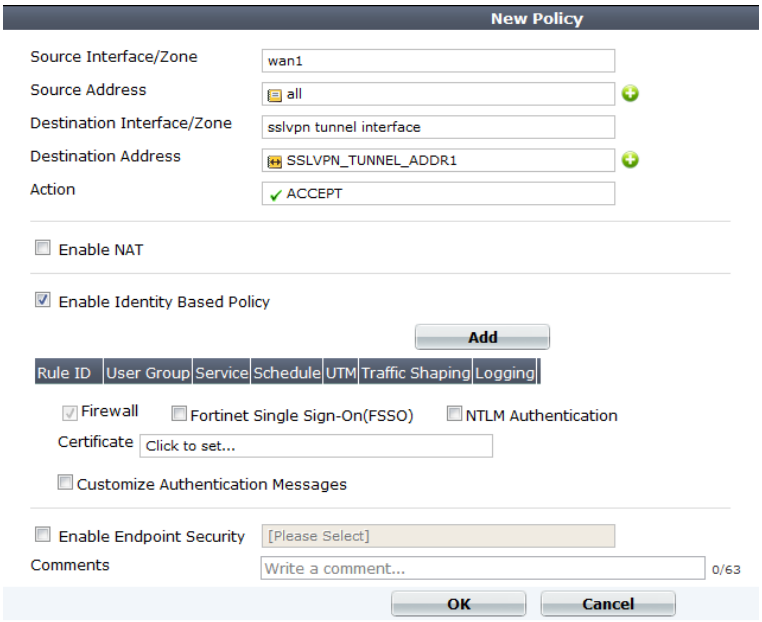
The Group Name configuration can be used to limit which users can authenticate or to limit what they can do in the VPN (by creating multiple groups in conjunction with the Allow SSL-VPN Access option).



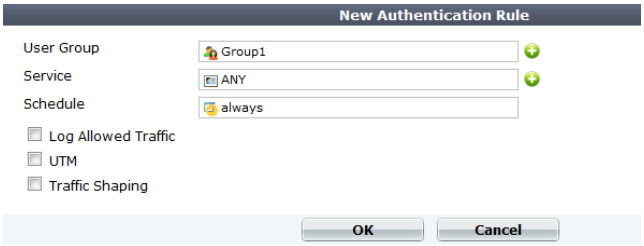
Firewall SSL VPN Policy

Create a firewall policy which enables SSL-VPN access into you chosen network. In this example, a policy is being created from WAN1 to the Internal network for the defined Group.

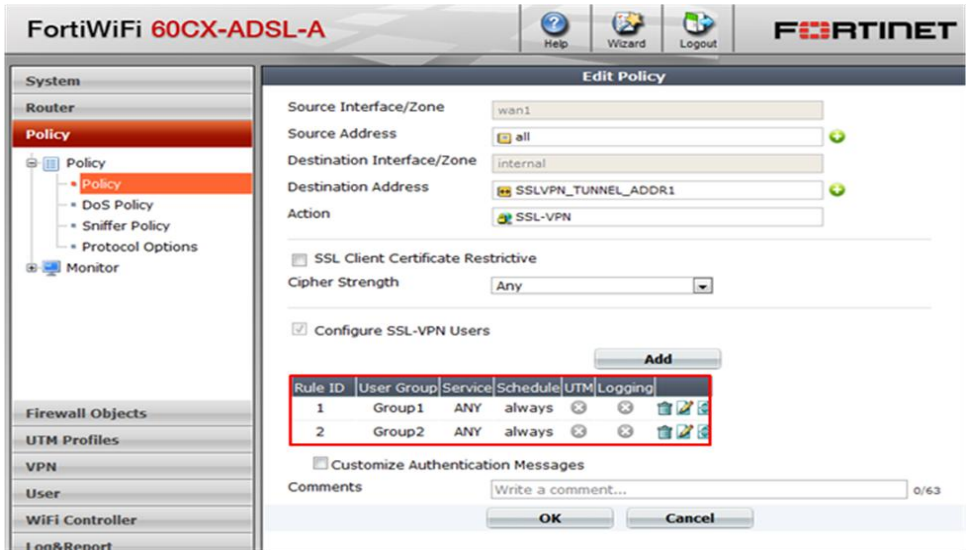
Browse to *Policy → Policy* and select ***Create New***. Select *Source Interface*: WAN1, *Destination Interface*: Internal and Action: SSL-VPN.



Enable *Identity Based Policy* and Add the all the User Groups allowed to log into the SSLVPN.



Select the *required Group* from the Available. Select Any from the Available Services. Click ***OK*** and ***OK*** again on the *Edit Policy page* to save the settings. Where multiple user groups have been configured to allow differentiated VPN access, specify all user groups at this point e.g

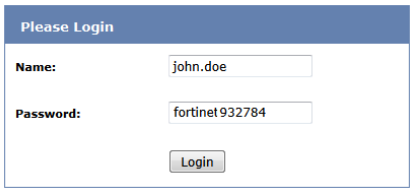


User Login – Password + Token PIN Appended

Attempt to log into the FortiGate SSL-VPN GUI e.g. https://192.168.1.99:10443 (dependent on your settings) with your new credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

Username: ***john.doe***
Password: ***<password><Token PIN>***

e.g. for a Password "fortinet" and one-time PIN of 318008, the login would become



However obviously the password would be starred out.

Successful authentication will provide the user with access to the VPN-Portal with the configuration specific to your configured user group and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

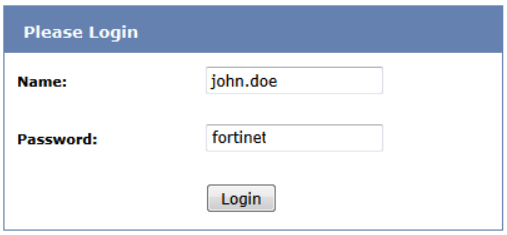
User Login – Token PIN Challenge

Whilst the PIN Appended method is the most widely supported method of authentication for 3rd party systems, FortiGate SSL VPN supports the RADIUS Challenge-Response mechanism. This allows the user to enter their username and password and then be challenged separately for the token PIN which is more intuitive. No changes need to be made to the systems to support either method and they can be used interchangeably.

Attempt to log into the FortiGate SSL-VPN GUI e.g. https://192.168.1.99:10443 (dependent on your settings) with your new credentials.

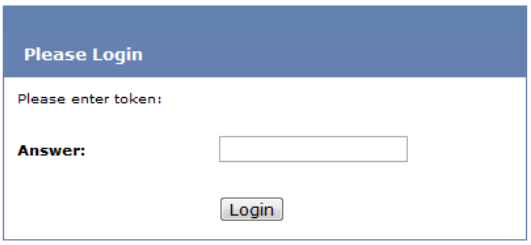
```
Username: john.doe
Password: <password>
```

e.g. for a Password "fortinet", the login would become



However obviously the password would be starred out.

The FortiAuthenticator will detect that the password is correct but the token PIN has not been provided and issue a RADIUS Challenge. FortiGate detects this and prompts the user for the additional detail.



The user should enter the correct token PIN and click login.

Successful authentication will provide the user with access to the VPN-Portal with the configuration specific to your configured user group and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

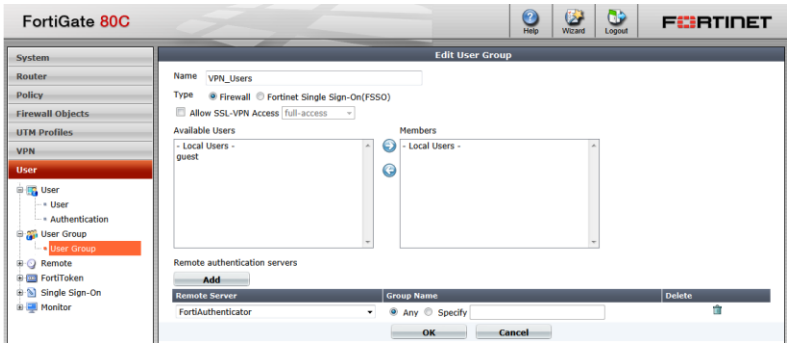
IPSec VPN

Note that this guide does not detail how to configure the IPSec VPN or the FortiClient Connect client, only how to enable secure authentication using FortiAuthenticator. For more information on configuring the VPN on FortiGate and the Forticlient Connect client please see the relevant documentation here http://docs.fortinet.com/fgt.html.

