Table of Contents

1 Category:Apache **1**

2 Category:API **2**

3 AppGate Security Server **3**

4 Introduction **4**

5 Prerequisites **5**
5.1 Login Page customisation prerequisites 5

6 Baseline **6**

7 Architecture **7**

8 Swivel Configuration **8**
8.1 Configuring the RADIUS server 8
8.2 Setting up Swivel Dual Channel Transports 8

9 AppGate Security Server Configuration **9**
9.1 Adding a Swivel RADIUS server 9
9.2 Test the RADIUS authentication 11
9.3 Optional: Login Page Customisation 11

10 Testing **13**

11 Additional Configuration Options **14**

12 Troubleshooting **15**

13 Known Issues and Limitations **16**

14 Additional Information **17**

15 Array Networks SPX Integration **18**

16 Introduction **19**

17 Additional Contributors **20**

18 Prerequisites **21**

19 Baseline **22**

20 Architecture **23**

21 Installation **24**

22 Swivel Configuration **25**
22.1 Configuring the RADIUS server 25
22.2 Enabling Session creation with username 25
22.3 Configure Password 25

23 Configure the custom login page **26**
23.1 Editing the Login Page 26
23.2 Copy the login page files 26
23.3 Create a Failed Login Page 26

24 Configure the Array Networks SPX **27**
24.1 Configure RADIUS authentication 27
24.2 Link custom page to URL for login 30
24.3 Link custom page to URL for failed login 32
24.4 Link custom page to URL for generic login error 32
24.5 Configure URL Policy 32

25 Verifying the Installation **34**

26 Troubleshooting **36**

27 Known Issues and Limitations **37**

28 Additional Information **38**

29 Arx Co-Sign Integration **39**

30 Aventail Integration **40**

31 Introduction **41**

32 Prerequisites **42**

33 Baseline **43**

Table of Contents

34 Architecture **44**

35 Swivel Configuration **45**
35.1 Configuring the RADIUS server 45
35.2 Enabling Session creation with username 45
35.3 Setting up Swivel Dual Channel Transports 45

36 SonicWall Aventail Integration **46**
36.1 Configuring The Sonicwall Aventail for RADIUS Authentication 46
36.2 Test the RADIUS authentication 47
36.3 Modifying the Aventail Sign-In Page for Turing 48
36.4 Creating A Custom Authentication Request Page 50

37 Verifying the Installation **52**

38 Known Issues and Limitations **53**

39 Configuration Options **54**
39.1 Turing Image Size 54
39.2 Security String Index 54
39.3 TURing and SMS 55
39.4 Manual Turing Display 55
39.5 Automated Turing Display 55

40 Troubleshooting **56**

41 Additional Information **57**

42 Barracuda SSL VPN Integration **58**

43 Introduction **59**

44 Prerequisites **60**

45 Baseline **61**

46 Architecture **62**

47 Swivel Configuration **63**
47.1 Configuring the RADIUS server 63
47.2 Enabling Session creation with username 63

48 Barracuda SSL VPN Configuration **64**
48.1 Create an authentication scheme 64
48.2 Barracuda RADIUS Configuration 66
48.3 Test the RADIUS authentication 69
48.4 Additional Configuration options 69

49 Testing **71**

50 Troubleshooting **73**

51 Known Issues and Limitations **74**

52 Additional Information **75**

53 Bluecoat ProxySG Integration **76**

54 Bomgar **77**

55 Introduction **78**

56 Prerequisites **79**

57 Baseline **80**

58 Architecture **81**

59 Swivel Configuration **82**
59.1 Configuring the RADIUS server 82
59.2 Configuring Two Stage Authentication 82
59.3 Setting up Swivel Dual Channel Transports 82

60 Bomgar Configuration **83**
60.1 Test the RADIUS authentication 83
60.2 Optional 83

61 Testing **84**

62 Additional Configuration Options **85**

63 Troubleshooting **86**

Table of Contents

64 Known Issues and Limitations **87**

65 Additional Information **88**

66 Category:CheckPoint **89**

67 Category:Cisco **90**

68 Category:Citrix **91**

69 Cyberoam UTM SSL VPN **92**

70 Introduction **93**
- 70.1 Prerequisites 93
- 70.2 Baseline 93
- 70.3 Architecture 93

71 Swivel Configuration **94**
- 71.1 Configuring the RADIUS server 94
- 71.2 PINsafe Dual Channel Authentication 94

72 Cyberoam CR25i Configuration **95**
- 72.1 Define a RADIUS server on the Cyberoam 95
- 72.2 Cyberoam SSL VPN Authentication Methods 96
- 72.3 Test the RADIUS authentication 97
- 72.4 Additional Cyberoam Configuration Options 97
- 72.5 Testing 98
- 72.6 Troubleshooting 99
- 72.7 Known Issues and Limitations 99
- 72.8 Additional Information 99

73 Ericom PowerTerm WebConnect **100**

74 Introduction **101**

75 Prerequisites **102**

76 Baseline **103**

77 Architecture **104**

78 Installation **105**
- 78.1 Swivel Integration Configuration 105
- 78.2 Ericom PowerTerm WebConnect Integration 106
- 78.3 Additional Installation Options 107

79 Verifying the Installation **108**

80 Uninstalling the Swivel Integration **110**

81 Troubleshooting **111**

82 Known Issues and Limitations **112**

83 Additional Information **113**

84 Category:F5 ..... **114**

85 Fortinet Fortigate Integration **115**

86 Introduction **116**

87 Prerequisites **117**

88 Baseline **118**

89 Architecture **119**

90 Swivel Configuration **120**
- 90.1 Configuring the RADIUS server 120
- 90.2 Enabling Session creation with username 120

91 Fortinet Fortigate Configuration **121**
- 91.1 Fortinet FortigateVersion 3.x Integration guide 121
- 91.2 Fortinet Fortigate Version 4.x Integration guide 121
- 91.3 Fortinet Fortigate Version 6.x Integration guide 123
- 91.4 Test the RADIUS authentication 129

92 Additional Configuration Options **130**
- 92.1 Forticlient 130
- 92.2 Login Page Customisation 130

93 Testing **131**

Table of Contents

94 Troubleshooting 132

95 Known Issues and Limitations 133

96 Additional Information 134

97 Category:Google 135

98 HOB Remote Desktop VPN 136

99 Introduction 137

100 Prerequisites 138

101 Baseline 139

102 Architecture 140

103 Swivel Configuration 141
- 103.1 Configuring the RADIUS server 141
- 103.2 Enabling Session creation with username 141
- 103.3 Setting up Swivel Dual Channel Transports 141

104 HOB RD VPN WebSecureProxy Integration 142
- 104.1 Create a RADIUS Server 142
- 104.2 Assign the PINsafe RADIUS server to a Connection 143
- 104.3 Additional Installation Options 144

105 Verifying the Installation 146

106 Uninstalling the PINsafe Integration 149

107 Troubleshooting 150

108 Known Issues and Limitations 151

109 Additional Information 152

110 Category:Joomla 153

111 Category:Juniper 154

112 Category:Mcafee 155

113 Meraki 156
- 113.1 Overview 156
- 113.2 Meraki Configuration 156
- 113.3 Custom Login Page 160

114 Category:Microsoft 161

115 Category:Mobile 162

116 Netgear 163

117 Introduction 164

118 Baseline 165

119 PINsafe configuration 166
- 119.1 Configuring the RADIUS server 166

120 Netgear Configuration 168
- 120.1 Configuring the Domain 168
- 120.2 Single Channel TURing Integration 168
- 120.3 Additional Configuration Options 170
- 120.4 Known issues 170

121 Netilla Integration 171

122 Nortel VPN Integration 172

123 Introduction 173

124 RADIUS Integration 174

125 TURING Integration 176

126 Notes 178

127 Category:Open ERP 179

128 OpenVPN integration 180
- 128.1 Introduction 180
- 128.2 Prerequisites 180

Table of Contents

128 OpenVPN integration
- 128.3 Baseline ... 180
- 128.4 Integration ... 180

129 Category:Oracle ... 184

130 Palo Alto Networks Integration ... 185
- 130.1 Introduction ... 185
- 130.2 Prerequisites ... 185
- 130.3 Baseline ... 185
- 130.4 Architecture ... 185
- 130.5 Swivel Configuration ... 185
- 130.6 Palo Alto Networks Configuration ... 187
- 130.7 Additional Configuration Options ... 191
- 130.8 Testing ... 193
- 130.9 Troubleshooting ... 193
- 130.10 Known Issues and Limitations ... 193
- 130.11 Additional Information ... 193

131 Category:SAML ... 194

132 Sawmill Integration ... 195
- 132.1 Sawmill Integration with Swivel ... 195
- 132.2 Prerequisites ... 195
- 132.3 Baseline ... 195
- 132.4 Architecture ... 195
- 132.5 Swivel Configuration ... 195
- 132.6 Sawmill Configuration ... 195
- 132.7 Process Data and View Reports ... 197
- 132.8 Verifying the Installation ... 198
- 132.9 Troubleshooting ... 198
- 132.10 Known Issues and Limitations ... 198
- 132.11 Additional Information ... 198

133 Category:SMS Provider ... 199

134 Category:Sonicwall ... 200

135 Splunk ... 201
- 135.1 Introduction ... 201
- 135.2 Requirements ... 201
- 135.3 Installation ... 201
- 135.4 Splunk Syslog Configuration ... 202
- 135.5 Splunk XML Log File Configuration ... 202
- 135.6 Verifying the Installation ... 203
- 135.7 Additional Information ... 204

136 Symantec Secure Web Gateway Integration ... 205

137 Category:Taskbar ... 206

138 VMware View (Horizon) ... 207
- 138.1 Introduction ... 207
- 138.2 Credits ... 207
- 138.3 Prerequisites ... 207
- 138.4 Baseline ... 207
- 138.5 Architecture ... 207
- 138.6 Swivel Configuration ... 207
- 138.7 VMware View Configuration ... 209
- 138.8 Additional Configuration Options ... 214
- 138.9 Testing ... 214
- 138.10 Troubleshooting ... 215
- 138.11 Known Issues and Limitations ... 215
- 138.12 Additional Information ... 215

139 WatchGuard Firebox ... 216

140 Overview ... 217

1 Category:Apache

2 Category:API

3 AppGate Security Server

4 Introduction

This document describes steps to configure a AppGate Security Server from Cryptozone with Swivel as the authentication server. Swivel can provide Two Factor authentication with SMS, Token, Mobile Phone Client and strong Single Channel Authentication TURing, Pinpad or in the Taskbar using RADIUS.

