Fortinet Fortigate Integration

Contents

- 1 Introduction
- 2 Prerequisites
- 3 Baseline
- 4 Architecture
- 5 Swivel Configuration
  - 5.1 Configuring the RADIUS server
  - 5.2 Enabling Session creation with username
- 6 Fortinet Fortigate Configuration
  - 6.1 Fortinet FortigateVersion 3.x Integration guide
  - 6.2 Fortinet Fortigate Version 4.x Integration guide
  - 6.3 Fortinet Fortigate Version 6.x Integration guide
  - 6.4 Test the RADIUS authentication
- 7 Additional Configuration Options
  - 7.1 Forticlient
  - 7.2 Login Page Customisation
- 8 Testing
- 9 Troubleshooting
- 10 Known Issues and Limitations
- 11 Additional Information

Introduction

This document describes steps to configure a Fortinet Fortigate with Swivel as the authentication server.

Prerequisites

Fortinet 3.x appliance and Fortinet 3.x integration script

or

Fortinet 4.x appliance and Fortinet 4.x integration script

Swivel 3.x

NAT/Public IP address if the Single Channel TURing image or other Dual channel images are to be displayed in the login page.

Baseline

Fortinet 3.x

Fortinet 4.x

Fortinet 6.x

Swivel 3.x

Swivel 4.x

Architecture

Fortinet authenticates users through RADIUS, and uses Swivel as a RADIUS server.

Swivel Configuration

Configuring the RADIUS server

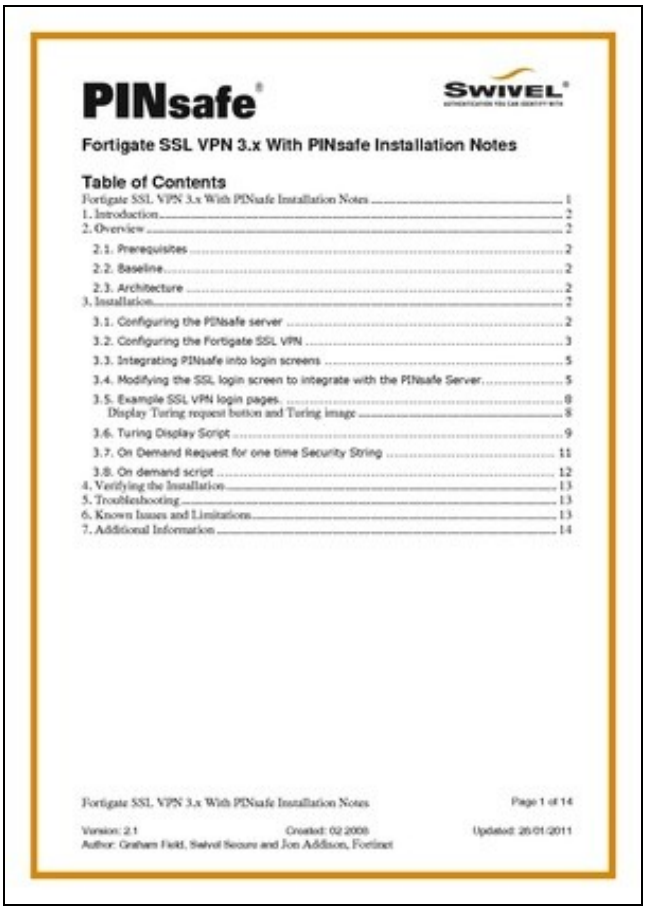
On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

Enabling Session creation with username

To allow the TURing image, PINpad and other single channel images, under Server/Single Channel set Allow session request by username to Yes.

Fortinet Fortigate Configuration

Fortinet FortigateVersion 3.x Integration guide



PINsafe

SWIVEL

Fortigate SSL VPN 3.x With PINsafe Installation Notes

Table of Contents

Fortigate SSL VPN 3.x With PINsafe Installation Notes 1
1. Introduction 2
2. Overview 2
2.1. Prerequisites 2
2.2. Baseline 2
2.3. Architecture 2
3. Installation 2
3.1. Configuring the PINsafe server 2
3.2. Configuring the Fortigate SSL VPN 3
3.3. Integrating PINsafe into login screens 5
3.4. Modifying the SSL login screen to integrate with the PINsafe Server 5
3.5. Example SSL VPN login pages 8
Display Turing request button and Turing image 8
3.6. Turing Display Script 9
3.7. On Demand Request for one time Security String 11
3.8. On demand script 12
4. Verifying the Installation 13
5. Troubleshooting 13
6. Known Issues and Limitations 13
7. Additional Information 14

Fortigate SSL VPN 3.x With PINsafe Installation Notes Page 1 of 14

Version: 2.1 Created: 02 2008 Updated: 26/01/2011

Author: Graham Field, Swivel Secure and Jon Addison, Fortinet

Fortinet Fortigate Version 4.x Integration guide

On the Fortigate Administration console select User/Remote/RADIUS, then click on Create New and enter the following information:

Name A descriptive name for the Swivel RADIUS servers

Primary Server Name/IP The IP or hostname of the Swivel server (Do not use a Swivel VIP in this field)