This section assumes you have a working IKE configuration.

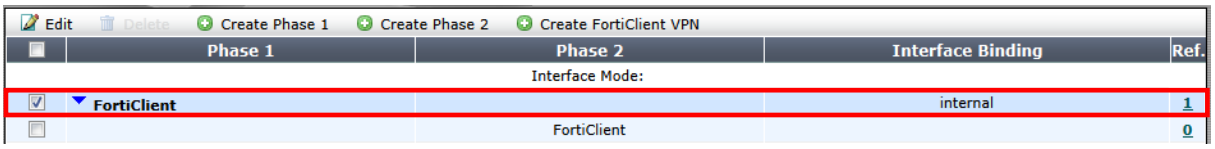
Create User Group

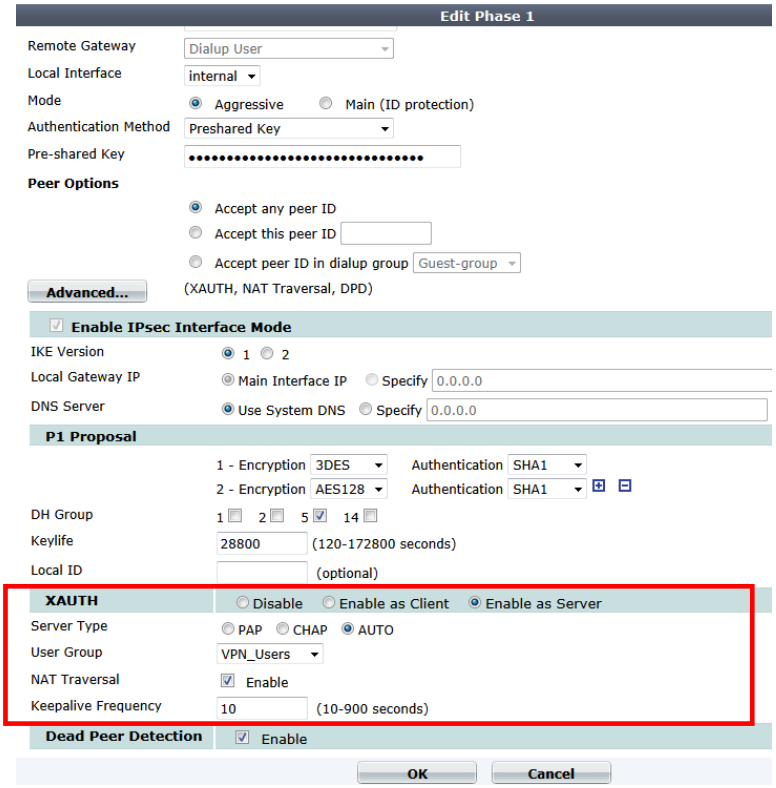
In *User → User Group*, select ***Create New***. Create a group called *VPN_Users* of *type firewall* and. Under *Remote Authentication Servers*, click *Add*. Select *FortiAuthenticator* from the drop down list and click *OK* to save.



Edit Existing IKE Policy

To enable FortiAuthenticator strong two-factor authentication, the existing IKE Policy must be configured to enable XAUTH (eXtended AUTHentication). To do this browse to VPN → IPSec → Auto Key (IKE) and Edit the Phase 1 settings of your VPN (select the radio button of the first entry for your VPN and click Edit)




Edit Phase 1
Remote Gateway
Dialup User
Local Interface
internal
Mode
Aggressive
Main (ID protection)
Authentication Method
Preshared Key
Pre-shared Key
Peer Options
Accept any peer ID
Accept this peer ID
Accept peer ID in dialup group
Guest-group
Advanced...
(XAUTH, NAT Traversal, DPD)
Enable IPsec Interface Mode
IKE Version
1
2
Local Gateway IP
Main Interface IP
Specify
0.0.0.0
DNS Server
Use System DNS
Specify
0.0.0.0
P1 Proposal
1 - Encryption
3DES
Authentication
SHA1
2 - Encryption
AES128
Authentication
SHA1
DH Group
1
2
5
14
Keylife
28800
(120-172800 seconds)
Local ID
(optional)
XAUTH
Disable
Enable as Client
Enable as Server
Server Type
PAP
CHAP
AUTO
User Group
VPN_Users
NAT Traversal
Enable
Keepalive Frequency
10
(10-900 seconds)
Dead Peer Detection
Enable
OK
Cancel

FortiManager

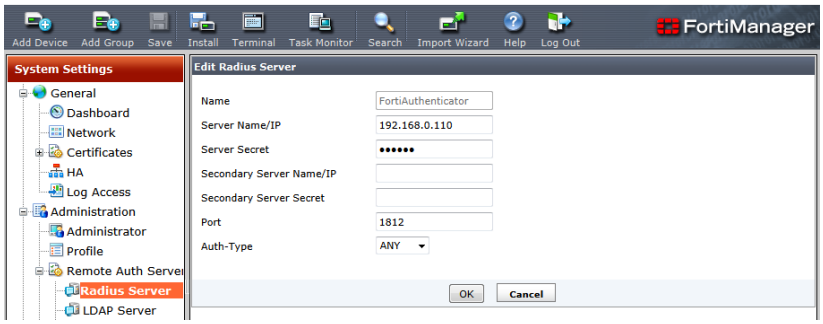
Caution

Before proceeding, ensure that you have followed the steps detailed in Chapter 2. Pay particularly attention to Section 2.2.5:- Configure a NAS and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Configure the RADIUS Server

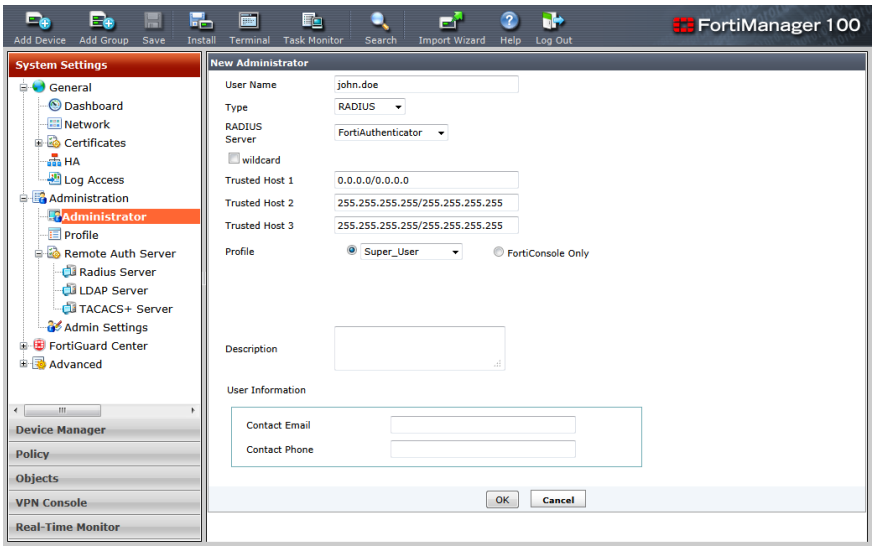
Log into the FortiManager GUI and browse to *System Settings → Administration → Remote Auth Server → RADIUS Server*. Select ***Create New***.

Enter the details of the remote FortiAuthenticator including the shared secret.