Swivel integration is made using RADIUS authentication protocol with an option to configure the login page.

5 Prerequisites

AppGate Security Server Appliance

AppGate documentation

Swivel 3.x, 3.5 or higher for RADIUS groups

NAT for Single channel access

5.1 Login Page customisation prerequisites

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, and security string number, **for external access this is usually through a NAT**.

6 Baseline

AppGate Security Server Appliance

Swivel 3.8

7 Architecture

The AppGate Security Server makes authentication requests against the Swivel server by RADIUS.

The client makes TURing requests against the Swivel server using HTTP/HTTPS

8 Swivel Configuration

8.1 Configuring the RADIUS server

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

8.1.1 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.

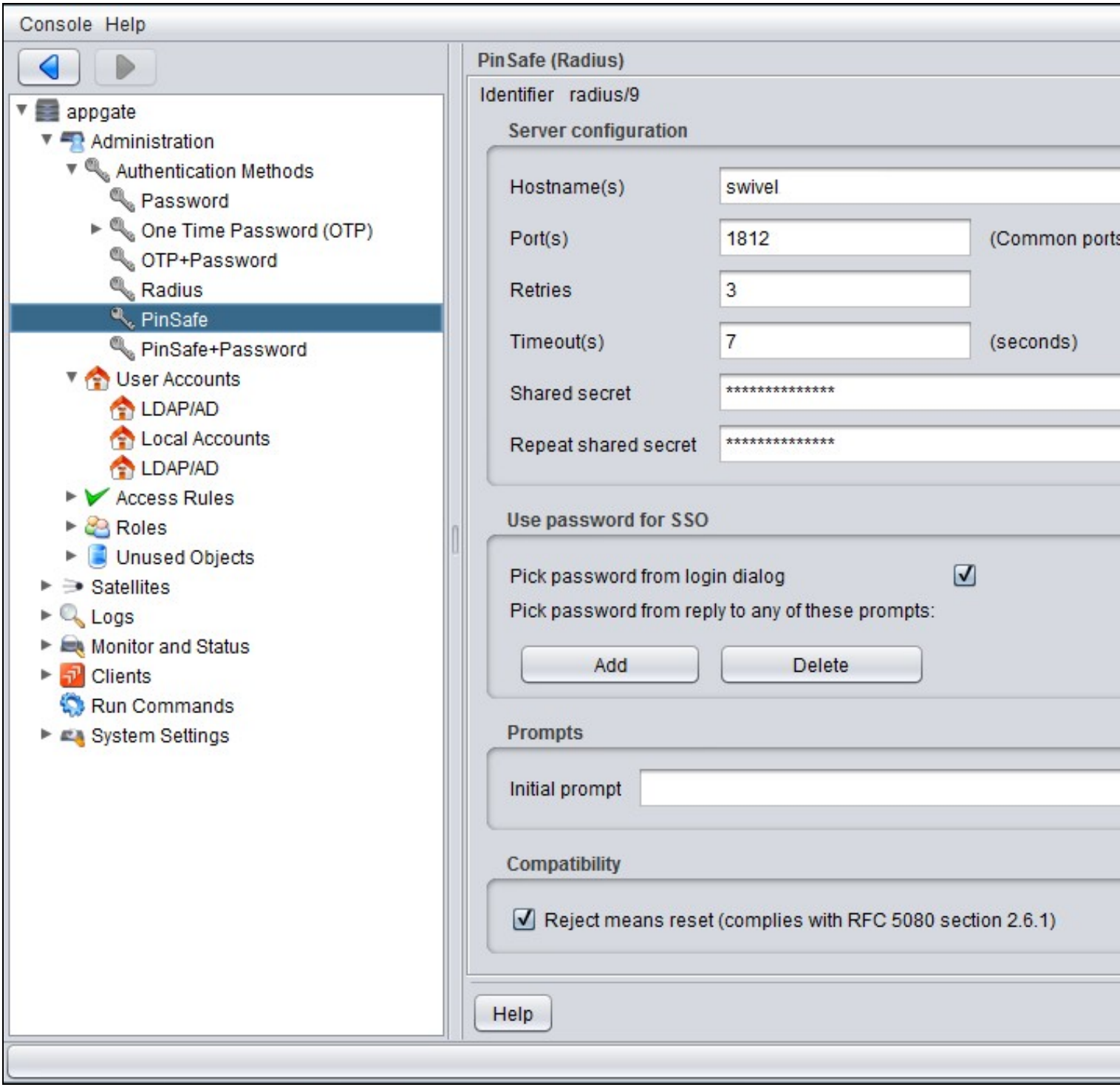
8.2 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