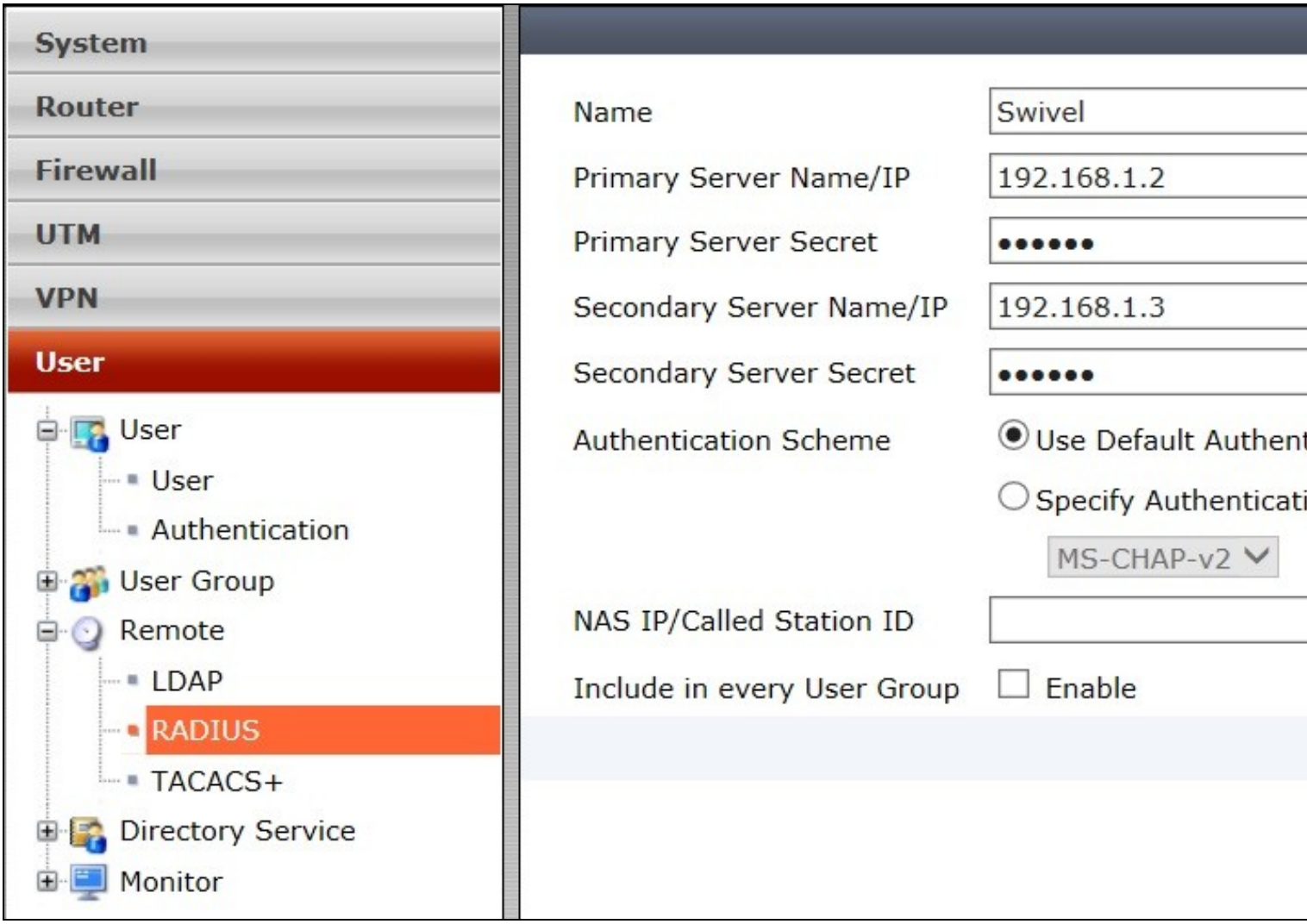
Primary Server Secret The shared secret entered on the Swivel RADIUS NAS

Standby Server Name/IP The IP or hostname of a standby Swivel server (Do not use a Swivel VIP in this field)