Create the Admin Users

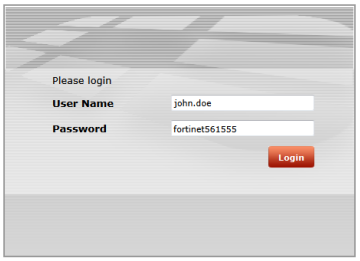
In *System Settings → Administration → Administrator*, select ***Create New***. Enter the user name, Auth Type RADIUS and select the RADIUS Server you created in the previous step.



Attempt to log into the FortiManager GUI e.g. https://192.168.1.99 (dependent on your settings) with your new credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

```
Username: john.doe
Password: <password><Token PIN>
```

e.g. for a Password “fortinet” and one-time PIN of 561555, the login would become



However obviously the password would be starred out.

Successful authentication will provide the user with access to the FortiManager and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

Wildcard Users

The wildcard user feature does not function correctly in FortiManager 4.3.1 and is scheduled to be resolved in version 4.3.1 (Mantis ID: 0145712).

This feature is functional in version 4.2 and allows users not explicitly named to authenticate using RADIUS.

FortiWeb

Caution

Before proceeding, ensure that you have followed the steps detailed in Chapter 2. Pay particularly attention to Section 2.2.5:- Configure a NAS and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Note

FortiWeb, as of version 4.0 MR3 PR6 does not support challenge-response so the Token-Appended method should be used.

Configure the RADIUS Server

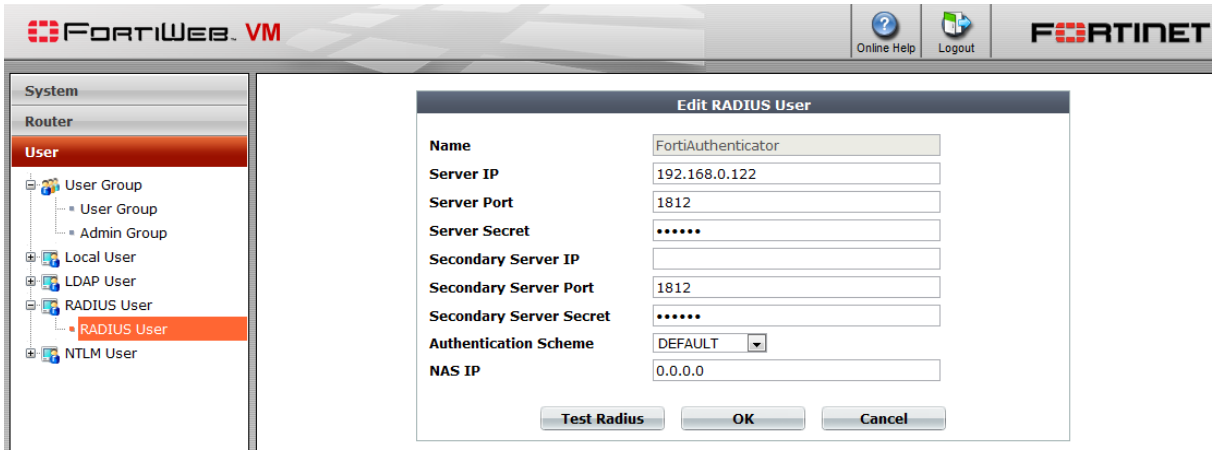
Log into the FortiWeb GUI and browse to *User → RADIUS User → RADIUS User*

Note

The FortiWeb GUI incorrectly refers to RADIUS User whereas this is actually the RADIUS Server (FortiAuthenticator) configuration. This will be changed in future versions of FortiWeb.

Select ***Create New***.

Enter the details of the remote FortiAuthenticator including the shared secret.

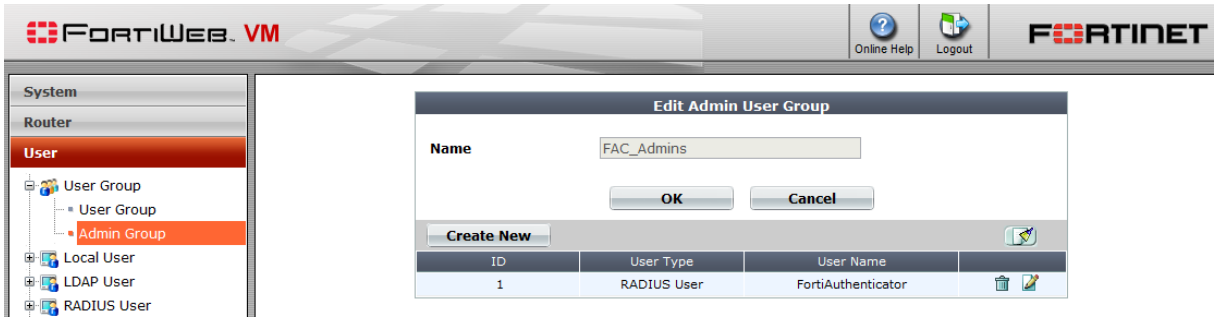


Create an Admin Group

In *User → Admin Group*, select ***Create New***. Enter the Auth Type RADIUS and select

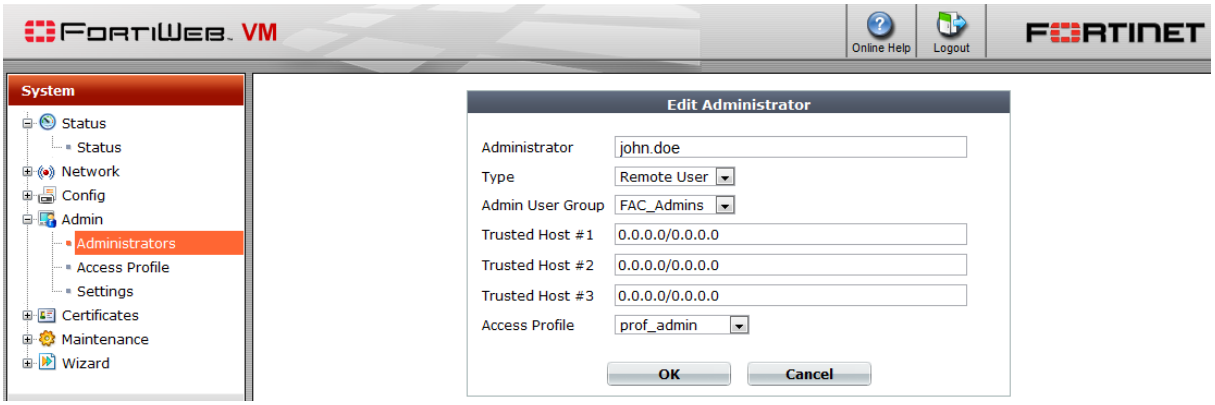
the RADIUS Server you created in the previous step under the heading user.

> **Caution**
>
> Enter the RADIUS server name at this point not the User Name. This is an error in the GUI and will be rectified in a later release of the FortiWeb GUI.



Create an Admin User

Browse to *System* → *Admin* → *Administrators*, select ***Create New***. Enter the details of the user to be authenticated, the type (Remote User), the Admin User Group (as created in the previous step) and the access profile to use.