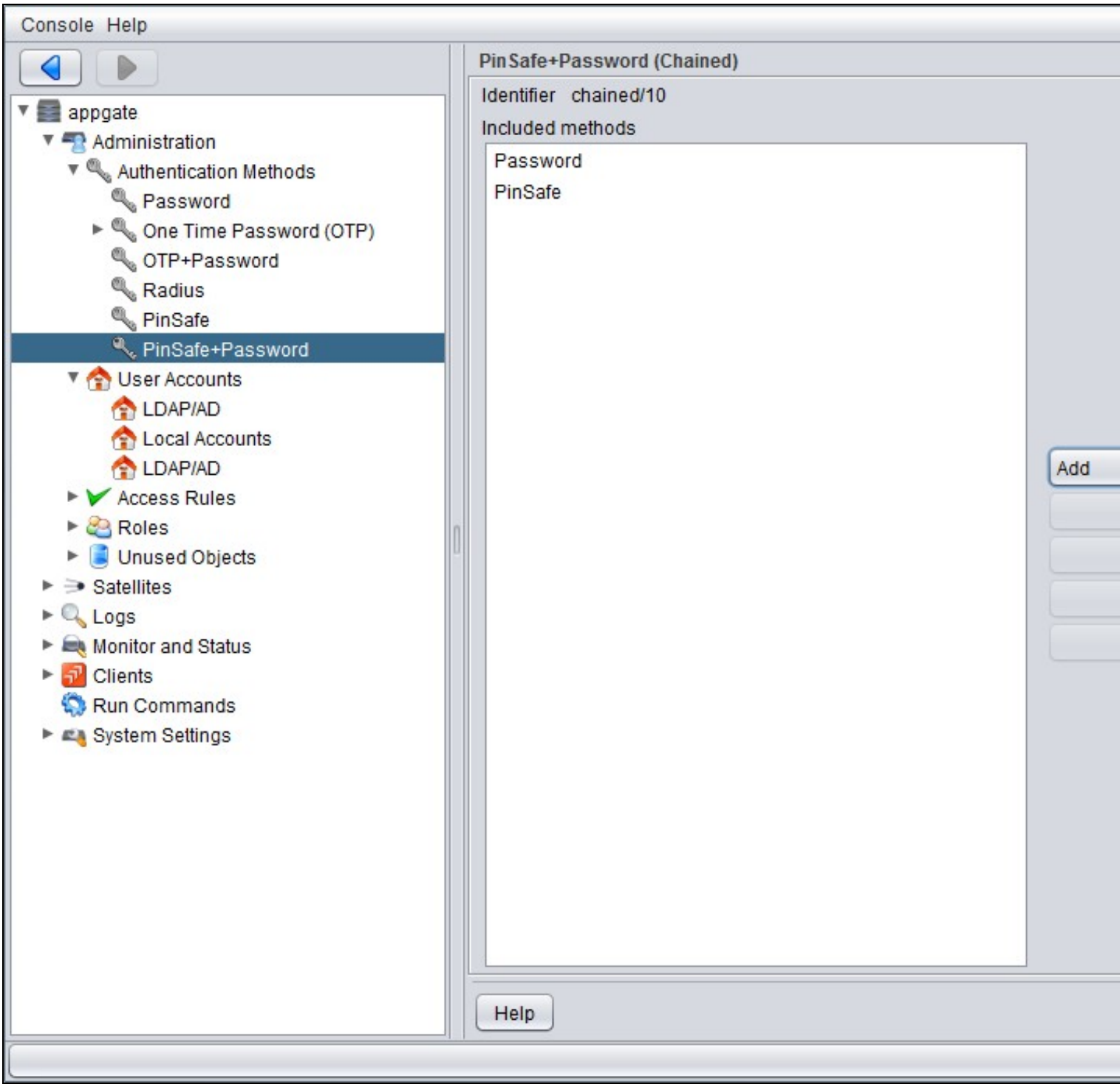
9 AppGate Security Server Configuration

9.1 Adding a Swivel RADIUS server

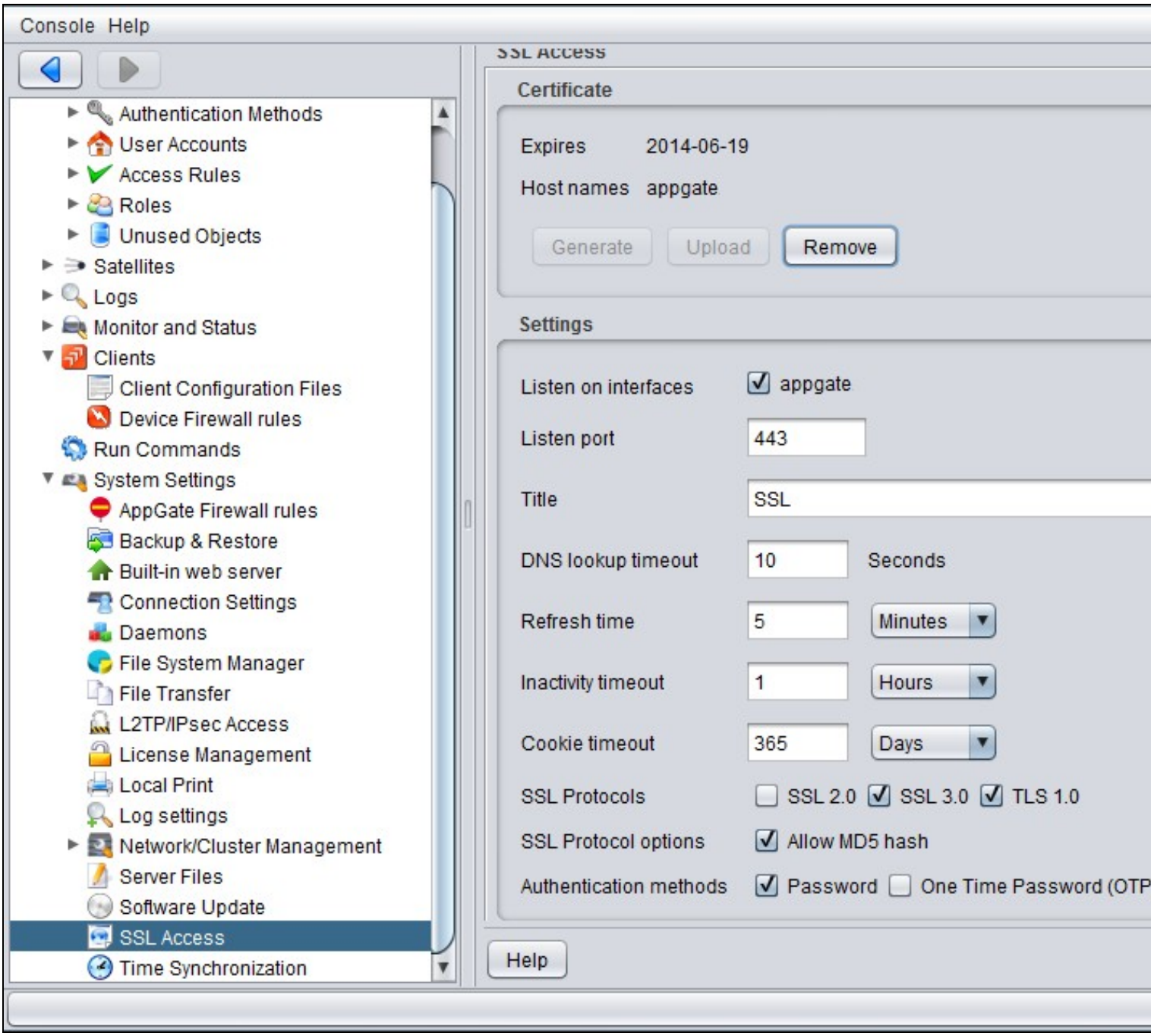
On the AppGate Security Server select Administration/Authentication Methods then Add Authentication Method.



It is recommended to use a password in combination with the OTC and this can be done by using a chained password.



On the AppGate Security Server select Administration/System Settings/SSL Access then select the required Authentication Methods allowed.



9.2 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.

9.3 Optional: Login Page Customisation

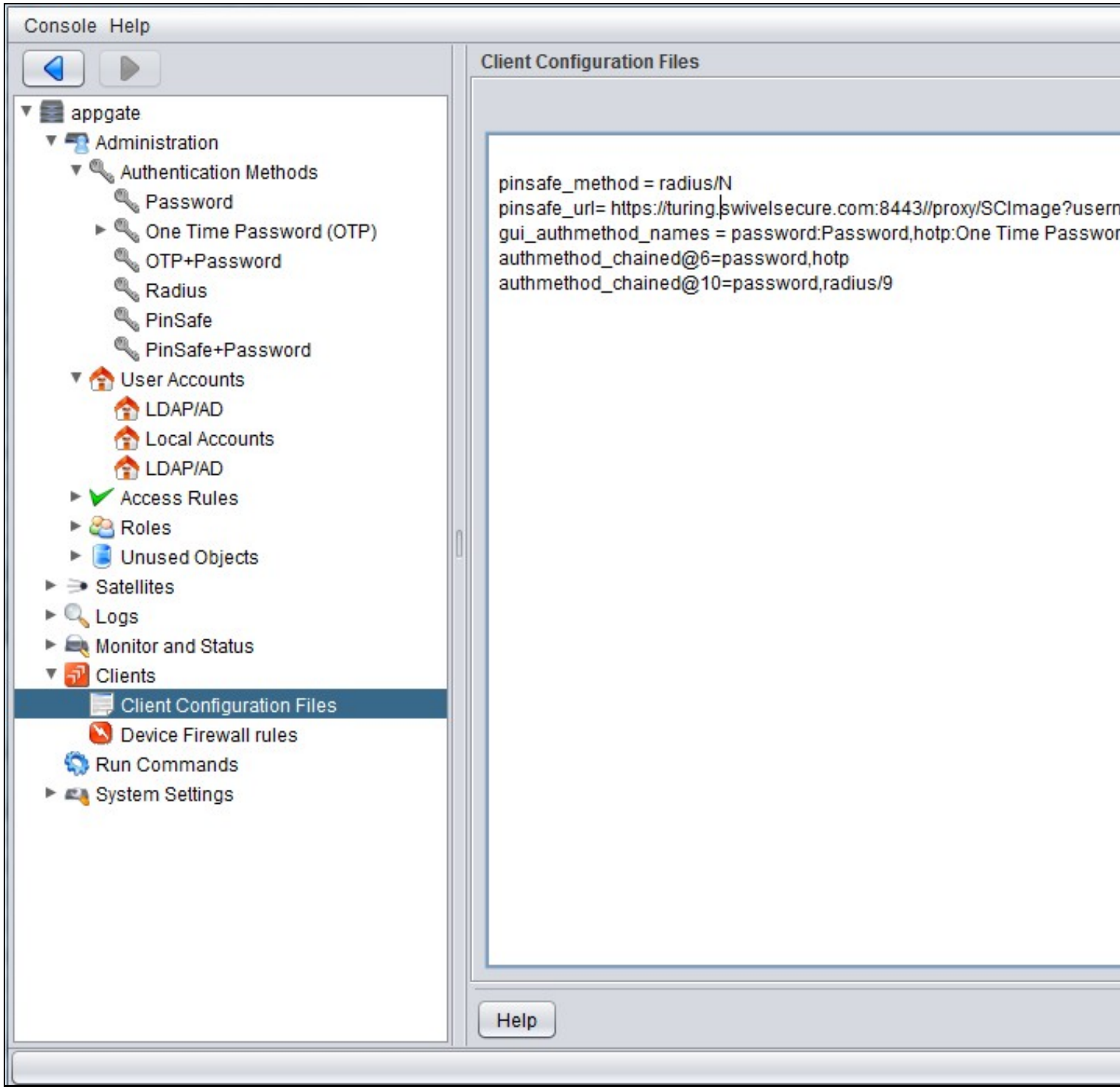
On the AppGate Security Server select Administration/User Accounts and for the required access account type ensure that RADIUS authentication is selecetd under the Authentication tab.

On the AppGate Security Server select Administration/Clients then Client Configuration Files and add the following lines:

pinsafe_method = radius/N

pinsafe_URL = http://server:port//pinsafe/SCImage?username=%u

where server is the Swivel sever public NAT and port the port to the Swivel server, usually 443 for a Swivel appliance. For further informationn refer to the AppGate Security Server documentation under RADIUS/Pinsafe.



10 Testing

11 Additional Configuration Options

12 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

13 Known Issues and Limitations

None

14 Additional Information

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

15 Array Networks SPX Integration

16 Introduction

This configuration document outlines how to integrate Swivel with the Array Networks SPX using password authentication in addition to the Swivel authentication.