Standby Server Secret The shared secret entered on the standby Swivel RADIUS NAS

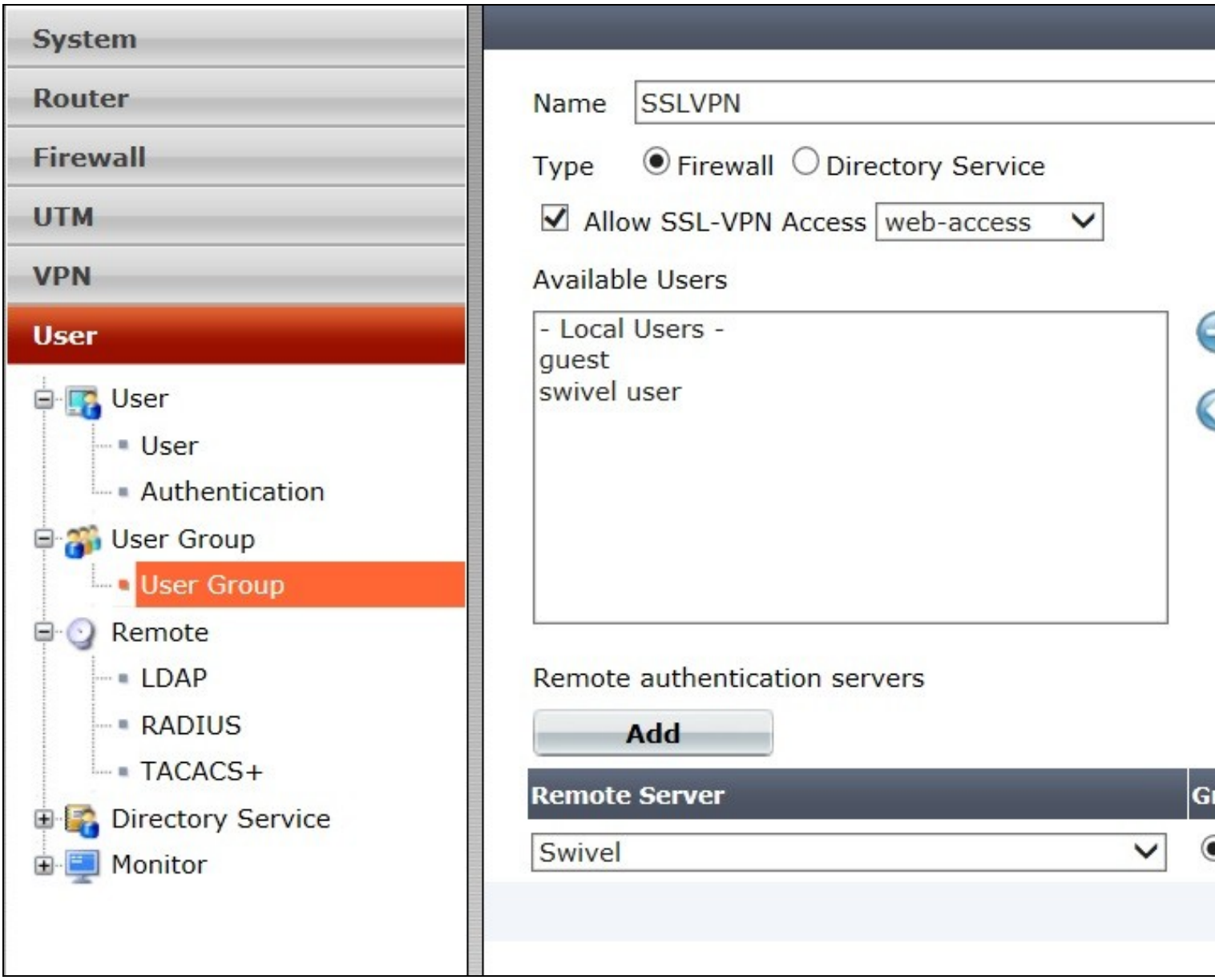
Authentication Scheme leave as Use Default Authentication Scheme unless Mobile App authentication or Check Password With Repository is used, in which case this should be set to use PAP.

By default the Fortigate and Swivel use port 1812 for RADIUS authentication.



On the Fortigate Administration console select User/User Group then select the required group, or create a new one, for Swivel Authentication then and under Remote authentication servers click on Add and select the Swivel Authentication server configured above. If not configured already the SSL-VPN access and any local user authentication can also be configured.

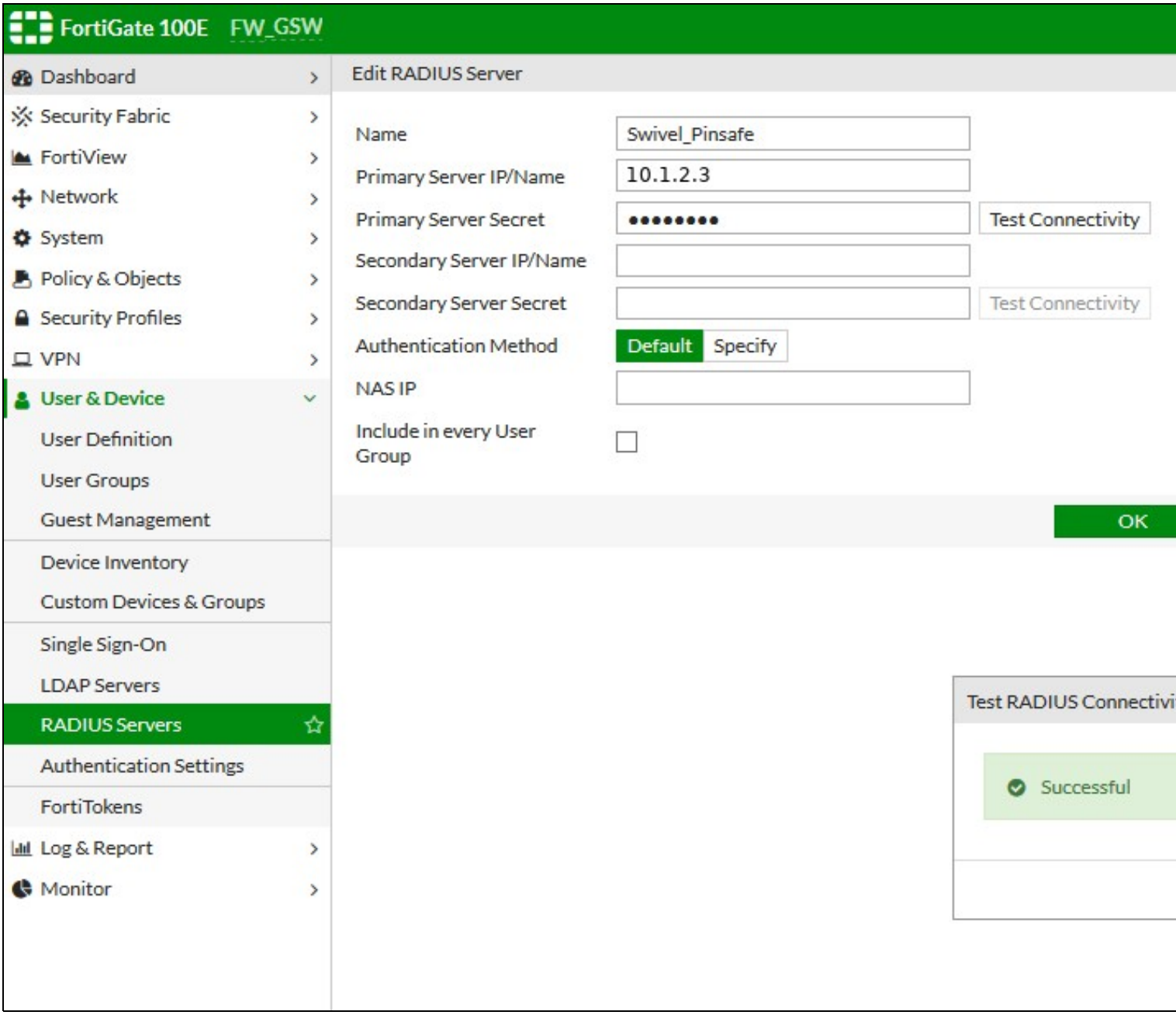
When multiple authentication servers are used, the Fortigate will use the username and password or One Time Code against each starting with local, until a successful authentication is made.