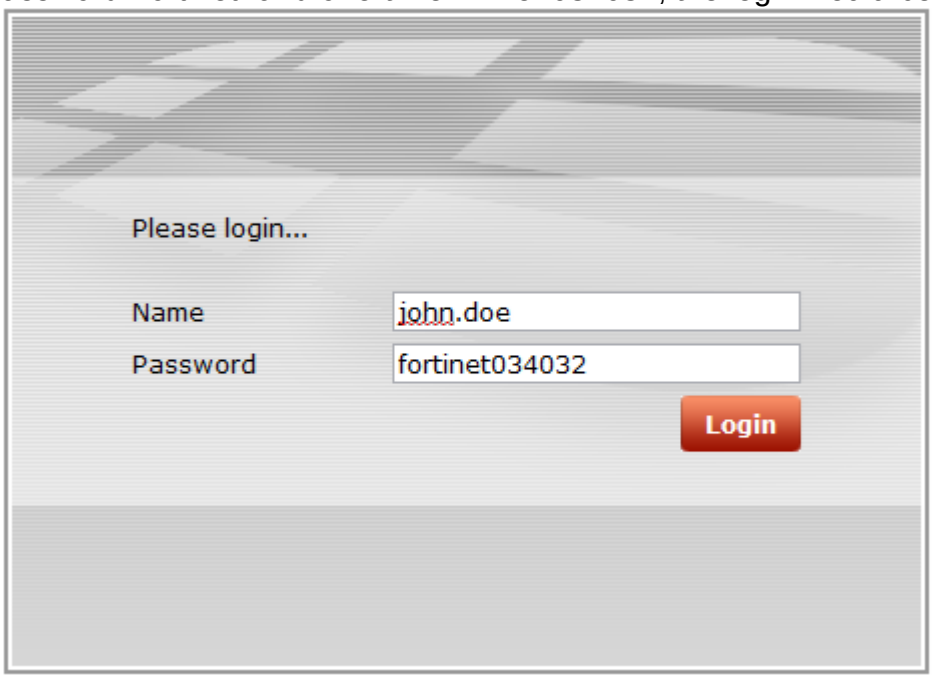
> **Note**
>
> FortiWeb does not currently support wildcard users or user groups

User Logon

Attempt to log into the FortiWeb GUI e.g. https://192.168.1.99 (dependent on your settings) with the FortiAuthenticator credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

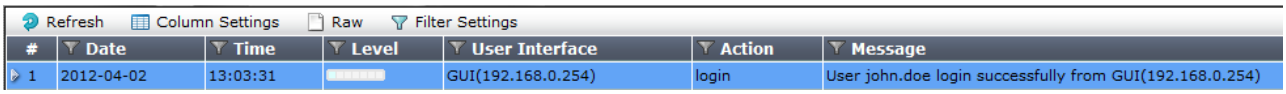
```
Username: john.doe
Password: <password><Token PIN>
```

e.g. for a Password “fortinet” and one-time PIN of 034032, the login would become



However obviously the password would be starred out.

Successful authentication will provide the user with access to the FortiWeb and will generate a login event log on the FortiAuthenticator



If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

FortiMail

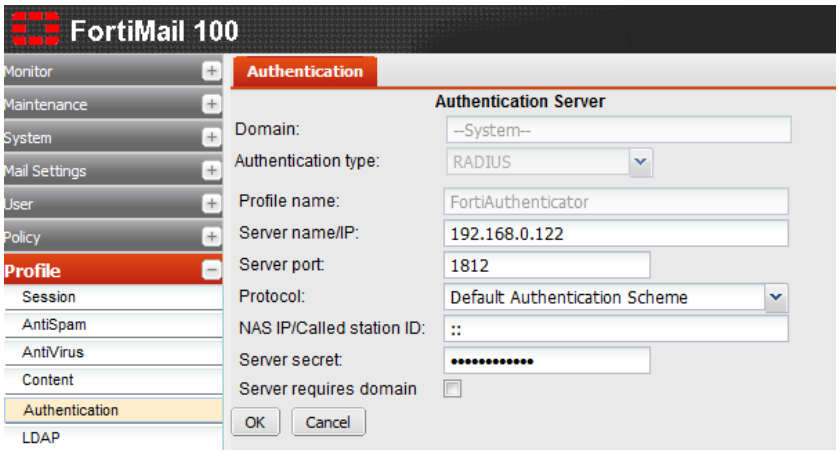
> **Caution**
>
> Before proceeding, ensure that you have followed the steps detailed in Chapter 2. Pay particularly attention to Section 2.2.5:- Configure a NAS and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Admin Login

Configure the RADIUS Server

Log into the FortiMail GUI and browse to *Profile → Authentication*. Select ***New***.

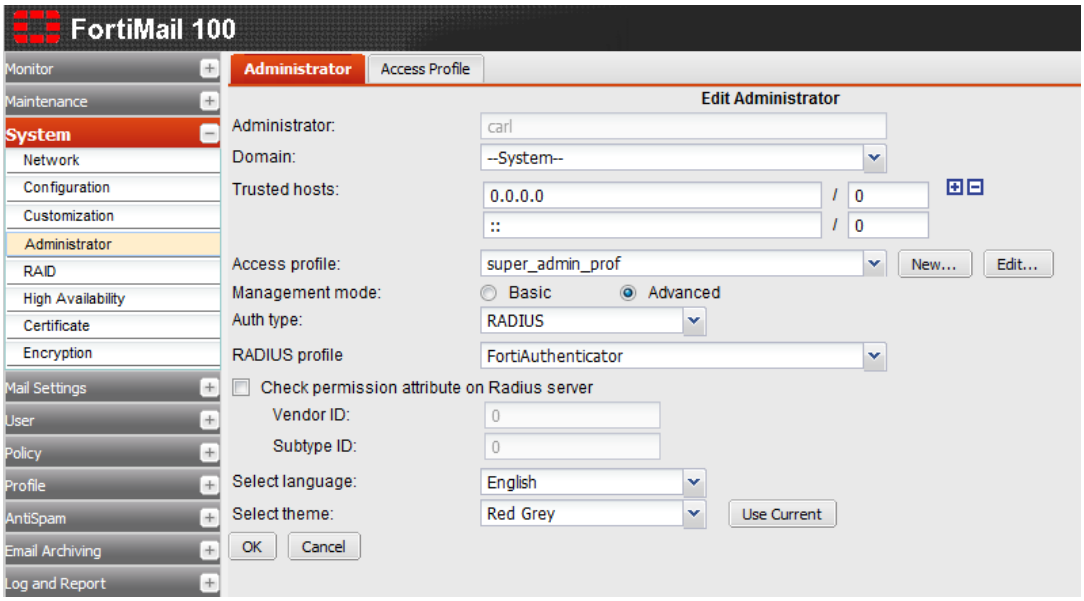
Enter the details of the remote FortiAuthenticator including the FortiAuthenticator IP, Authentication Port (1812), Port, Protocol (authentication scheme) and shared secret.



In *System → Administrator*, select ***New***. Enter the user name, Auth Type RADIUS and select the RADIUS Server you created in the previous step.

> **Caution**
>
> FortiMail Administrator configuration does not support the use of wildcard users, i.e. those not defined locally. The use of a wildcard "*" for username will not work here.

Create the Admin User

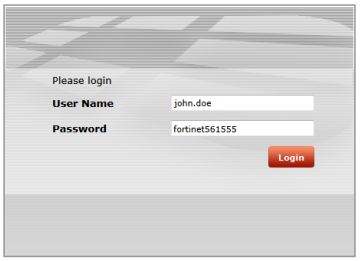


Admin User Logon

Attempt to log into the FortiManager GUI e.g. https://192.168.1.99 (dependent on your settings) with your new credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

```
Username: john.doe
Password: <password><Token PIN>
```

e.g. for a Password “fortinet” and one-time PIN of 561555, the login would become



However obviously the password would be starred out.

Successful authentication will provide the user with access to the FortiManager and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

Cisco IOS based switches and routers

The following was tested with a Cisco 2950 switch running IOS 12.1(13). Whilst this should work with other versions and IOS based routers, the command structure on the Cisco IOS is liable to vary between versions so please consult the Cisco documentation for changes.

> **Caution**
>
> Before proceeding, ensure that you have followed the steps detailed in Chapter 2. Pay particularly attention to Section 2.2.5:- Configure a NAS and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Telnet Authentication

Configure the Cisco switch to allow remote access via Telnet. To do this enter enable mode on the switch and execute conf t to begin editing the config:

```
Switch> en
Enter Password: *********
Switch# conf t
Switch(config)#
```

Enter the following commands to enable an IP address on the switch and enable telnet management

```
Switch(config)# interface Vlan1
Switch(config)# ip address 192.168.0.253 255.255.255.0
Switch(config)# ip default-gateway 192.168.0.1
Switch(config)# no shutdown
```

Enter the following commands to enable two-factor authentication

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group
radius
Switch(config)# radius-server host 192.168.0.122 auth-port
1812 key fortinet1234
Switch(config)# radius-server retransmit 3
```

Attempt to log in to the switch via telnet and you should be presented with a two-factor

enhanced login e.g.