17 Additional Contributors

Swivel Secure would like to thank Wender Putters from Connect Data Solutions

18 Prerequisites

Array Network SPX 8.2, 8.3, 8.4

Swivel 3.x

If the TURing is required to be used a NAT is required to the Swivel virtual or hardware appliance

Website to host custom login page, this can be the Swivel virtual or hardware appliance.

Custom login page, this can be downloaded from here: here

19 Baseline

Array Networks SPX 8.2.2.0 and also 8.4.4.2 Build 9

Swivel 3.5 and Swivel 3.7

20 Architecture

The Array Networks SPX makes authentication requests against the Swivel virtual or hardware appliance by RADIUS. The login page is redirected from the Array Networks SPX onto another web server. The Swivel virtual or hardware appliance can be used to host this page. The hosted page must be accessible from the internet.

If the AD password is required to be used then these are added together into the RADIUS request, and Swivel has to have the *require password* and *check password with repository set to yes*. Remember that in Swivel 3.7 and earlier this is a global setting. In Swivel 3.8 it is possible to set password checks by NAS devic rather than being a global setting.

21 Installation

22 Swivel Configuration

22.1 Configuring the RADIUS server

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

22.2 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.

22.3 Configure Password

Swivel 3.7 and earlier

If the AD Password is required to be used, on the Swivel Administration Console select Policy/Password, enable *Require Password* and *check password with repository*

Swivel 3.8 and later

If the AD Password is required to be used, on the Swivel Administration Console select RADIUS NAS, enable *check password with repository*

23 Configure the custom login page

23.1 Editing the Login Page

Edit the file login.html with the required values

The externally accessible IP address of the Swivel virtual or hardware appliance needs to be set for the following lines:

_AN_base_host = "http://192.168.100.100:8080";

_AN_base_path = "http://192.168.100.100:8080/login";

sUrl = "https://192.168.100.100:8443/proxy/SCImage?username=";

Change the IP address for that of the public URL. For a Swivel virtual or hardware appliance the sURL also needs to be changed as follows:

For a Virtual or hardware appliance:

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

For a software only install see Software Only Installation

23.2 Copy the login page files

The login page can be hosted on a web server. Note that this page needs to be accessible from the internet by the client.

To use Swivel as a to host the login page:

Copy login.html to one of the following locations:

Swivel Virtual or hardware Appliance: create the folder ROOT in /usr/local/tomcat/webapps2 using a program such as WinSCP, see the WinSCP How To Guide, then ensure that the ownership/group of the folder and file are *swivel* and permissions for the ROOT folder are rwxrwxr-x. Copy in the file login.html and ensure the permissions are rw-rw-r--, and it is owned by the swivel user.

Software only install: <path to Tomcat>/webapps/ROOT

Test that the web page is accessible

Virtual or hardware appliance: http://IP of Swivel server:8443/login.html

For a software only install see Software Only Installation

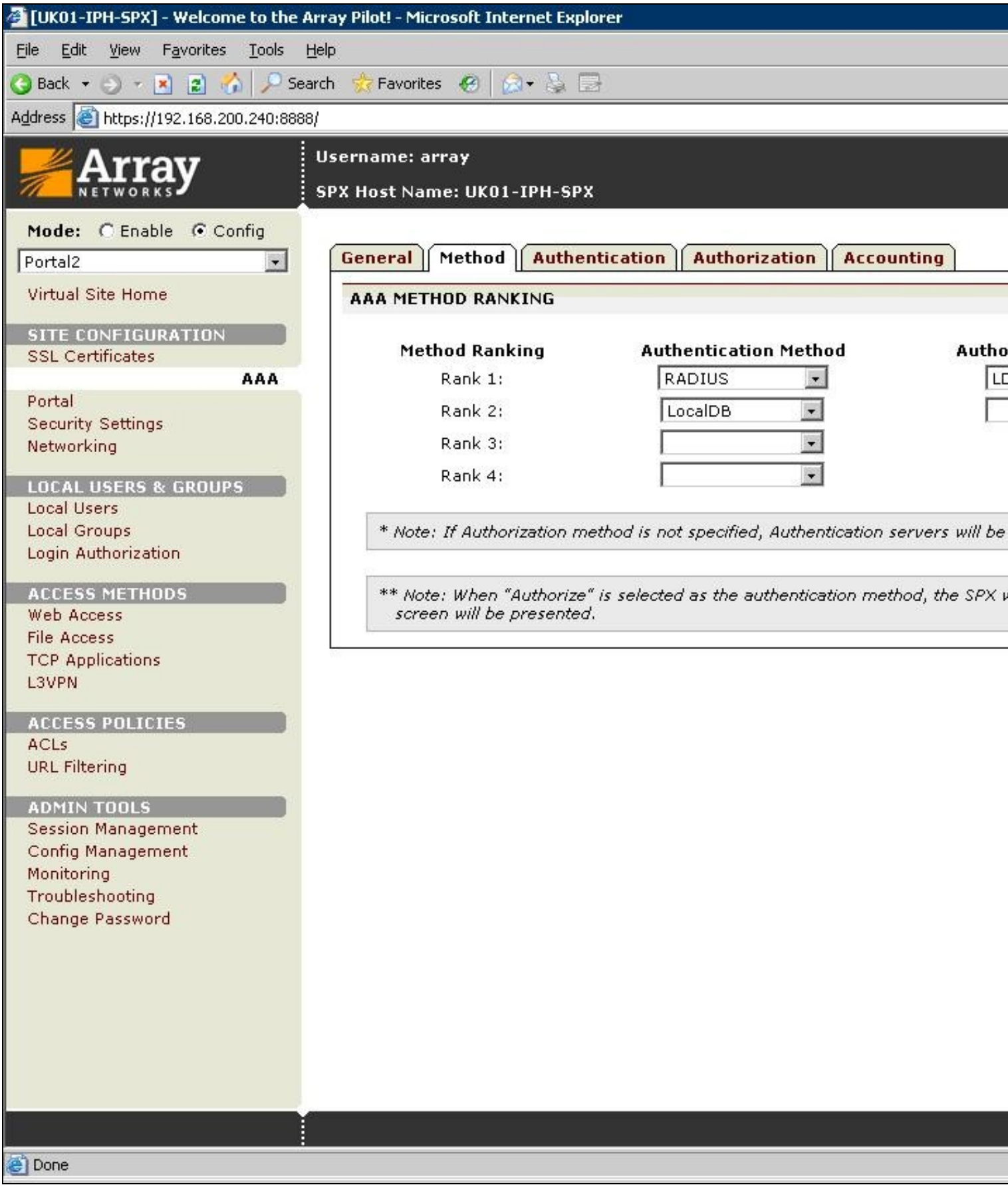
23.3 Create a Failed Login Page

When a login fails, the page redirects, to ensure that this is a Swivel login page either redirect the login failure back to the Swivel login.html, or make a copy of that file and edit it as required, such as to indicate that a login has failed.