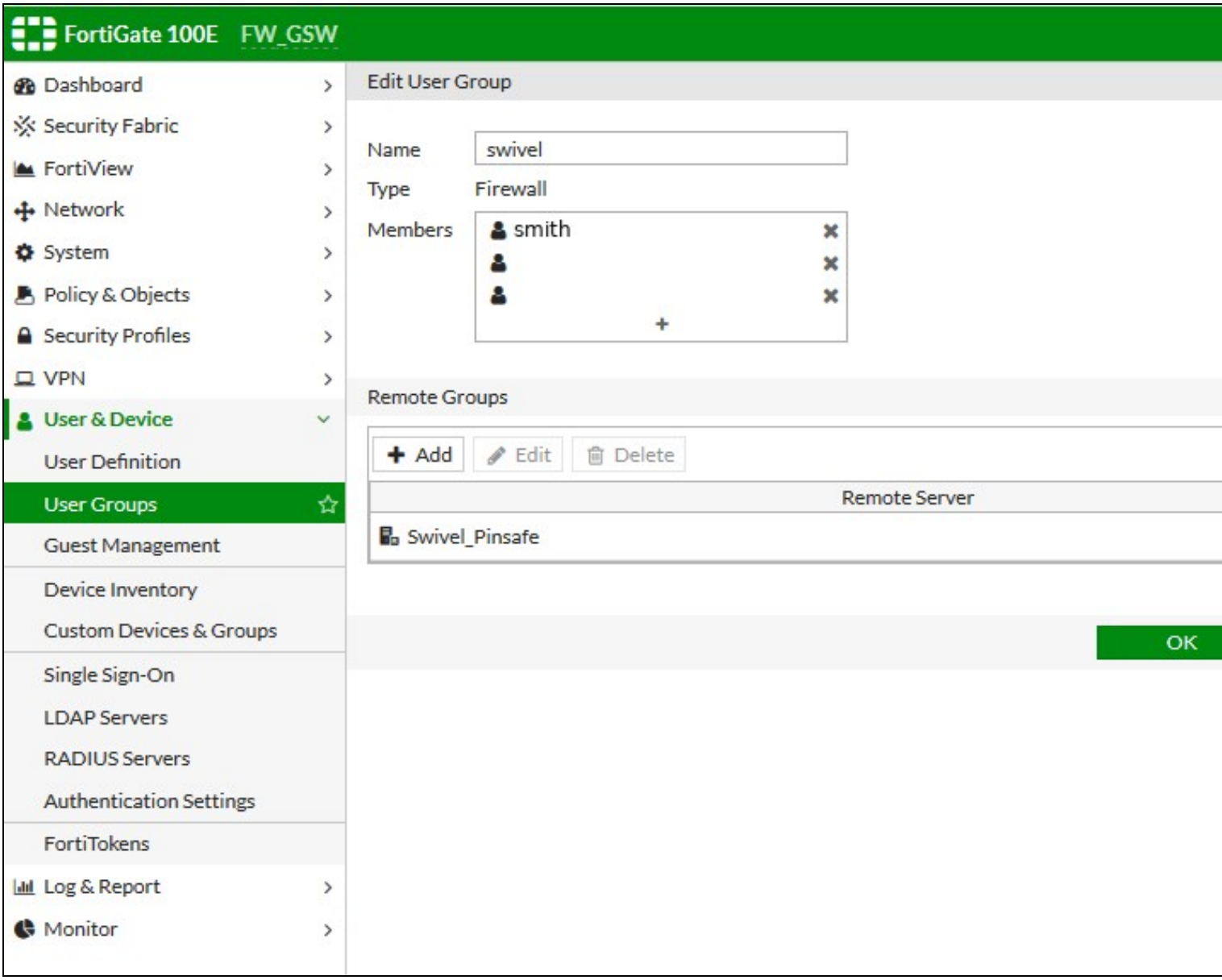
Fortinet Fortigate Version 6.x Integration guide

The images below show the steps to follow for a successful integration between swivel and fortinet products running version 6. Make sure to follow the first steps for integration with v4 products.

