Configuring FortiGate 200B with RSA SecurID for Two Factor Authentication

Written by Jonathan Tew

Introduction

Our company had an existing RSA installation and wanted to leverage this investment with new FortiGate appliances. The installation was not as easy as we had anticipated even though both vendors hold leadership positions in their respective industries. The available documentation did not cover the actual scenario of true two factor authentication. We were able to determine the proper configuration and it is relatively straight forward. We wanted to document the configuration to improve what is available to the internet community.

Assumptions

This documentation assumes the following components are in place:

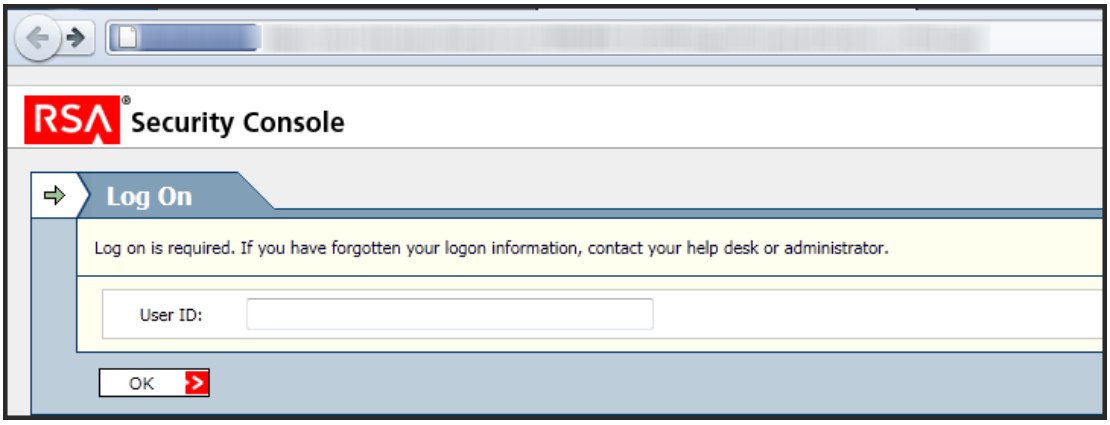
- Fortinet 200B Appliance with version 4.0 MR2 Patch 6
- RSA SecurID 130 Appliance

We also assume that you have experience creating your own certificate authority and generating a certificate for the appliance and end users.

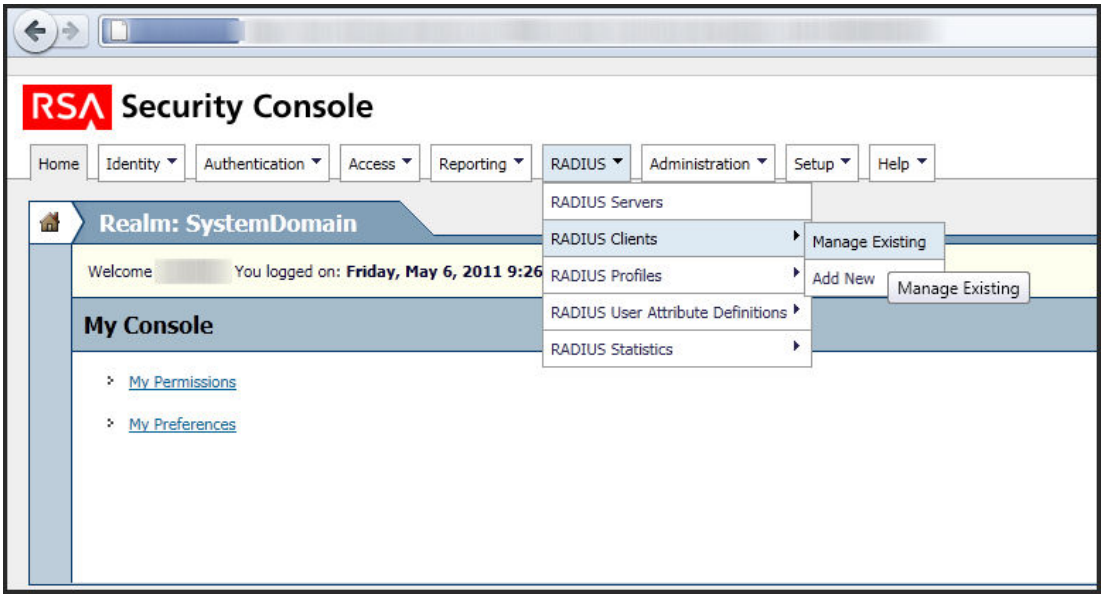
Please note that any sensitive information is blurred out. It's a faint blur, so examine the images carefully to note that certain fields are filled in, but blurred.