```
telnet 192.168.0.253
User Access Verification

Username: john.doe
Password: fortinet

Please enter token:721194

Switch>
```

Notice that the login has dropped the user into the non privileged admin level denoted by the >. Enable mode is accessed via the command ***enable*** and entering the enable password.

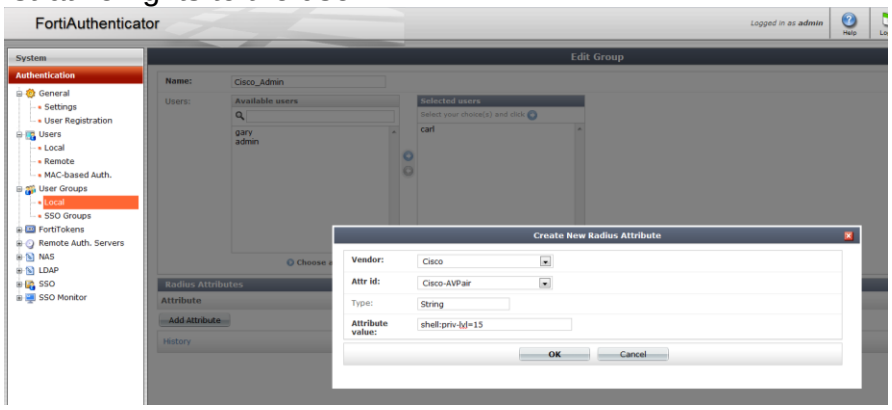
Configure Enable Authorization

To directly authenticate the user into enable mode, it is possible to include an authorization attribute in the RADIUS Access-Accept packet. Cisco uses the following attribute from their standard RADIUS Dictionary for this purpose:

```
Cisco-AVPair = shell:priv-lvl=15
```

RADIUS Attributes can be configured either at the group or user level. The following example sets this attribute at the group level but the configuration mechanism is the same for both.

- Browse to *Authentication → User Groups → Local* and create a new group called ***Cisco_Admins***. Add the required users to this group.
- Edit the Group and select *Add Attributes*.
- Select the *Vendor* ***Cisco*** and *Attribute-ID* ***Cisco-AV-Pair***
- In the *Attribute Value* field enter shell:priv-lvl=15 which specifies to give full administrative rights to the user.



Create a second Attribute with *Vendor* ***Default*** (this is the RADIUS RFC standard

dictionaries), *Attribute-ID* ***Service-Type*** and *Attribute Value* ***NAS-Prompt-User***.

To configure the switch to accept these attributee, enter the following configuration

```
Switch(config)#aaa authorization exec default radius
```

Attempt to login again

```
telnet 192.168.0.253
User Access Verification

Username: john.doe
Password: fortinet

Please enter token:983403

Switch#
```

Notice that the user is granted the enable (15) privilege level denoted by #.

Privilege Levels

The default Cisco IOS privilege levels are defined as:

Privilege Level	Result
0	Seldom used, but includes five commands: disable, enable, exit, help, and logout
1	User level only (prompt is switch>). The default level for login
15	Privileged level (prompt is router#), the level after going into enable mode

Whilst authorization levels 0, 1 and 15 are configured by default, levels 2 to 14 are undefined and can be used to create additional levels by adding and removing specific CLI commands e.g.

To specify which commands will exist in privilege level 7, issue the following commands on Switch1 from the console:

Switch1(config)# privilege configure level 7 snmp-server host
Switch1 (config)# privilege configure level 7 snmp-server enable
Switch1 (config)# privilege configure level 7 snmp-server
Switch1 (config)# privilege exec level 7 ping

Switch1 (config)# privilege exec level 7 configure terminal
Switch1 (config)# privilege exec level 7 configure

This level can be then authorized by creating a separate FortiAuthenticator group, including the required users and specifying the new RADIUS Attribute privilege level e.g.