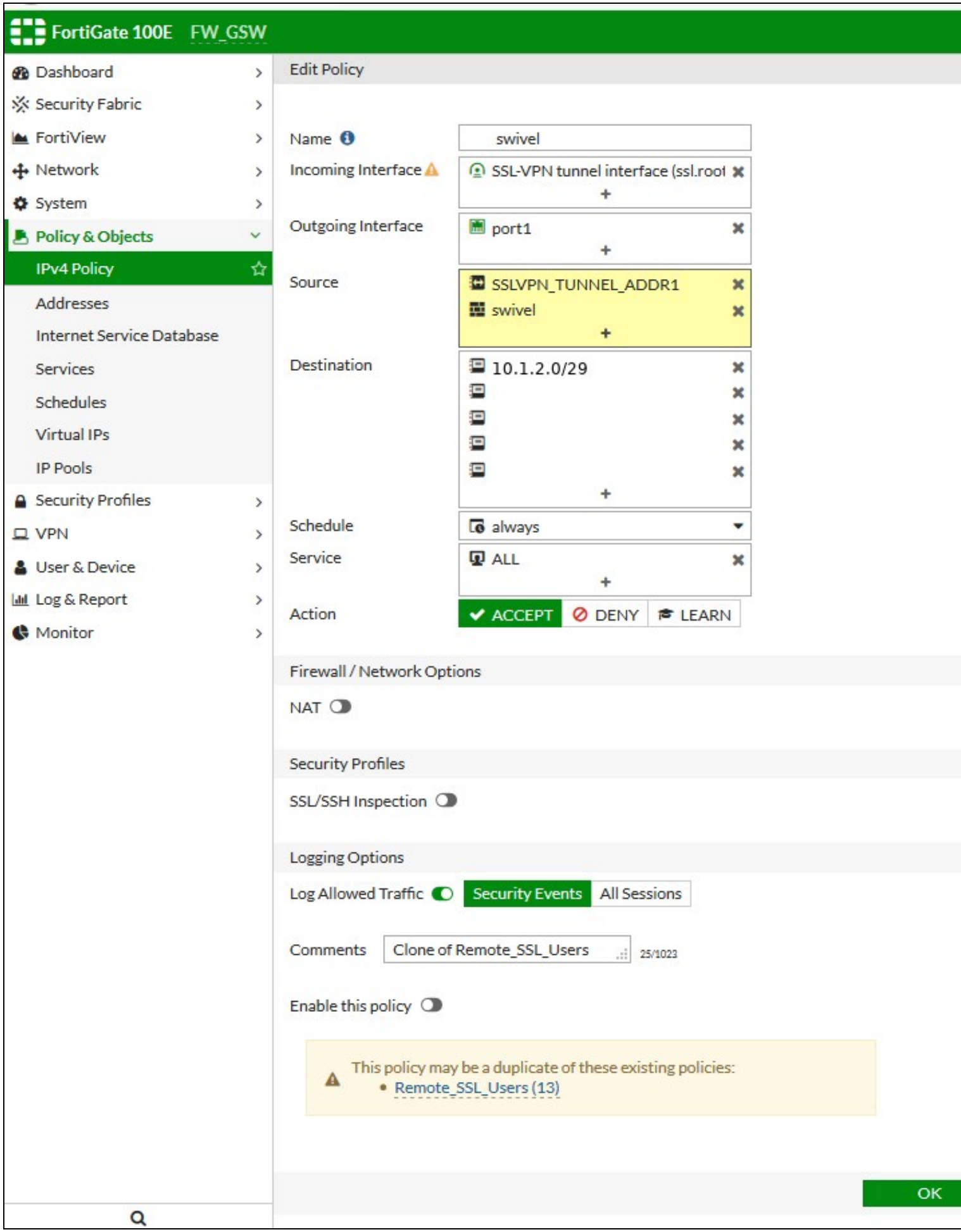
For further information regarding Fortinet FortiOS 6: https://docs.fortinet.com/uploaded/files/4328/fortios-v6.0.0-release-notes.pdf