Configuring the RSA SecurID

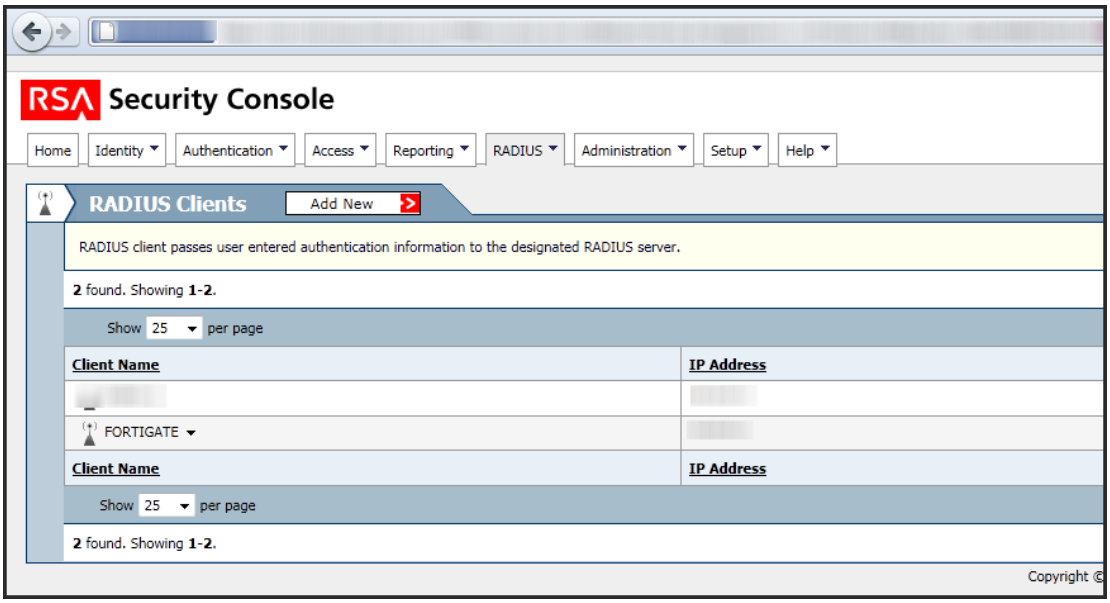
First go to the IMS Console for SecurID and login



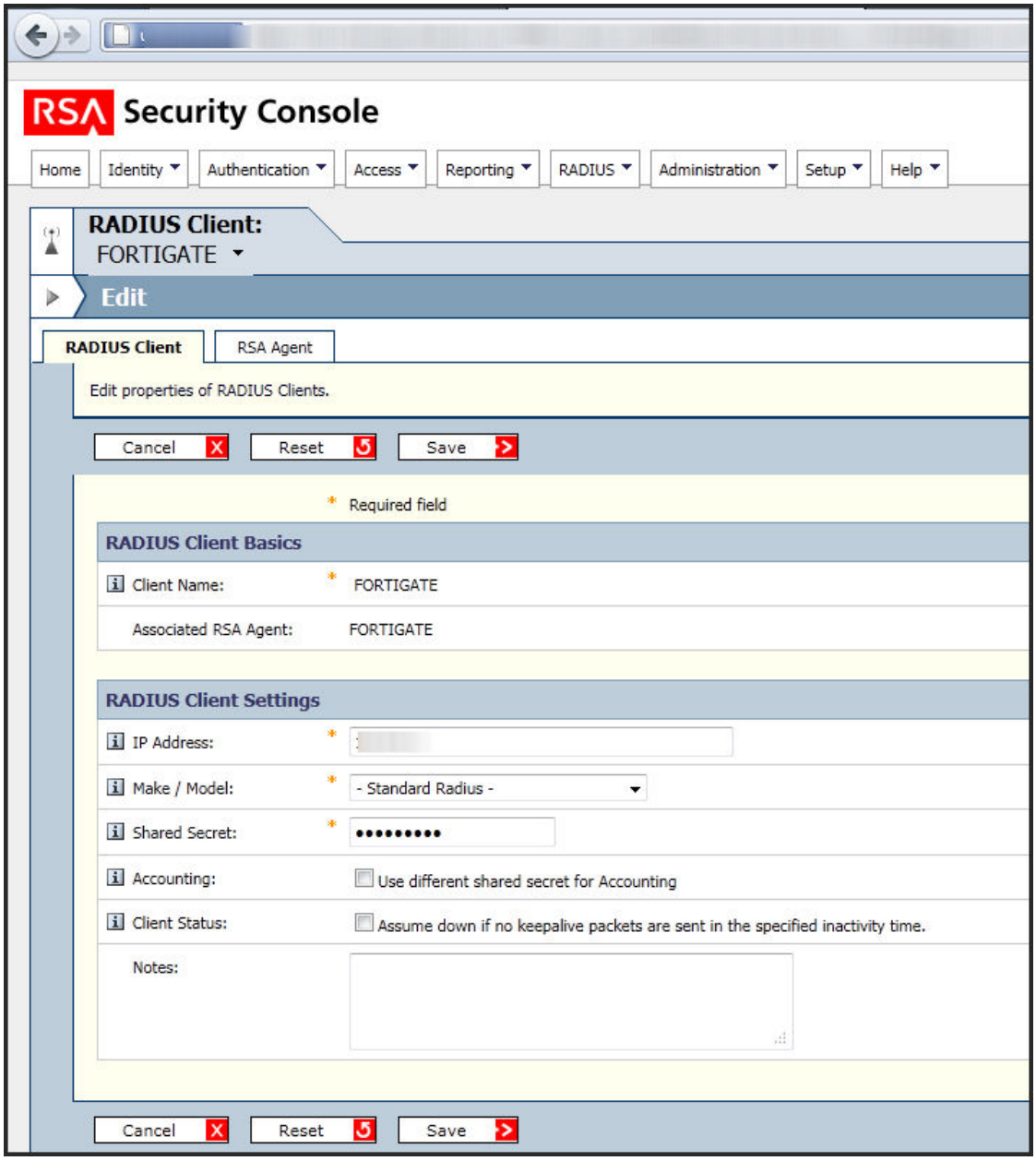
Next go to RADIUS -> RADIUS Clients -> Manage Existing.