```
Cisco-AVPair = shell:priv-lvl=7
```

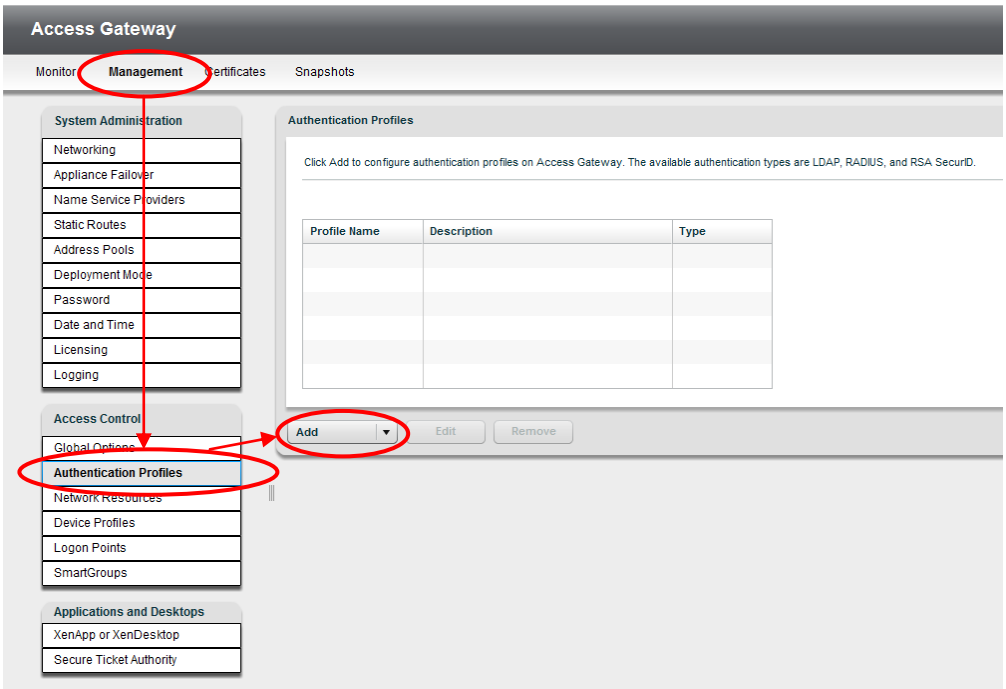
Citrix Access Gateway 5.0

Caution

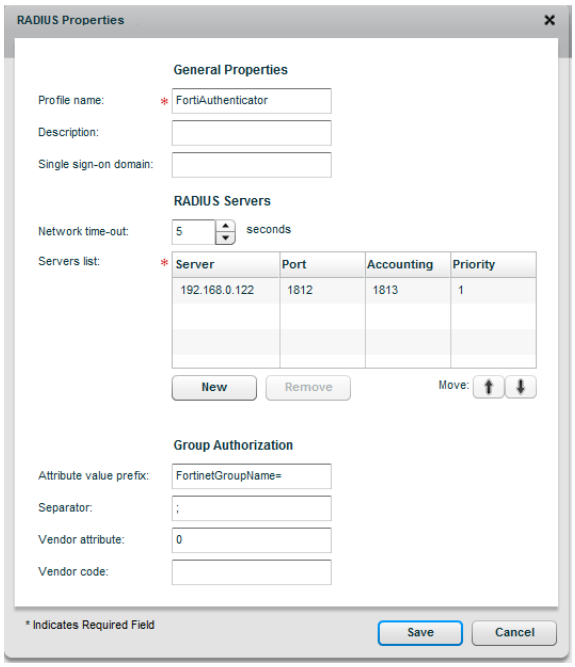
Before proceeding, ensure that you have followed the steps detailed in Chapter 2. Pay particularly attention to Section 2.2.5:- Configure a NAS and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Configure the RADIUS Server

Log into the Citrix Access Gateway Management GUI https://<Management IP>/lp/AdminLogonPoint and browse to Management Access → Control → *Authentication Profiles*. Select ***Add***.



Enter the details of the remote FortiAuthenticator including the IP Address and shared secret and click ***Save***



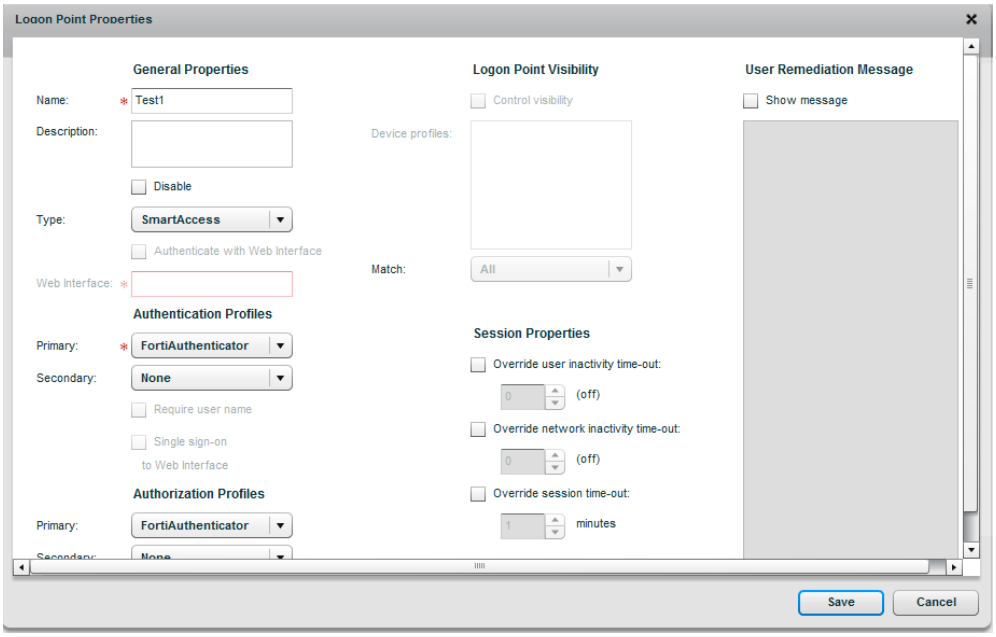
Create a logon point

Note

A logon point in Citrix Access Gateway is the URL to which the user logs on to access a protected resource. In this example, a test Logon Point is created but the same detail can be used to modify an existing Logon Point

Browse to Access Control → *Logon Points*. Select ***New***.

Create a Test logon point e.g. ***Test1*** with *type* ***SmartAccess.*** Select the FortiAuthenticator as the Primary Authentication Profile as created in the previous section. Optionally configure an authorisation profile using the same FortiAuthenticator settings. Select ***Save***.



User logon to the Citrix Access Gateway

There are 2 option for FortiAuthenticator authenticated logon to the Citrix Access Gateway:

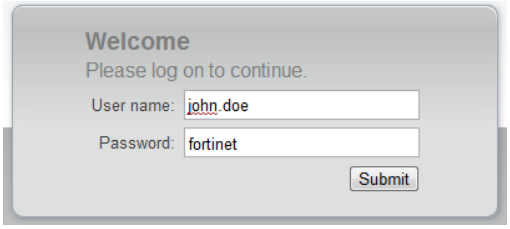
- Token Appended
- Challenge-Response

Challenge-Response is the most simple method for users and is shown below

Attempt to log into the Citrix Access Gateway User GUI with the user credentials from the FortiAuthenticator. The Username and Password can be entered without the token PIN e.g.

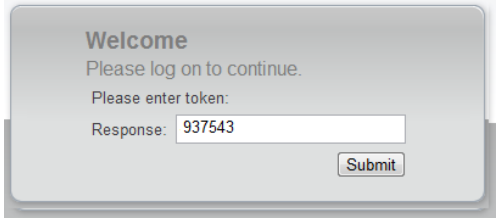
```
Username: john.doe
Password: <password>
```

e.g. for a Password “fortinet” and one-time PIN of 937543, the login would become



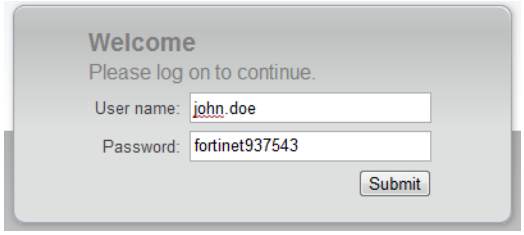
However obviously the password would be starred out. The FortiAuthenticator detects

the missing token PIN and sends a RADIUS challenge which the Citrix Access Gateway presents to the user



Successful authentication will provide the user with access to the Citrix Access Gateway resource.

As an alternative a single step login can be made to bypass the challenge e.g.



Successful authentication will provide the user with access to the Citrix Access Gateway resource and will generate a login event in *Monitor → Audit*

```
192.168.0.254 - 0xb0409002a18b9b1:john.doe\:Test1: [04/Apr/2012:06:08:41 -
0700] "" - - "" "" Login "NavUI"
```

If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

Linux Login

Linux uses Pluggable Authentication Modules (PAM) to extend the usual local authentication methods out to external third party devices.

This makes Linux is very flexible in how it can be integrated with two-factor authentication. Applications can be configured so that e.g. locally accessed services can be authenticated via password only whilst applications accessible over the internet can be authenticated using strong two-factor methods.

The instructions below are for Ubuntu 11.04 however, PAM is pretty standard across all Linux distributions so the instructions should be usable with only minor changes.

Integrating Linux with RADIUS (FortiAuthenticator)

In order to integrate with RADIUS authentication and therefore FortiAuthenticator, first you must install the PAM RADIUS Module

```
$ sudo apt-get install libpam-radius-auth
```

Once installed, edit *`/etc/pam_radius_auth.conf`*. The default configuration will contain the following examples (commented out):

```
#127.0.0.1      secret             1
#other-server    other-secret       3
```

To configure the FortiAuthenticator, add an additional line of the format

```
<FortiAuthenticator Name / IP>      <RADIUS Shared secret>
<Timeout>
```

e.g.

```
192.168.0.110       fortinet    3
```

To configure the FortiAuthenticator, add an additional line of the format

Enabling Strong Authentication for SSH

Caution

Before configuring, make sure that the user you are trying to authenticate already

exists on the Linux system. This limitation will be covered in a later section.

To enable two factor authentication in SSH by editing the file *`/etc/pam.d/ssh`* and insert the following lines in before the line `# Standard Un*x authentication`

```
# Enable Two-Factor Authentication with FortiAuthenticator
auth       sufficient     pam_radius_auth.so         debug
```

* Note that the debug option at the end of the line increases debugging sent to *`/var/log/auth.log`* and can be removed once successfully configured.

Attempt to log into SSH using your chosen client with your new credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

```
Username: john.doe
Password: <password><Token PIN>
```

e.g. for a Password "fortinet" and one-time PIN of 947826, the login would become

```
login as: john.doe
Password: fortinet947826
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-10-generic i686)
Last login: Mon Aug 22 18:09:18 2011 from 192.168.0.24
john.doe@Scooter:~$
```

However obviously the password would be starred out.

Successful authentication will provide the user with access to the system via SSH and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

Enabling Challenge-Response

The configuration described above requires the user to log in with the RADIUS username and password appended with the PIN. The benefit of this is that it supports almost any system which can authenticate with RADIUS. However, the FortiAuthenticator also supports a challenge-response mechanism. When the platform detects that only the password has been returned, it will respond with a RADIUS Challenge-Response and expect the PIN to be returned. This requires the client to support this additional step which the OpenSSH server does.

To configure this step on the SSH Server, edit *`/etc/ssh/sshd_config`* and change