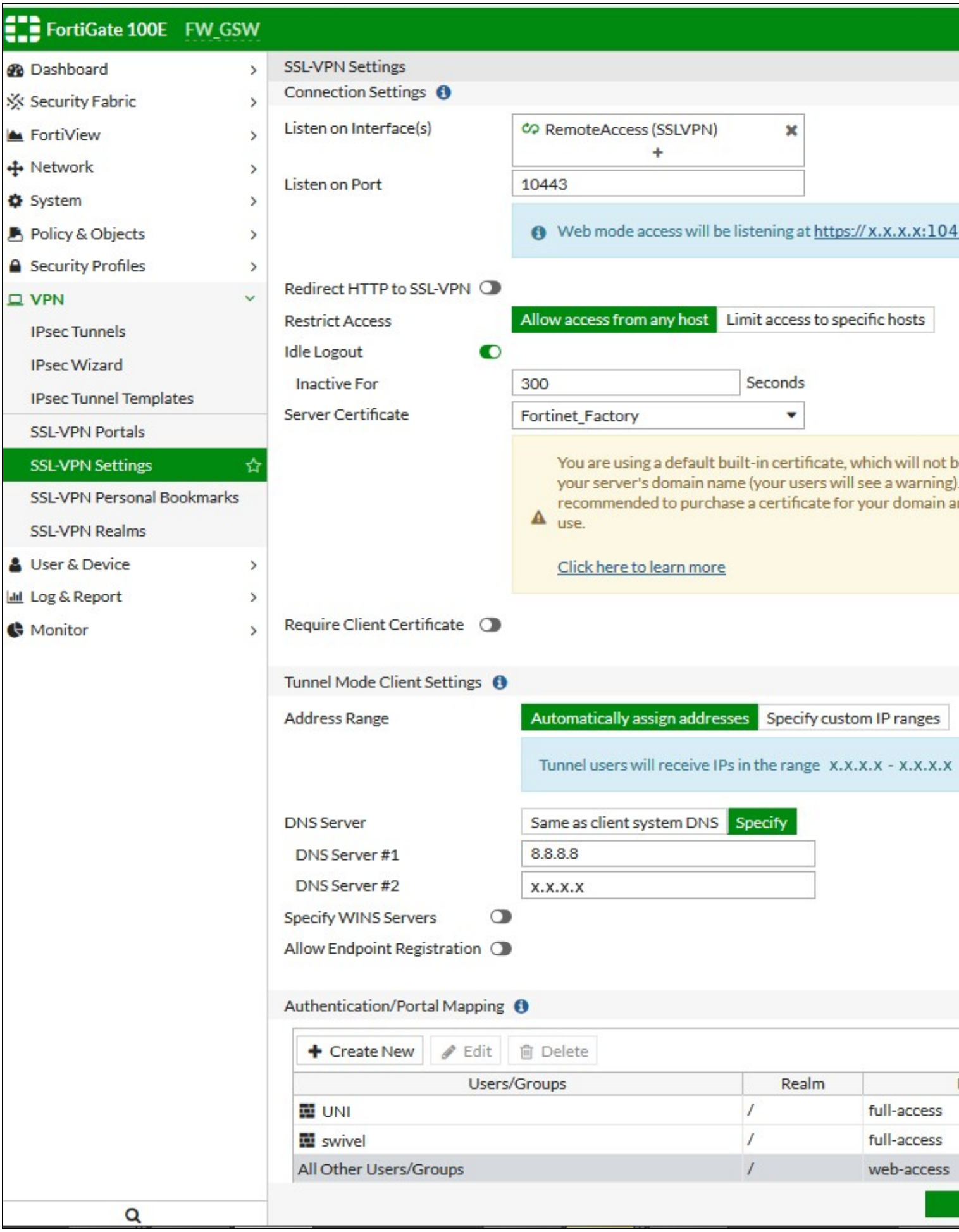
Select Radius Servers, create a Swivel Radius Server to bind to the the Appliance and test the connection. After create a user group for Swivel.



Edit Policy and fill all the entries. Destination might have more entries for different network and sub nets ranges.


FortiGate 100E FW_GSW
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
IPv4 Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Security Profiles
VPN
User & Device
Log & Report
Monitor
Edit Policy
Name
swivel
Incoming Interface
SSL-VPN tunnel interface (ssl.root
Outgoing Interface
port1
Source
SSLVPN_TUNNEL_ADDR1
swivel
Destination
10.1.2.0/29
Schedule
always
Service
ALL
Action
ACCEPT
DENY
LEARN
Firewall / Network Options
NAT
Security Profiles
SSL/SSH Inspection
Logging Options
Log Allowed Traffic
Security Events
All Sessions
Comments
Clone of Remote_SSL_Users
25/1023
Enable this policy
This policy may be a duplicate of these existing policies:
Remote_SSL_Users (13)
OK

Go to SSL VPN settings and check the settings. Default for listening will be port 10443. The DNS #2 can also have a resolution DNS specific for the customer's environment.