Since I've already configured my FORTIGATE RADIUS client you will see it in the screen shot below. If you are performing a new configuration then click on the "Add New" button.

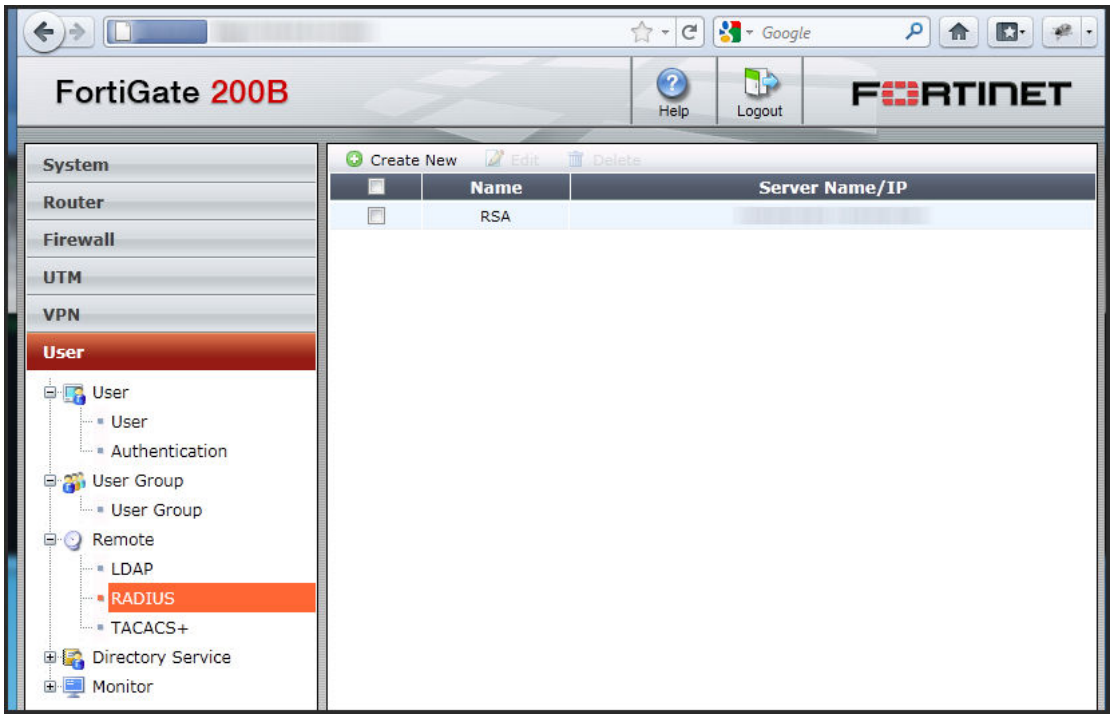


The configuration is really simple. Just make sure the IP address matches the internal management IP address of the FortiGate unit.