```
ChallengeResponseAuthentication no
```

to

```
ChallengeResponseAuthentication yes
```

And restart the SSH Server to apply the setting

```
$ sudo restart ssh
```

Apache

This document details how to enable RADIUS authentication in Apache2 for use with FortiAuthenticator two-factor authentication. If Apache2 is not installed, install it with

```
sudo apt-get install apache2
```

The Ubuntu 11.04 build of Apache2 comes with the mod-auth-radius module installed and enabled, however, if you need to manually install it

```
sudo apt-get install libapache2-mod-auth-radius
```

and enable it with

```
a2enmod auth_radius
```

At this point, confirm that you can browse to the Apache2 server via http://localhost/ or via the IP/FQDN of your test server.

Modifying the Apache configuration

There is a great deal of documentation on the internet recommending where to place the relevant configurations lines about to be described. The majority of this does not appear to work with the current installation of Apache2 on Ubuntu 11.04 for whatever reason.

The majority of documentation recommends that the RADIUS server configuration is put into *`/etc/apache2/apache2.conf`* or *`/etc/apache2/httpd.conf`* however, this does not work and generates an error in the *`/var/log/apache2/error.log`*

```
[warn] AuthRadiusActive set, but no RADIUS server IP - missing
AddRadiusAuth in this context?
```

The following has been tested and confirmed to work correctly.

Edit the default site *`/etc/apache2/sites-enabled/000-default`* , or your specific server site if this is configured, adding the lines shown in **bold** in the positions specified:

```
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        AddRadiusAuth 192.168.0.110:1812 fortinet 5:3
        AddRadiusCookieValid 5
        DocumentRoot /var/www
        <Directory />
```

```
                Options FollowSymLinks
                AllowOverride None
                AuthType Basic
                AuthName        "FortiAuthenticator        Secure
Authentication"
                AuthBasicAuthoritative Off
                AuthBasicProvider radius
                AuthRadiusAuthoritative on
                AuthRadiusActive On
                Require valid-user
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
  </Directory>
```

When completed, restart the Apache2 daemon

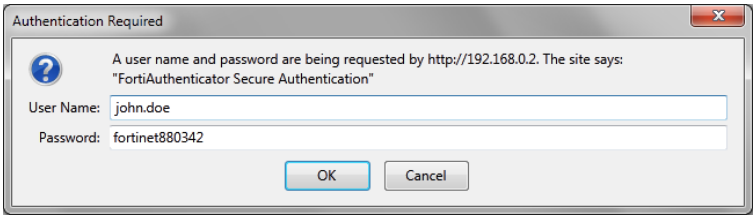
```
sudo /etc/init.d/apache2 restart
```

Clear the cache on your browser and restart to avoid any locally cached content from being displayed without the need for authentication (can be confusing when debugging).

Browse to the web site configured e.g. http://localhost/ and you should be prompted for your credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