24 Configure the Array Networks SPX

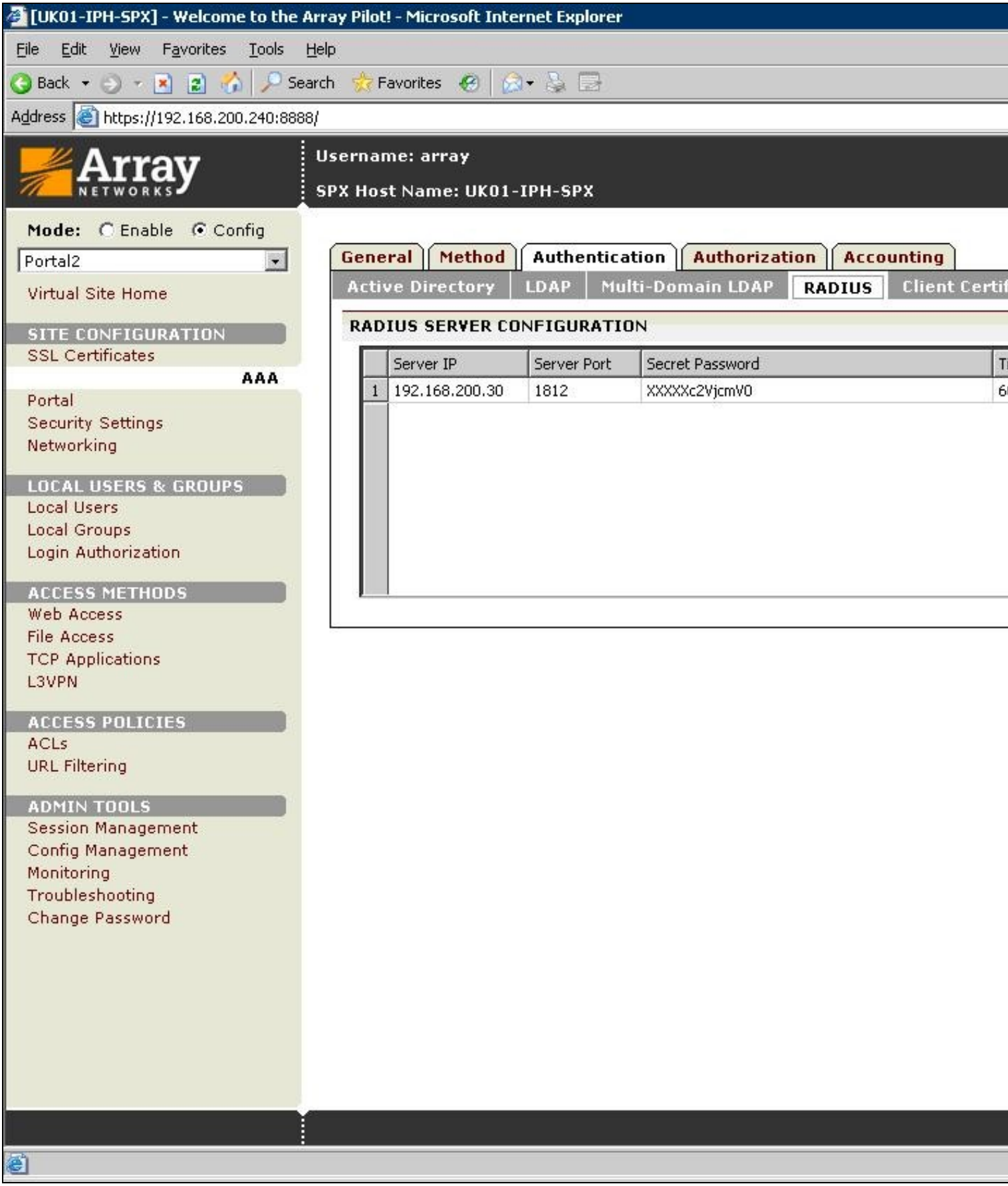
24.1 Configure RADIUS authentication

On the Array Networks SPX Select under Site Configuration AAA, then method. Configure the RADIUS server on the authentication menu. Set the authentication method to RADIUS



On the Authentication tab, Swivel needs to be configured as the RADIUS server for the VPN, ensuring that the shared secret matches that set on the RADIUS->NAS screen on Swivel.

If you want to configure more RADIUS servers for failover, add more servers.


[UK01-IPH-SPX] - Welcome to the Array Pilot! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.200.240:8888/
Array NETWORKS
Username: array
SPX Host Name: UK01-IPH-SPX
Mode: Enable Config
Portal2
Virtual Site Home
SITE CONFIGURATION
SSL Certificates
AAA
Portal
Security Settings
Networking
LOCAL USERS & GROUPS
Local Users
Local Groups
Login Authorization
ACCESS METHODS
Web Access
File Access
TCP Applications
L3VPN
ACCESS POLICIES
ACLs
URL Filtering
ADMIN TOOLS
Session Management
Config Management
Monitoring
Troubleshooting
Change Password
General Method Authentication Authorization Accounting
Active Directory LDAP Multi-Domain LDAP RADIUS Client Certif
RADIUS SERVER CONFIGURATION
Server IP Server Port Secret Password
1 192.168.200.30 1812 XXXXXc2VjcmV0

24.2 Link custom page to URL for login

The custom log-in page created then needs to be associated with the url of the log-in page. On the Array Networks SPX Select under Site Configuration Portal then External pages, enter the path to the Swivel virtual or hardware appliance. Note that this page needs to be accessible from the internet by the client.

The required settings are:

URL: Full address of where the login page can be reached

Username: default: uname, the username attribute used in the login page

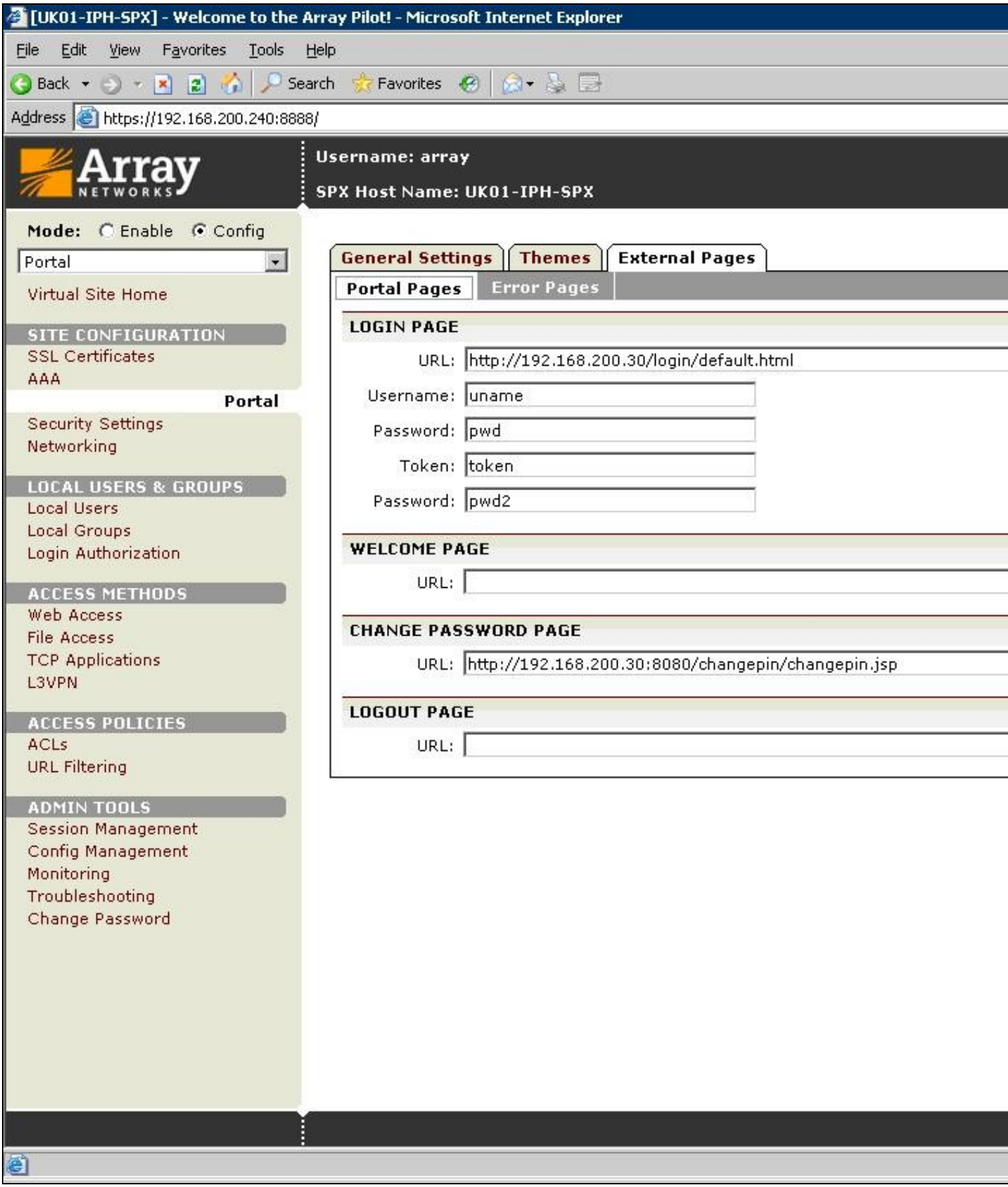
Password: default: pwd, the password attribute used in the login page

Token: default: token, the token attribute used in the login page

Password: default: pwd2, the secondary password attribute

Other options

Change Password Page Full address of the ChangePIN page


[UK01-IPH-SPX] - Welcome to the Array Pilot! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.200.240:8888/
Array NETWORKS
Username: array
SPX Host Name: UK01-IPH-SPX
Mode: Enable Config
Portal
Virtual Site Home
SITE CONFIGURATION
SSL Certificates
AAA
Portal
Security Settings
Networking
LOCAL USERS & GROUPS
Local Users
Local Groups
Login Authorization
ACCESS METHODS
Web Access
File Access
TCP Applications
L3VPN
ACCESS POLICIES
ACLs
URL Filtering
ADMIN TOOLS
Session Management
Config Management
Monitoring
Troubleshooting
Change Password
General Settings
Themes
External Pages
Portal Pages
Error Pages
LOGIN PAGE
URL: http://192.168.200.30/login/default.html
Username: uname
Password: pwd
Token: token
Password: pwd2
WELCOME PAGE
URL:
CHANGE PASSWORD PAGE
URL: http://192.168.200.30:8080/changepin/changepin.jsp
LOGOUT PAGE
URL:

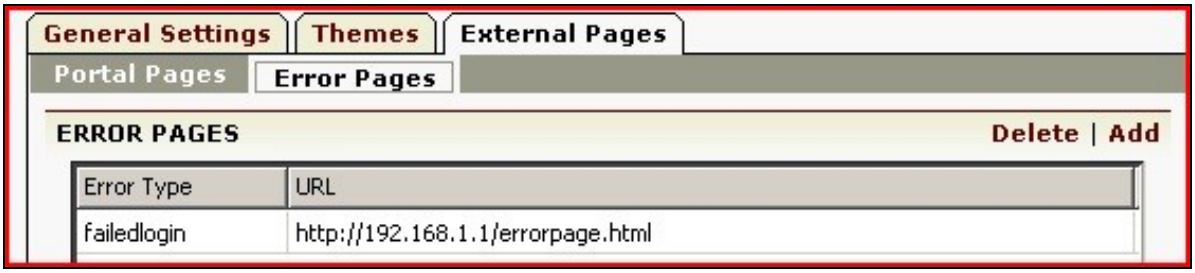
24.3 Link custom page to URL for failed login

The custom failed log-in page created then needs to be associated with the url of the log-in page. On the Array Networks SPX Select under Site Configuration Portal then External pages, select Error Pages, and for error type select failed login, enter either the path to the Swivel page or to a custom failed login page. Note that this page needs to be accessible from the internet by the client. Click save and the login page will now be listed.