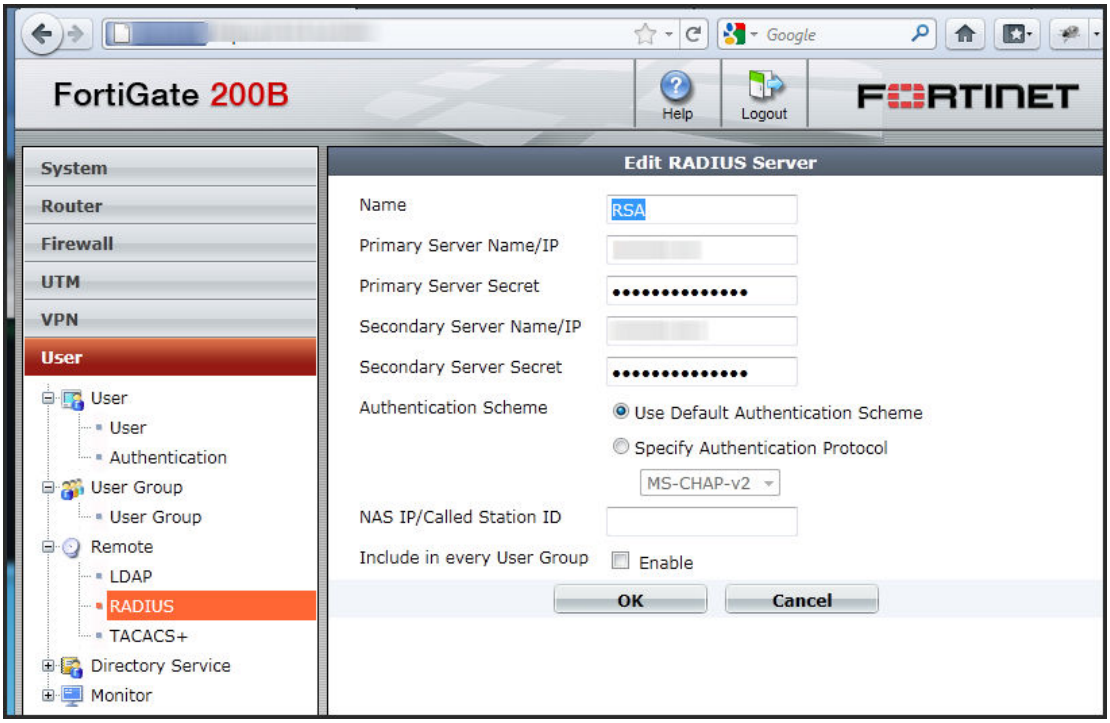

RSA Security Console
Home
Identity
Authentication
Access
Reporting
RADIUS
Administration
Setup
Help
RADIUS Client:
FORTIGATE
Edit
RADIUS Client
RSA Agent
Edit properties of RADIUS Clients.
Cancel
Reset
Save
* Required field
RADIUS Client Basics
Client Name: * FORTIGATE
Associated RSA Agent: FORTIGATE
RADIUS Client Settings
IP Address: *
Make / Model: * - Standard Radius -
Shared Secret: *
Accounting: Use different shared secret for Accounting
Client Status: Assume down if no keepalive packets are sent in the specified inactivity time.
Notes:
Cancel
Reset
Save

FortiGate Configuration RADIUS Configuration

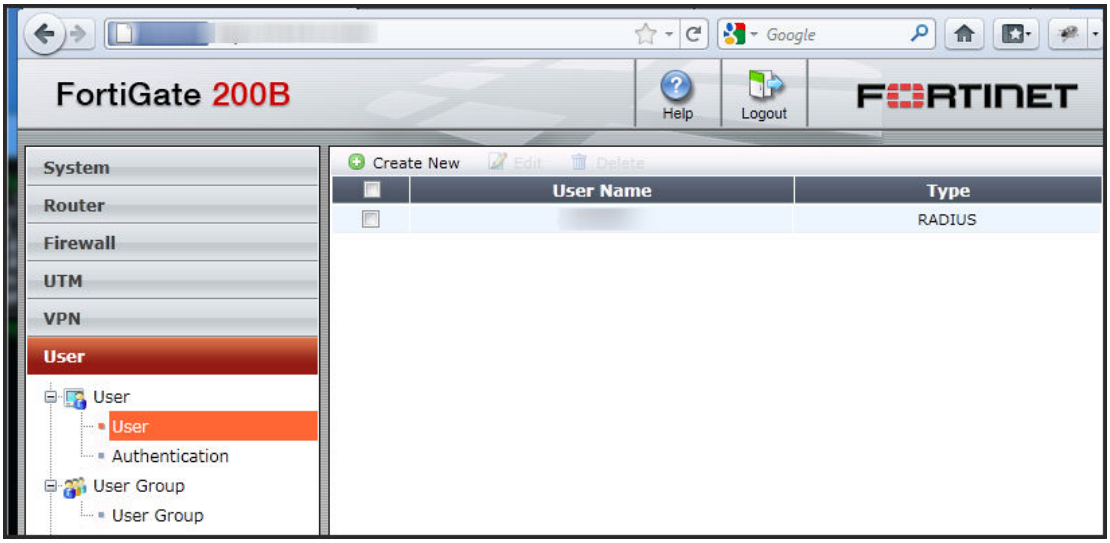
The next step is configuring the FortiGate RADIUS user. Begin by navigating to User → Remote → RADIUS. Here you will see I have a Remote user named "RSA" configured.



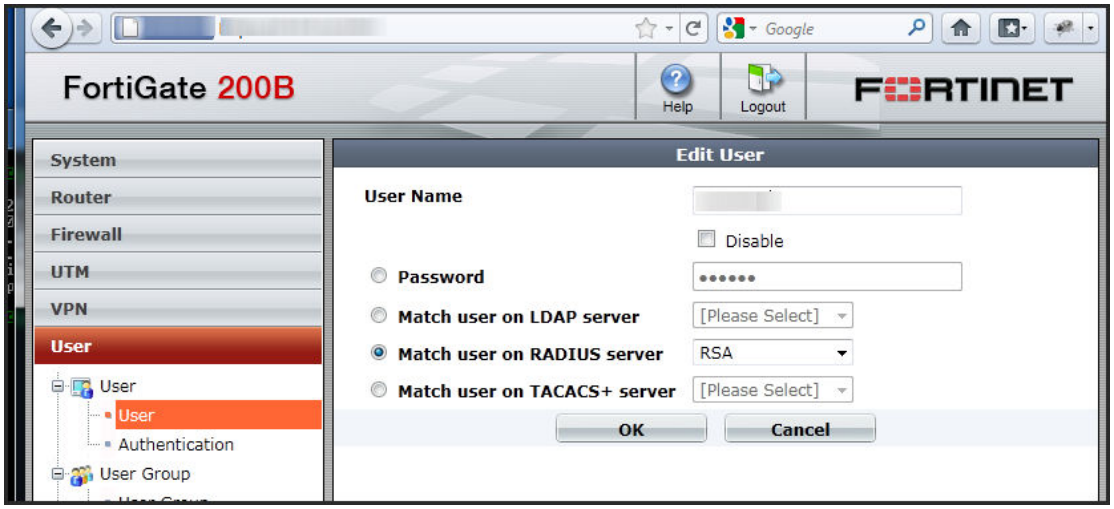
Notice that the configuration of the RSA user is relatively simple. I have the Primary and Secondary IP address (blurred out) configured for the RSA SecurID 130 appliances.



Next we need to create an actual user under User → User → User in the left hand navigation. Notice that I've created a single user with the type of RADIUS below.