FortiGate 100E FW_GSW
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Templates
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Personal Bookmarks
SSL-VPN Realms
User & Device
Log & Report
Monitor
SSL-VPN Settings
Connection Settings
Listen on Interface(s)
RemoteAccess (SSLVPN)
Listen on Port
10443
Web mode access will be listening at https://x.x.x.x:104
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Server Certificate
Fortinet_Factory
You are using a default built-in certificate, which will not b
your server's domain name (your users will see a warning).
recommended to purchase a certificate for your domain a
use.
Click here to learn more
Require Client Certificate
Tunnel Mode Client Settings
Address Range
Automatically assign addresses
Specify custom IP ranges
Tunnel users will receive IPs in the range x.x.x.x - x.x.x.x
DNS Server
Same as client system DNS
Specify
DNS Server #1
8.8.8.8
DNS Server #2
x.x.x.x
Specify WINS Servers
Allow Endpoint Registration
Authentication/Portal Mapping
Create New
Edit
Delete
Users/Groups
Realm
UNI
/
full-access
swivel
/
full-access
All Other Users/Groups
/
web-access

Test the RADIUS authentication

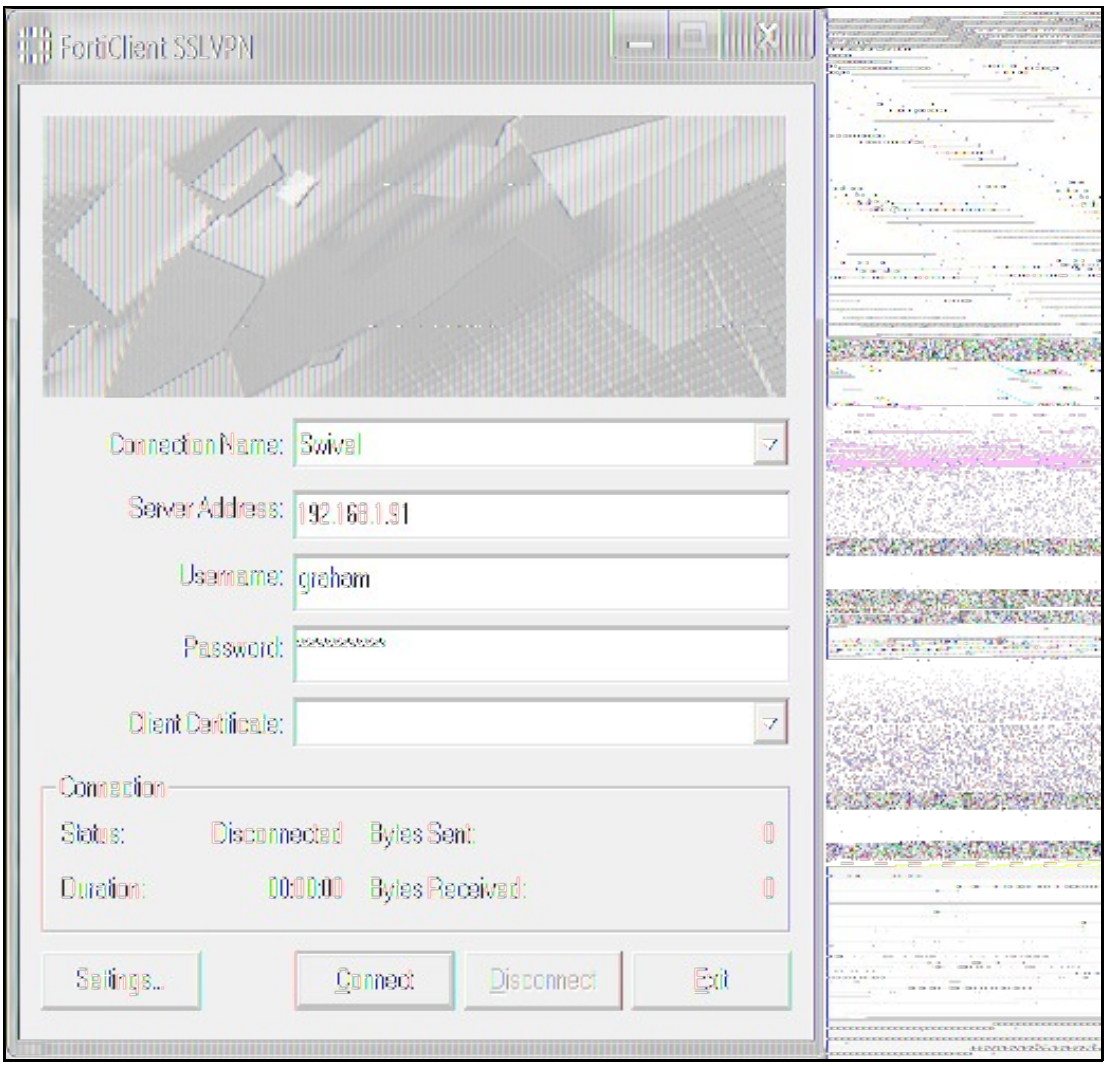
At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select User Administration and the required user then View Strings, and select an appropriate authentication string or OTC for the user. At the SSL VPN login enter the required OTC. Check the Swivel logs for a RADIUS success or rejected message. If no RADIUS message is seen, check that the Swivel RADIUS server is started and that the correct ports are being used.

Additional Configuration Options

Swivel can also check a password in addition to the One Time Code using Check Password with repository, see Password How to Guide

Forticlient

The above authentication integration will also work with the Fortinet Fortigate Fortclient for Client VPN access.



Login Page Customisation

The above configuration will allow authentication to be made by SMS, Mobile App, Hardware Token, and the Swivel Taskbar utility. To allow single channel authentication such as TURing or Pinpad, or images for other forms of authentication such the the security string index, then the login page can be modified. It may also be possible to modify other pages such as the Login Challenge Page.

On the Fortigate Administration console select System/Config/Replacement Messages, then click on SSL VPN to reveal the SSL VPN login message, then click on the edit icon. Paste in the required login page modifications.