Custom page for failed login:



The custom login page should be listed under Error Pages



24.4 Link custom page to URL for generic login error

It is also recommended to create another error page (as above) using the same custom login page URL (as above) but for a **generic login error**, which is a selectable Error Type. This prevents the default localhost login page of the Array being presented in the event of a generic login error.

24.5 Configure URL Policy

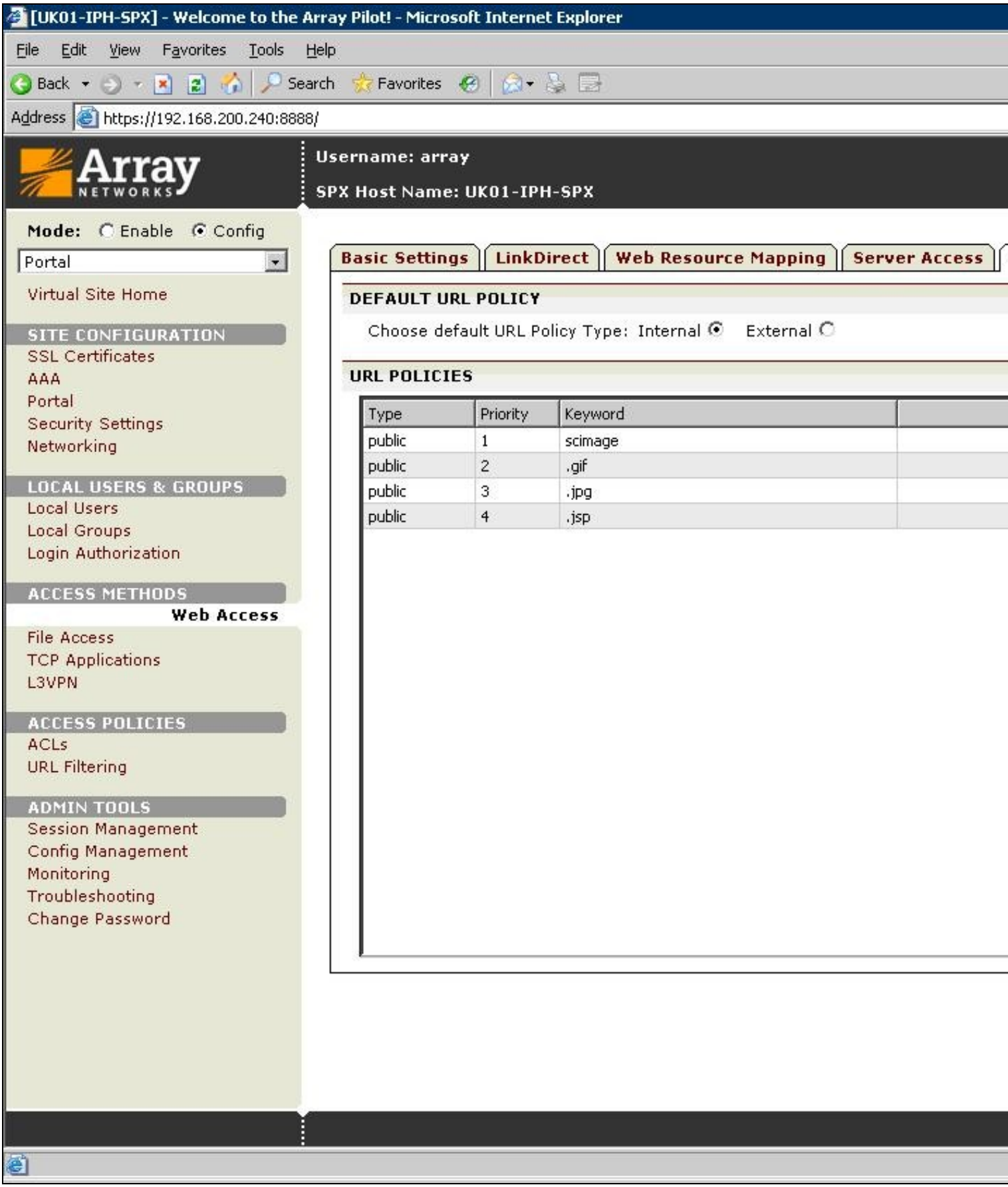
This page allows certain attributes to be used in the login page. On the Array Networks SPX Select under access methods/Web Access then URL Policies. Create the following policies:

Priority: 1 Type Public: keyword: SCImage

Priority: 2 Type Public: keyword: .gif

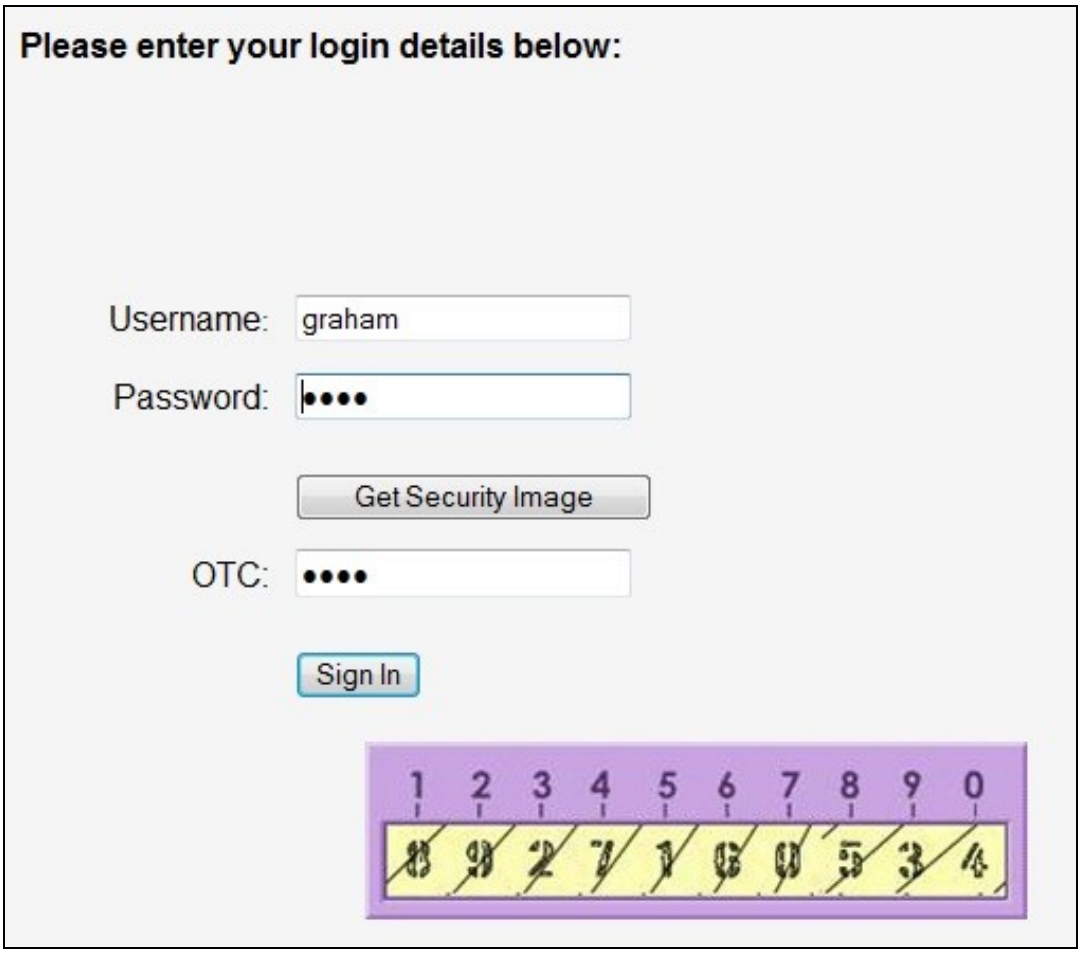
Priority: 3 Type Public: keyword: .jpg

Priority: 4 Type Public: keyword: .jsp


[UK01-IPH-SPX] - Welcome to the Array Pilot! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.200.240:8888/
Array NETWORKS
Username: array
SPX Host Name: UK01-IPH-SPX
Mode: Enable Config
Portal
Virtual Site Home
SITE CONFIGURATION
SSL Certificates
AAA
Portal
Security Settings
Networking
LOCAL USERS & GROUPS
Local Users
Local Groups
Login Authorization
ACCESS METHODS
Web Access
File Access
TCP Applications
L3VPN
ACCESS POLICIES
ACLs
URL Filtering
ADMIN TOOLS
Session Management
Config Management
Monitoring
Troubleshooting
Change Password
Basic Settings
LinkDirect
Web Resource Mapping
Server Access
DEFAULT URL POLICY
Choose default URL Policy Type: Internal External
URL POLICIES
Type Priority Keyword
public 1 scimage
public 2 .gif
public 3 .jpg
public 4 .jsp