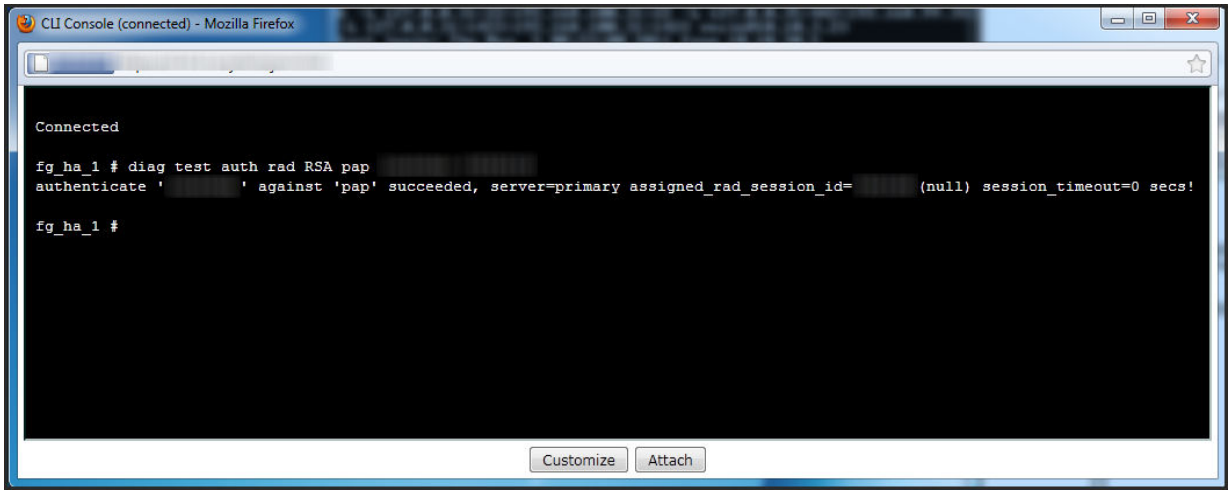
Notice that the user is simple to configure. I've provided the username (which needs to match the user on the RSA box) and selected Match user on RADIUS server and selected RSA. This means that when the user tries to connect the authentication credentials are sent over to the RSA server for validation.



At this point we have a user that is doing OTP authentication with the RSA SecurID appliance. I learned how to test this authentication with the RSA box on the command line from a CryptoCard FortiGate implementation guide. *Thanks CryptoCard for the excellent documentation!* So if we open up the CLI console and type in the following command:

```
diag test auth rad <radius server name><auth protocol><username><One-Time Password>
```

We should see it successfully authenticate.



At this point though we have only achieved a single factor of authentication (the one time password from the RSA token). We need to have two factors of authentication.

Configuring Certificate Authentication

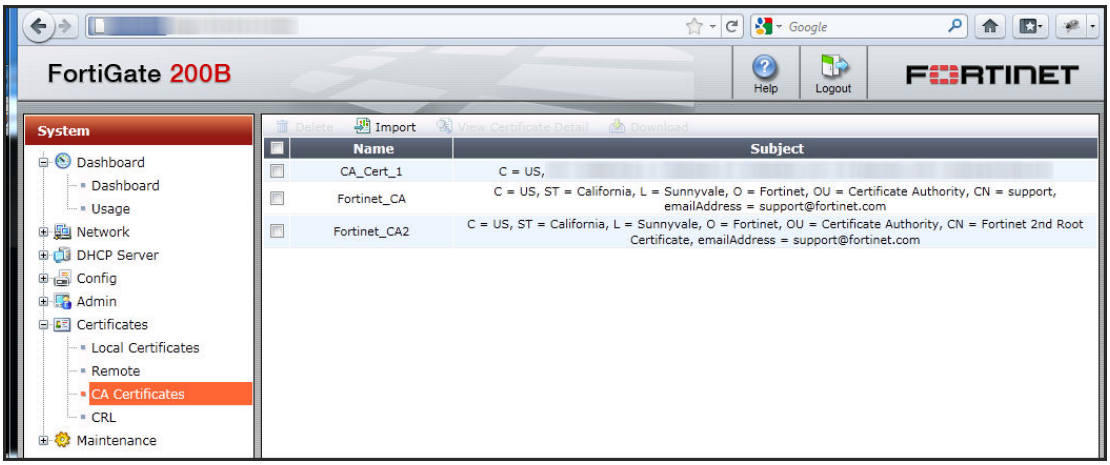
For this exercise you are going to need the following certificates:

- Your own certificate authority root certificate

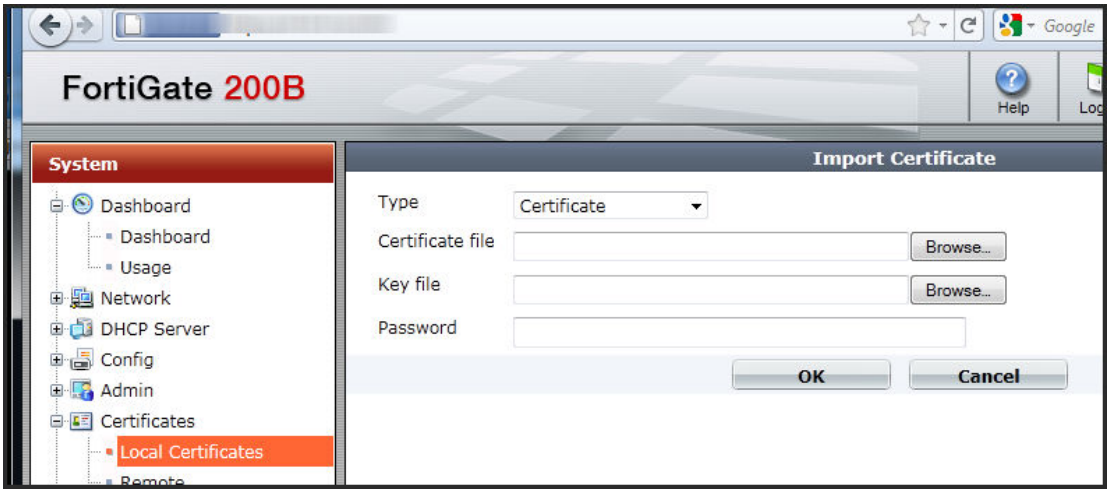
- A private key and certificate for the FortiGate appliance that matches the host name that you are going to access the appliance with.
- A client certificate for your windows machine.

The actual generation of these certificates is out of the scope of this documentation. There are tons of great documents about how to accomplish this task with either Windows Server 2008 or OpenSSL.

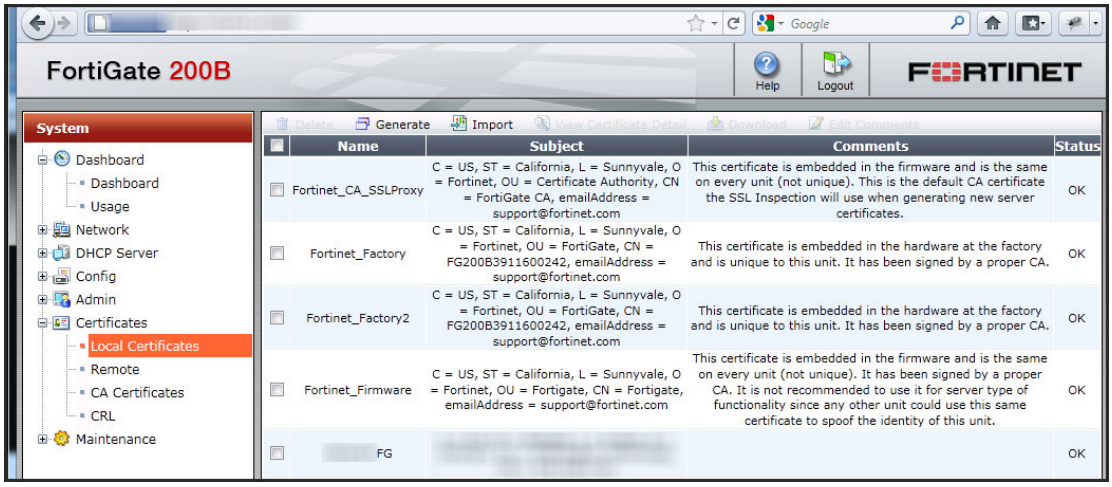
The first step is to import the certificate authority root into the System -> Certificates -> CA Certificates. Click on the Import button and upload the certificate. After the certificate is imported the screen will look like the picture below:



Notice the CA_Cert_1 has been added to the list. Next click on System -> Certificates -> Local Certificates -> Import within the FortiGate left navigation. On that screen choose the type “Certificate” from the drop down list. This will allow you to upload both the certificate and private key file into the FortiGate appliance. You’ll need the private key password which should be provided to you by whoever within your organization generated the key pair.

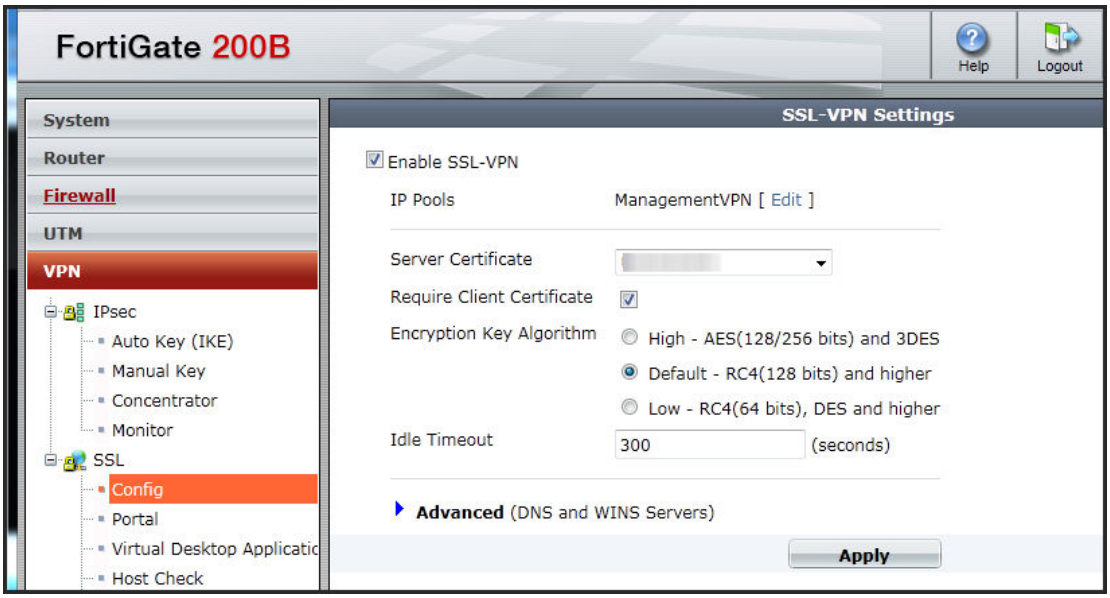


After the certificate is imported it will display in the list underneath all the factory installed FortiGate certificates.