```
Username: john.doe
Password: <password><Token PIN>
```

e.g. for a Password “fortinet” and one-time PIN of 880342, the login would become



However obviously the password would be starred out.

Successful authentication will provide the user with access to the page and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong. Additional debugging can be performed using the Apache2 logs located in `/var/log/apache2`. Most useful is the error.log which will display a log if the RADIUS server credentials are incorrectly configured.

Debugging

FortiAuthenticator is incredibly simple to get working however, should you encounter difficulty there are some simple steps which can be taken to diagnose the problem.

Logging

If authentication is failing on your NAS, the first place to check to see why is the FortiAuthenticator log files.

Bad Password

Pretty self-explanatory, try resetting the password if the user insists they have the correct credentials.

276	Tue Aug 23 11:37:04 2011	information	Event	Authentication	20102	RADIUS:Authentication failed, bad password	john.doe

If this persists, verify that the pre-shared secret is correct on both the NAS and the FortiAuthenticator.

Bad Token Code

This may be due to user error (entering the incorrect Token) or may be caused by time issues.

277	Tue Aug 23 11:38:16 2011	information	Event	Authentication	20103	RADIUS:Authentication failed, bad token code	john.doe

To debug this issue, verify the following:

- Ensure the user is not trying to use a previously used Token number. i.e. you cannot log in twice with the same Token number.
- The time and time zone on the FortiAuthenticator is correct and preferably synchronised using NTP.
- The Token is correctly synced with the FortiAuthenticator. Verify the drift by syncing the token as shown in Section

Nothing Logged

If there is no failure or successful authentication logged. This will be due to one of two things:

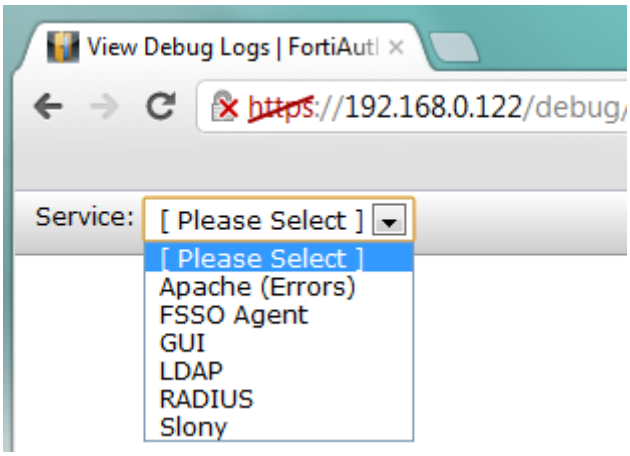
- **Request is not reaching the FortiAuthenticator**
    - Verify that any intervening firewalls are permitting the required traffic through the network. RADIUS Authentication traffic will require UDP Port 1812 opening to the FortiAuthenticator and pseudo-stateful responses allowed to return.

- **Request is reaching the FortiAuthenticator but is being ignored**
  - If traffic is seen reaching the FAC (e.g. by packet sniffing) but is being ignored, it is most likely that the requesting NAS not configured in the FortiAuthenticator. Verify that the NAS is sending the traffic from the expected IP and not from a secondary IP or alternative interface. The FortiAuthenticator RADIUS server will not respond to requests from an unknown NAS for security reasons.
  - One other, less likely possibility is the NAS_Calling_IP Attribute is set to an incorrect value.

Extended Logging

The standard GUI Logs found Logging → Log Access → Logs provide a concise summary of events occurring on the system, particularly the information needed for audit purposes (who logged in, when and where from). However there are times when a more detailed view is required in order to debug issues.

Detailed system and application logs can be found by browsing to http://<FAC_IP>/debug .



There are several log files as detailed below with the most useful **highlighted in Bold**:

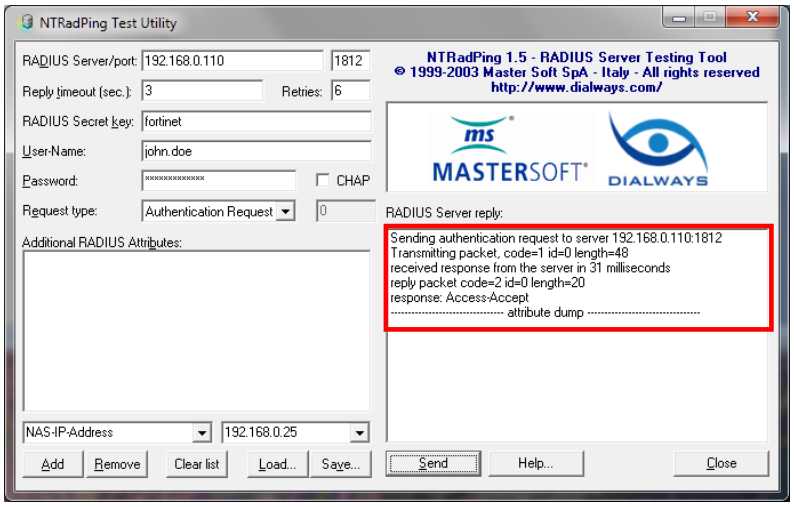
Apache (Errors)	-	Errors encountered by the WebServer.
FSSO Agent	-	Details of Fortinet Single Sign-On events
GUI	-	Errors encountered whilst rendering the appliance GUI
LDAP	-	**Details of the LDAP authentication process for both local and remote connections**
RADIUS	-	**Details of the RADIUS authentication process**
Slony	-	Detail of the HA process

Traffic Sniffing

It is useful to be able to monitor traffic being sent and received to the FortiAuthenticator. This is achieved by using Wireshark to capture traffic on UDP port 1812.

RADIUS Packet Generation

Testing authentication directly without the use of a NAS device is useful to rule out issues with the NAS device. This is most easily achieved by using a tool such as NTRADPing



Appendix A – Supported Two-Factor Authentication Methods

Product	Feature	FortiToken	FortiToken (Sync)	FortiAuthenticator (Token Appended)	FortiAuthenticator (Token Challenge)	Wildcard Users	Tested Version
FortiGate 4.0	**NAT Route Mode**						
	Web Based Management	Supported	Not Supported	Supported	NFR: 41120	Supported	**FortiGate 4.0 MR3 PR6**
FOS 4.0 MR3 PR5	SSH Based Management	Supported	Not Supported	Supported	Not Supported	Supported	**FortiClient 4.0 MR3 GA**
	Telnet Management	Supported	Not Supported	Supported	Not Supported	Supported	
	IPSEC VPN (FortiClient)	Supported	Not Supported	Supported	Supported	Supported	
	SSL VPN (Web)	Supported	Not Supported	Supported	Supported	Supported	
	SSL VPN (FortiClient)	Supported	Not Supported	Supported	Supported	Supported	
	Identity Based Policy	Supported	NFR Scheduled 5.0	Supported	Supported	Supported	
	Web Filtering Overrride	Not Supported	Not Supported	Supported	Not Supported	Supported	
	Explicit Proxy						
	Identity Based Policy (Basic Auth)	Bug (Connection Reset)	Not Supported	Supported	Not Supported	Not Supported	
	Identity Based Policy (Forms Auth)	Bug (Connection Reset)	Not Supported	Supported	Not Supported	Not Supported	
	Web Filtering Overrride	Not Supported	Not Supported	Supported	Not Supported	Not Supported	
FortiManager	Web Based Management	Not Supported	Not Supported	Supported	Not Supported	Mantis 145712	**FortiManager 4.3.1**
	SSH Based Management	Not Supported	Not Supported	Supported	Not Supported	Mantis 145713	
FMG 4.0 MRx PRx	Telnet Management	Not Supported	Not Supported	Supported	Not Supported	Mantis 145714	
FortiAnalyzer	Web Based Management	Not Supported	Not Supported	Supported	Not Supported	Not Supported	**FortiAnalyzer 4.0 MR3 PR1**
	SSH Based Management	Not Supported	Not Supported	Supported	Not Supported	Not Supported	
FAZ 4.0 MRx PRx	Telnet Management	Not Supported	Not Supported	Supported	Not Supported	Not Supported	
FortiMail	Web Based Management	Not Supported	Not Supported	Supported	Not Supported	Not Supported	**FortiMail 4.0 MR3 GA**
	SSH Based Management	Not Supported	Not Supported	Supported	Not Supported	Not Supported	
FML 4.0 MRx PRx	Telnet Management	Not Supported	Not Supported	Supported	Not Supported	Not Supported	
FortiWeb	Web Based Management	Not Supported	Not Supported	Supported	Not Supported	Not Supported	**FortiWeb 4.0 MR3 PR6**
	SSH Based Management	Not Supported	Not Supported	Supported	Not Supported	Not Supported	
FWB 4.0 MR3 PR6	Telnet Management	Not Supported	Not Supported	Supported	Not Supported	Not Supported	
Citrix Access Gateway	Web Based Management	Not Supported	Not Supported	Supported	Supported	Supported	**Citrix Access Gateway 5.0**
	SSH Management	Not Supported	Not Supported	Supported	Supported	Supported	
	Web Based User Authentication	Not Supported	Not Supported	Supported	Supported	Supported	
SSH	SSH Login	Not Supported	Not Supported	Supported	Supported	Supported	**OpenSSH version 5.8p1**
Apache	Web Authentication	Not Supported	Not Supported	Supported	Supported	Supported	**Apache 2.2.17**
Tested with FortiAuthenticator 1.0 MR3							

Appendix B – Syncing FortiTokens

Under most circumstances, it is not necessary to synchronise a FortiToken unless the time on the host FortiAuthenticator system has been allowed to deviate from the correct time. It is essential that the time is kept accurate at all times to prevent issues occurring so configuration of an NTP server is recommended.

Under normal operation, the natural drift of the time on the FortiToken (as found in all clocks) is accounted for automatically by the FortiAuthenticator. Every time a user logs in, the FortiAuthenticator calculates the drift and if it is within +/- 1 (where 1 is a token cycle of 60 seconds), the drift is adjusted accordingly. Should the drift deviate by greater than 1 (i.e. the clock is more than 60 seconds out) since the last login, a manually synchronisation is required.

Note

If this is required for several tokens, it is an indicator that the time may be inaccurate on the FortiAuthenticator. Verify the current time and the NTP settings.

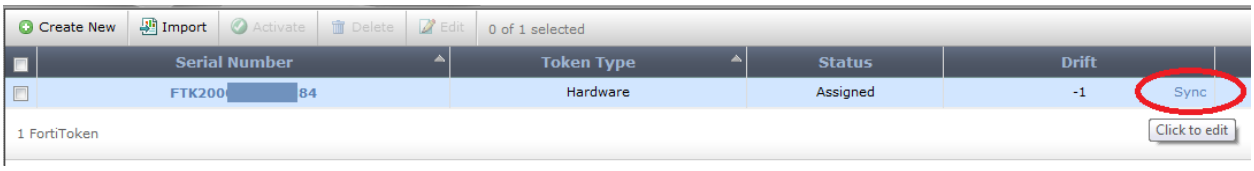
Administrator Synchronisation

It is possible for the administrator to synchronise a token for use on the FortiAuthenticator and sometime advisable when issuing new tokens which have been held in storage for an extended period or are being reissued.

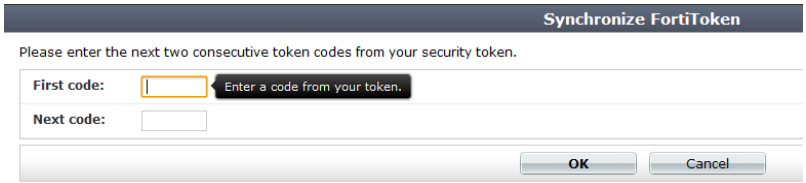
Note

If this is required for several tokens, it is an indicator that the time may be inaccurate on the FortiAuthenticator. Verify the current time and the NTP settings.

Browse to *Authentication → FortiTokens* and hover the mouse over the required token drift category. An option to *sync* will appear



Select Sync and follow instructions to input 2 consecutive Token PINs.



Key points to note during the Synchronisation process are:

- Ensure that the FortiAuthenticator time is accurate before proceeding
- Ensure the serial of the token you are trying to syncronize matches that on the reverse of the token.
- Ensure that the token has not been used in the preceding 60 seconds. All tokens are one time passwords and cannot therefore be used to authenticate (successful or otherwise) and synchronize.
- Once successfully synchronised, wait a further 60 seconds before attempting to log in. A token used to synchronize cannot be re-used to authenticate.

User Synchronisation

Should it be required, FortiAuthenticator provides a mechanism for the user to perform their own manual synchronisation. The user should be allowed to access the FortiAuthenticator WebUI e.g https:/<FAC_IP>/login/.

On logging into the FortiAuthenticator the user will be prompted to enter their token PIN. If the token PIN is out of sync, they will be prompted to enter 2 consecutive PINs. If the user receives no such prompt, the token is already correctly synchronized.