25 Verifying the Installation

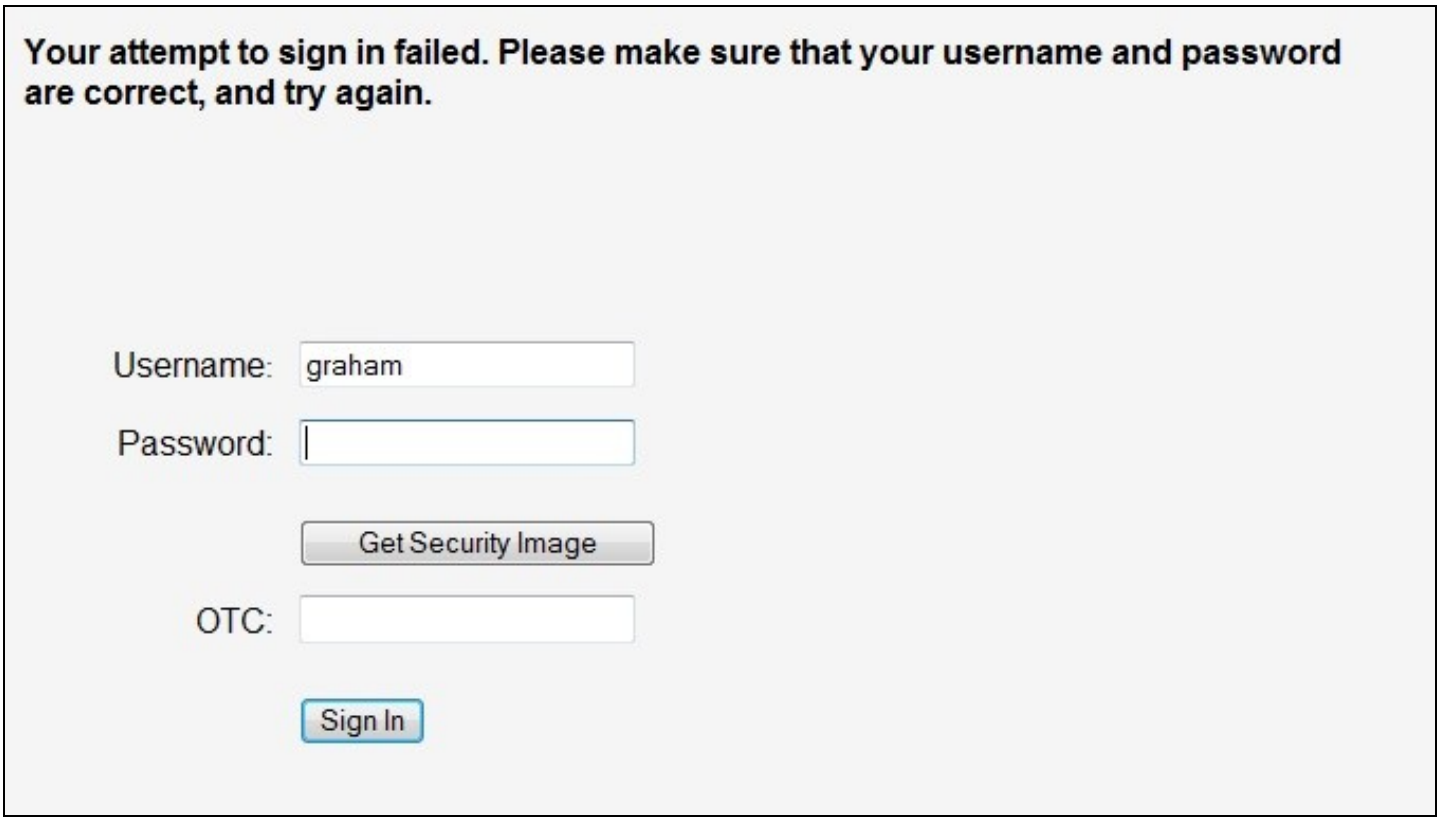
Browse to the login page, enter a username, click on the Request Turing button and the Turing image should appear. Check for Session requests with that username on Swivel, and RADIUS requests.



Test using the SMS option without clicking on the Turing button. Note: If the Single Channel Turing image is clicked it will expect a Single Channel login for the length of the session request (usually 2 minutes). Check for RADIUS requests on Swivel.



Ensure that the failed login redirects to a Swivel login page.



26 Troubleshooting

Check the Swivel logs and system event logs for any errors or lack of communication as well as the Array Networks SPX logs.

27 Known Issues and Limitations

28 Additional Information

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

29 Arx Co-Sign Integration

Arx Co-Sign Integration Guide

30 Aventail Integration

SonicWall Aventail clientless SSL VPN Gateway

Integration Guide

31 Introduction

This document outlines the steps required to integrate the SonicWALL Aventail SSL VPN with Swivel. SonicWALL Aventail SSL VPN appliances are able to use external RADIUS servers for providing authentication and Swivel provides RADIUS authentication, so this forms the basis for the integration approach. This document is designed for use with version 10.x of the SonicWALL Aventail and is significantly different to 9.x and earlier versions.

Swivel users can use either Swivel?s Single Channel (TURing, Pattern) or Dual Channel (SMS, J2ME) methods to retrieve Security Strings, which are applied against the user?s PIN to extract a One-Time Code (OTC) which represents the password for an authentication request.

With Dual Channel methods, the user already holds one or more Security Strings on their mobile device (and can request more at any time) so with the Aventail VPN configured to use the matching Swivel server for RADIUS authentication, no further integration is required. However if Swivel is set to send many security strings in a single text message, then the login page can be modified to indicate to the user which string to use. For details of this refer to the additional details section. (The Authentication configuration section below describes how to achieve the RADIUS configuration).

However with Single Channel methods, the user must be presented with a Turing or Pattern image at sign-in time (representing a single time-limited Security String), so they can extract their OTC. The SonicWall Aventail makes a proxy request to Swivel so a NAT rule is not required to Swivel, see below for details.

32 Prerequisites

SonicWall Aventail 10.5.2

or SonicWall Aventail 10.5.3 Client Hot Fix 003

Swivel 3.x

Aventail login page script

33 Baseline

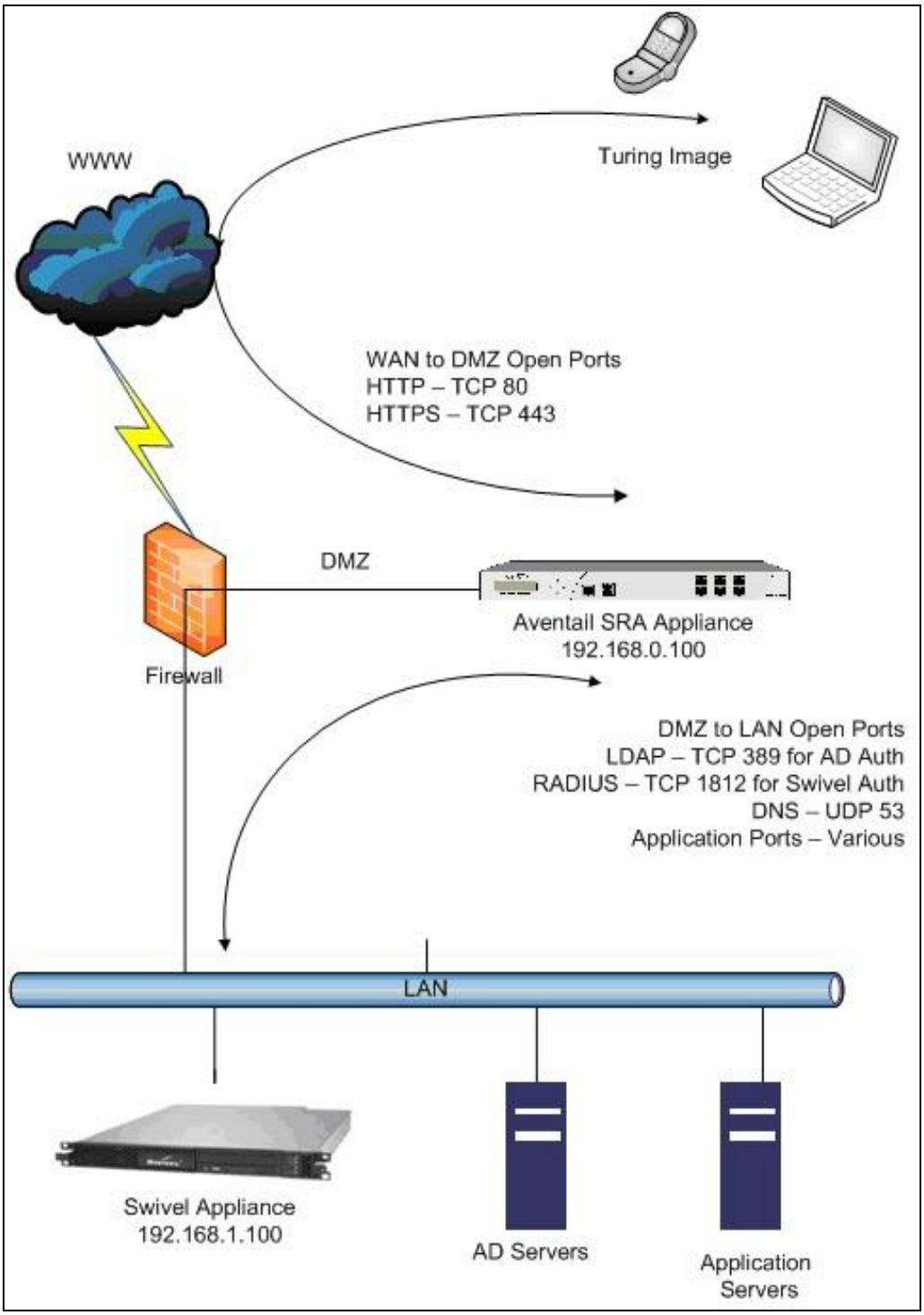
SonicWall Aventail 10.5.2 and 10.6.2-196

Swivel 3.7

34 Architecture

The user connects to the SonicWALL Aventail VPN using a web browser, pointing to the appropriate sign-in URL for the VPN in question.