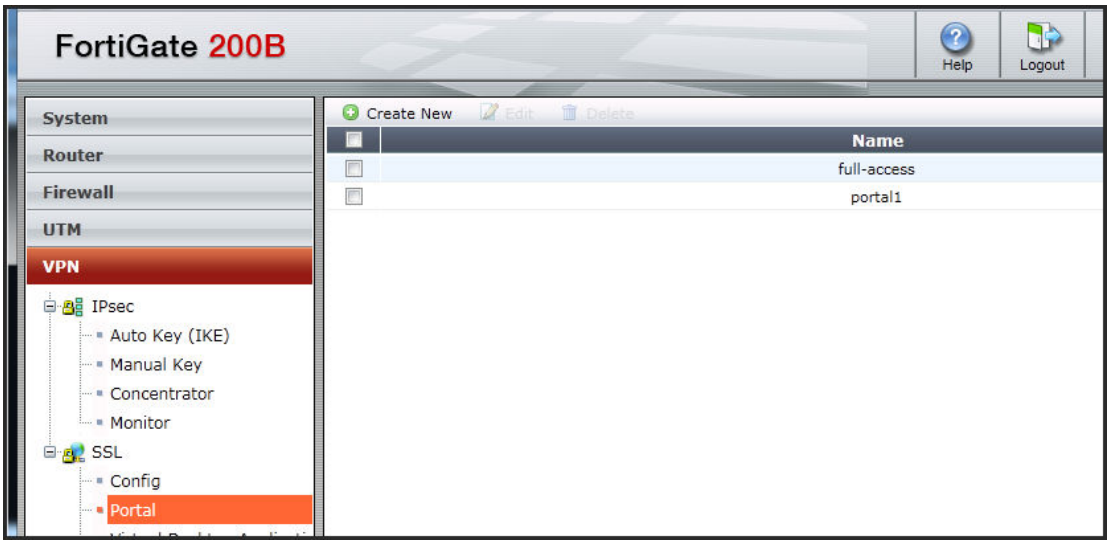

FortiGate 200B
Help
Logout
FORTINET
System
Dashboard
Dashboard
Usage
Network
DHCP Server
Config
Admin
Certificates
Local Certificates
Remote
CA Certificates
CRL
Maintenance
Delete
Generate
Import
View Certificate Detail
Download
Edit Comments
Name
Subject
Comments
Status
Fortinet_CA_SSLProxy
C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FortiGate CA, emailAddress = support@fortinet.com
This certificate is embedded in the firmware and is the same on every unit (not unique). This is the default CA certificate the SSL Inspection will use when generating new server certificates.
OK
Fortinet_Factory
C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FG200B3911600242, emailAddress = support@fortinet.com
This certificate is embedded in the hardware at the factory and is unique to this unit. It has been signed by a proper CA.
OK
Fortinet_Factory2
C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FG200B3911600242, emailAddress = support@fortinet.com
This certificate is embedded in the hardware at the factory and is unique to this unit. It has been signed by a proper CA.
OK
Fortinet_Firmware
C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = support@fortinet.com
This certificate is embedded in the firmware and is the same on every unit (not unique). It has been signed by a proper CA. It is not recommended to use it for server type of functionality since any other unit could use this same certificate to spoof the identity of this unit.
OK
FG
OK

VPN Configuration

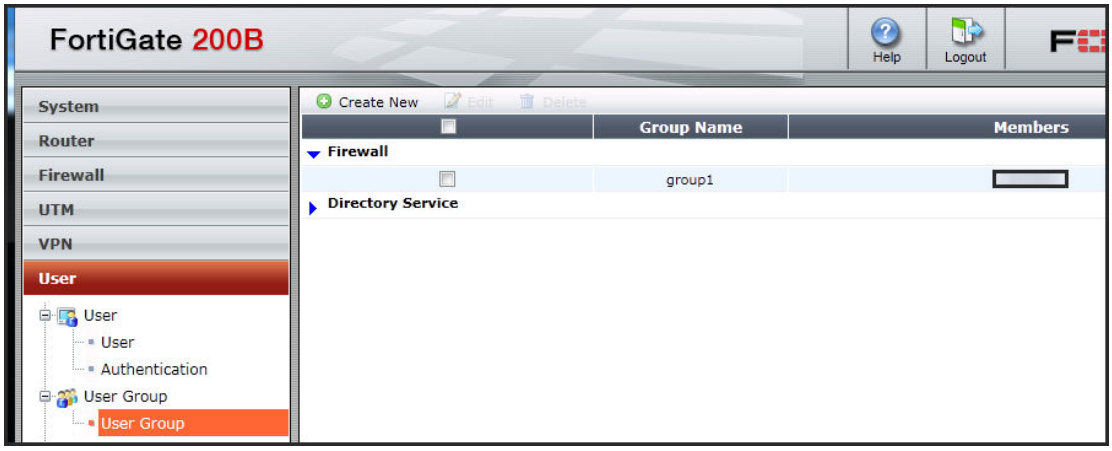
Now that we have the RSA authenticating user configured and the certificates installed on the server we need to configure the VPN. First we need to configure our VPN to use our server certificate and require a client certificate. This is configured under VPN → SSL → Config. The required Client Certificate is what will provide us the second factory of authentication. The client certificate will have to be signed by our internal certificate authority that we imported in the prior steps of this documentation.