Note Single channel images usually require a NAT to be used to the Swivel server.

Modify the script to use the Swivel server details:

```
//URL of radiusTuring page on the PINsafe server....
var sUrl="https://192.168.1.3:8443/proxy/SCImage?username=";
```

For a Swivel appliance the following should be used with the Swivel server IP/DNS name for the NAT entry:

var sUrl="https://192.168.1.3:8443/proxy/SCImage?username=";

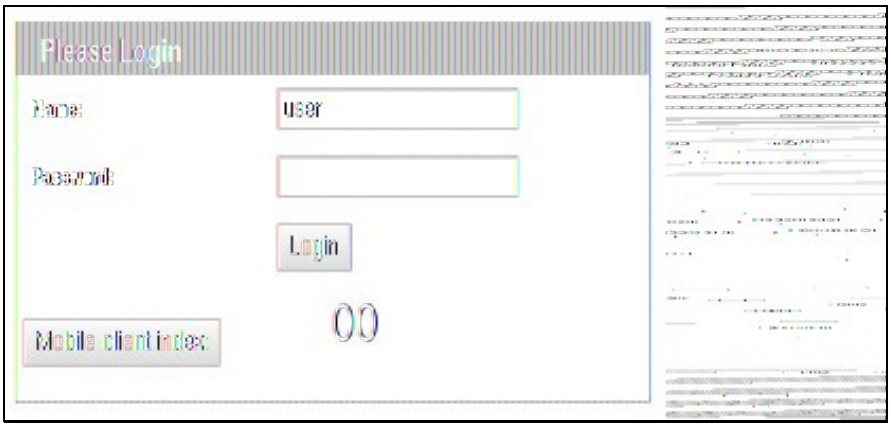
For a software only install see Software Only Installation

Testing

Browse to the VPN login page and test a Swivel authentication.

Example TURing login page

Example security string index login for Mobile or for SMS



Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

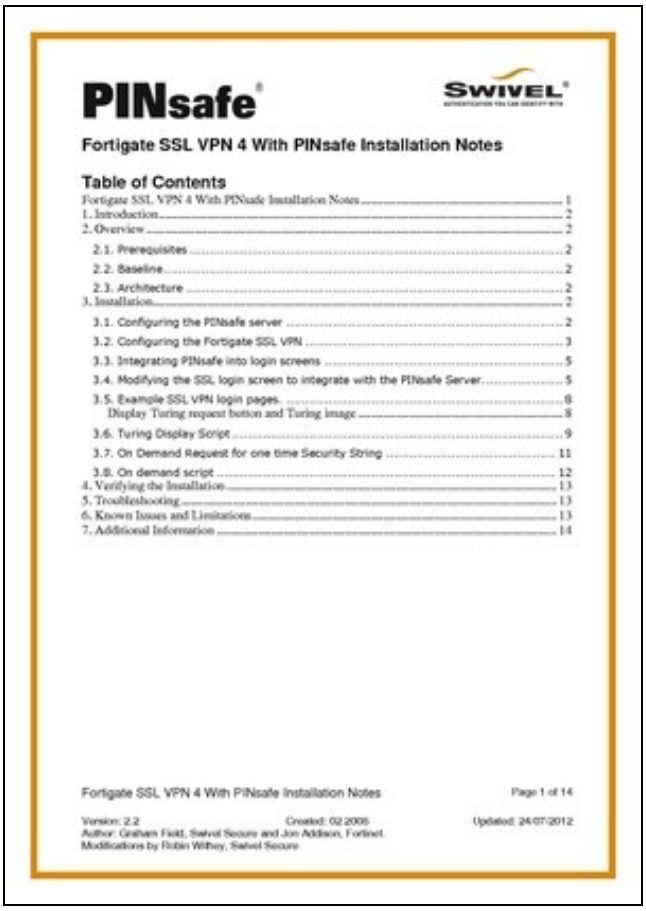
Login page modifications absent

This can be caused if the script has been altered with line feeds inserted in a text editor from wrap around text. View the login page source and see if it contains the page modifications, and are not being displayed correctly.

Known Issues and Limitations

None

Additional Information



PINsafe®

SWIVEL®

Fortigate SSL VPN 4 With PINsafe Installation Notes

Table of Contents

Fortigate SSL VPN 4 With PINsafe Installation Notes 1
1. Introduction 2
2. Overview 2
2.1. Prerequisites 2
2.2. Baseline 2
2.3. Architecture 2
3. Installation 2
3.1. Configuring the PINsafe server 2
3.2. Configuring the Fortigate SSL VPN 3
3.3. Integrating PINsafe into login screens 5
3.4. Modifying the SSL login screen to integrate with the PINsafe Server 5
3.5. Example SSL VPN login pages 8
Display Turing request button and Turing image 8
3.6. Turing Display Script 9
3.7. On Demand Request for one time Security String 11
3.8. On demand script 12
4. Verifying the Installation 13
5. Troubleshooting 13
6. Known Issues and Limitations 13
7. Additional Information 14

Version: 2.2 Created: 02.2008 Updated: 24.07.2012

Author: Graham Field, Swivel Secure and Jon Addison, Fortinet.
Modifications by Robin Withey, Swivel Secure

For assistance in Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com