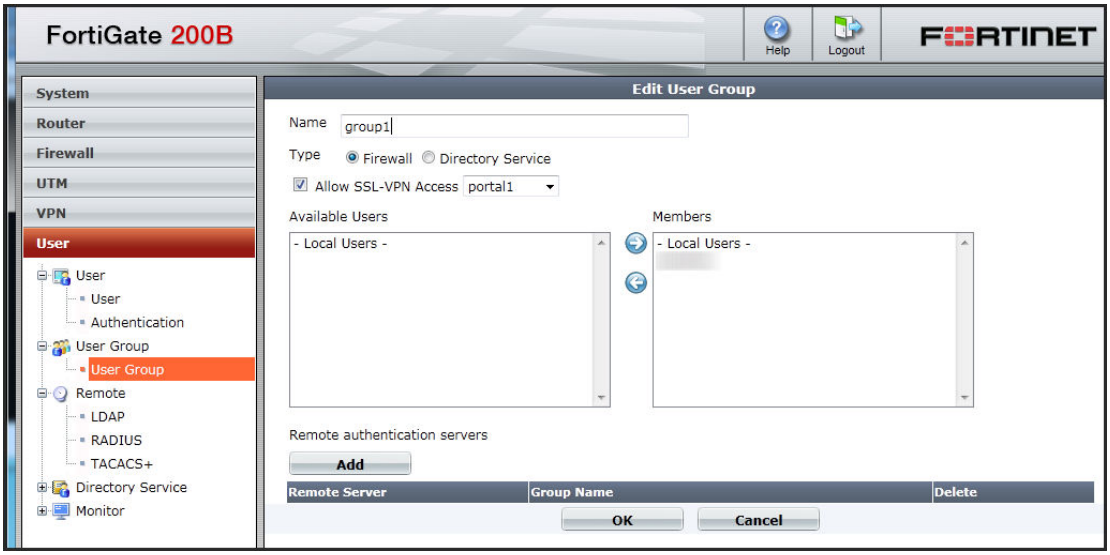
Next configure the VPN portal under VPN → SSL → Portal. In this case we configured "portal1"



Finally we need to configure a user group that includes our user and grants them access to the VPN portal. This configuration is done under User -> User Group -> User Group.



Notice we have a group “group1” configured with our single user over in the members section.

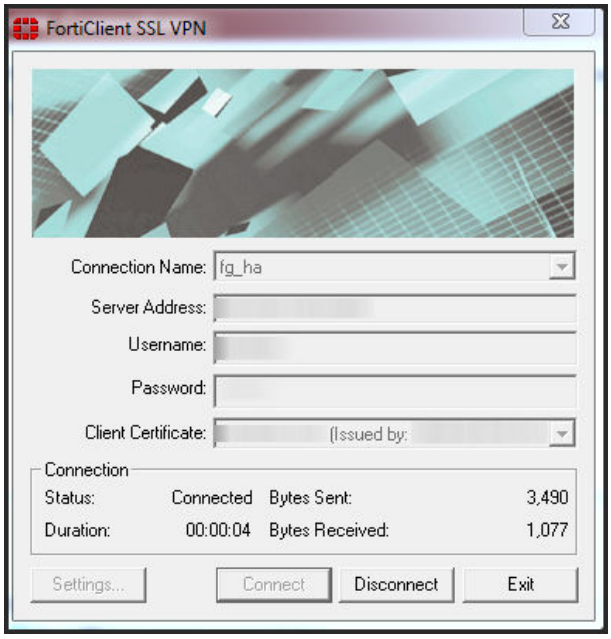


Testing VPN Connection

Before fighting with the FortiClient VPN users you should do the following:

1) Make sure your OTP token is working properly by RSA SecurID by testing it through their self-service console.
2) Test the OTP token on the FortiGate CLI using the diag command shown above.
3) See if you can properly connect to the web interface of the FortiGate at **Error! Hyperlink reference not valid.** Please note that your browser should prompt for your client side certificate AND the server should present the CA signed server certificate. Try logging in through the web interface first. It is more tolerant of token syncing, etc.

If we fire up our FortiClient SSL VPN application we can attempt to connect to the FortiGate we should enter our RSA OTP into the password field and select our client certificate. Only client certificates installed into Windows are going to show in the drop down. Make sure you've installed the certificate. Once you connect it should look like this:



If something is wrong the FortiClient will stop at a certain percentage and display a negative error code. The error messages provide very little meaningful information. There are some CLI commands that can display meaningful information to help debug what is going on:

```
diag deb reset
diagnose debug application sslvpn -1
diag debug enable
```

It is critical to run the "FortiClient SSL VPN" as administrator to successfully connect. You cannot connect without it running as administrator.

We did not complete a connection via the larger FortiClient software. It spawns a "FortiClient SSL VPN" login window like the standalone client does, but in our trial it did not connect successfully.