The SonicWALL Aventail VPN is configured to use Swivel for radius authentication. Users are stored and maintained in Swivel.



35 Swivel Configuration

35.1 Configuring the RADIUS server

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

35.2 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.

35.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

36 SonicWall Aventail Integration

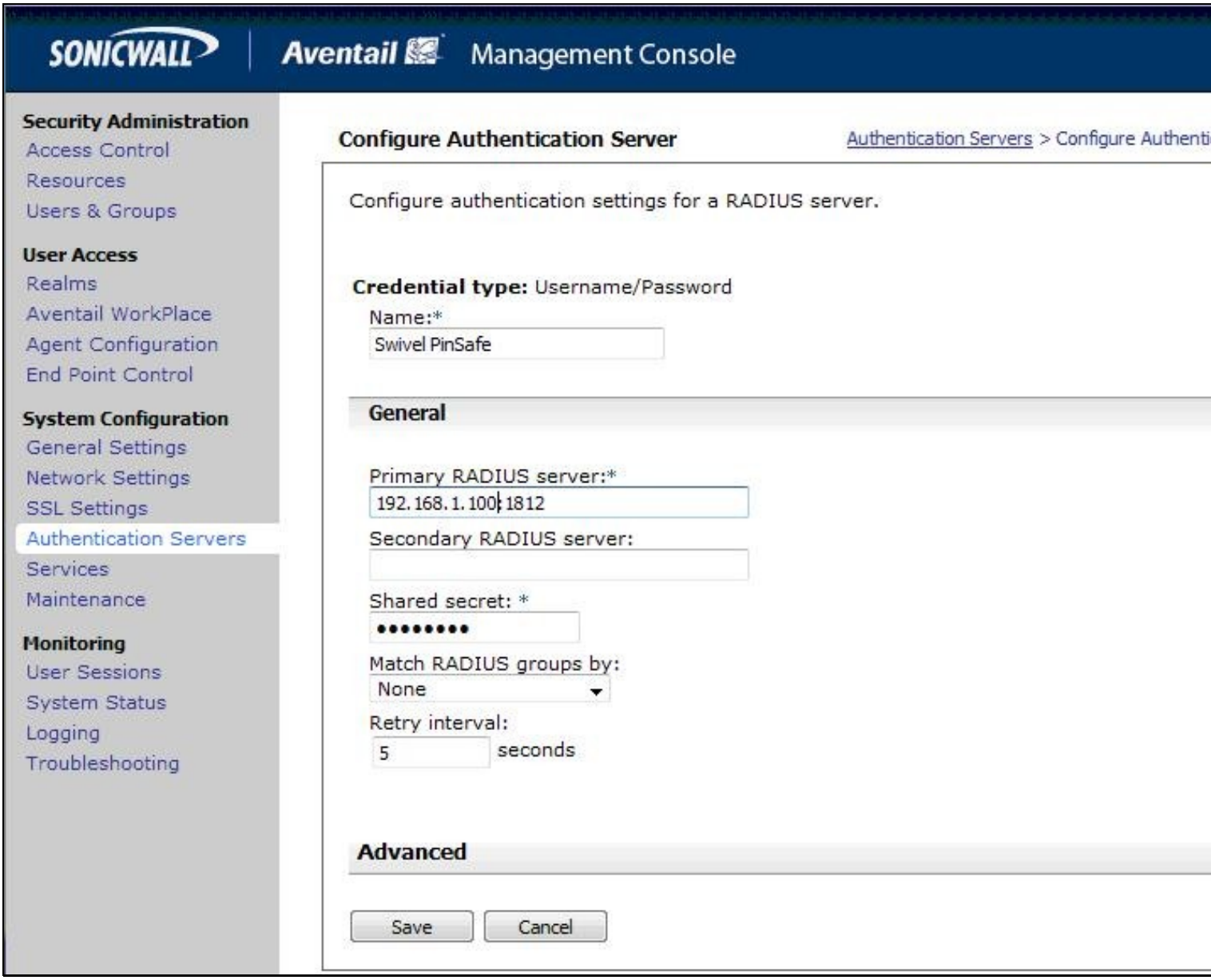
36.1 Configuring The Sonicwall Aventail for RADIUS Authentication

A new Authentication Server needs to be set up with RADIUS username/password authentication. The Primary RADIUS server needs to be set to the IP address of the Swivel virtual or hardware appliance followed by the authorisation port (see below). The secret needs to match the secret set on the NAS configuration screen.

If you want to configure a secondary Swivel RADIUS server for failover you would add the details of the server in the ?Secondary RADIUS server? section on this page.

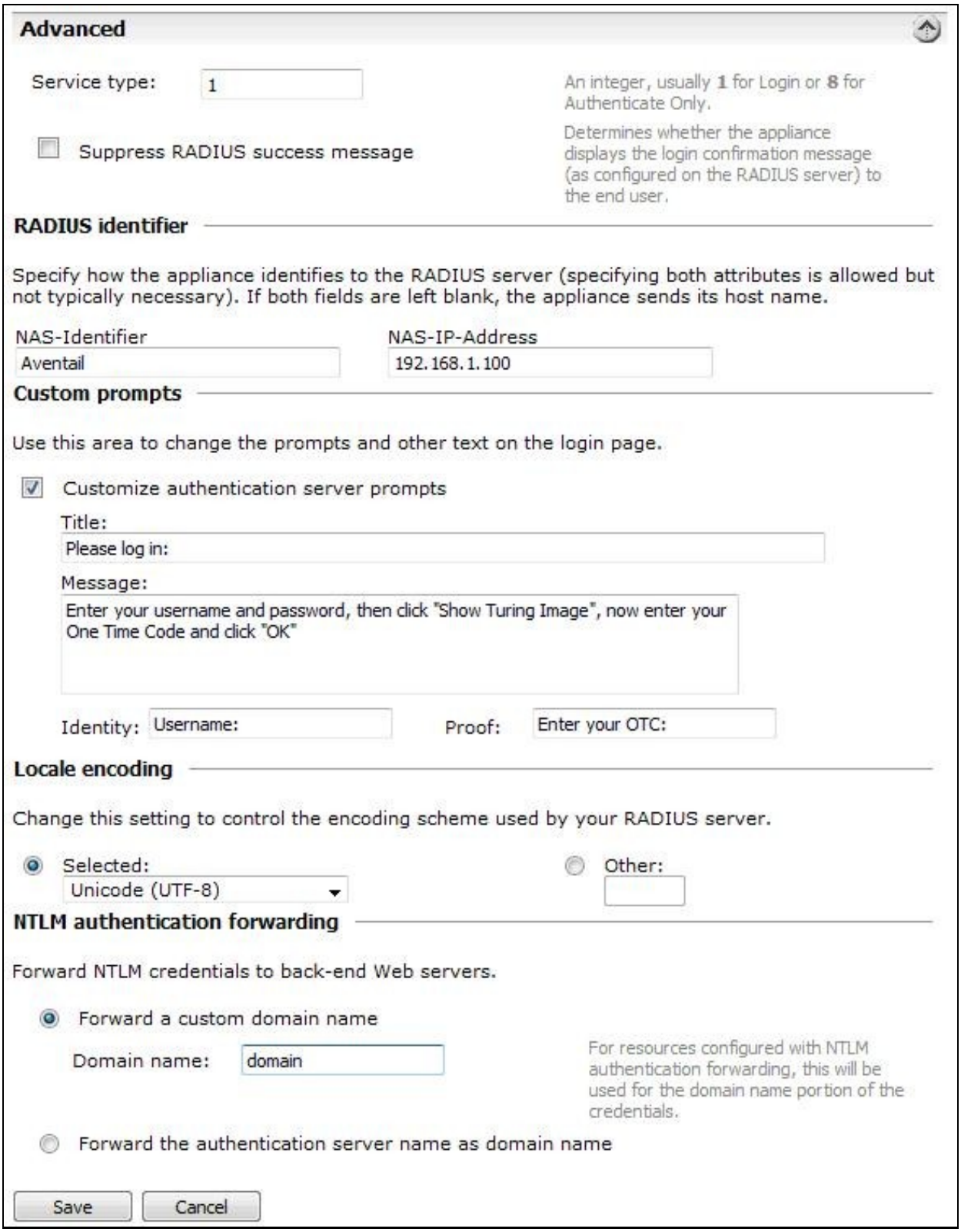
Swivel can be configured as the Primary Authentication Server or the Secondary Authentication server using *Chained Authentication*, typically AD will be the Primary authentication server and Swivel as the secondary authentication server. To configure this on the SonicWall Aventail Administration console click on Realms, then click on the name of the realm to be modified, or click New and select an authentication server in the drop down list. Click Advanced and select a Secondary Authentication server (If it has not yet been defined click on New to create it).

SonicWALL Aventail Authentication Server RADIUS Configuration



Under the Advanced section you should specify the NAS settings and you can also customise the password prompt to show ?Enter your OTC:? or whatever is you preference.

Advanced RADIUS settings



36.2 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.

36.3 Modifying the Aventail Sign-In Page for Turing

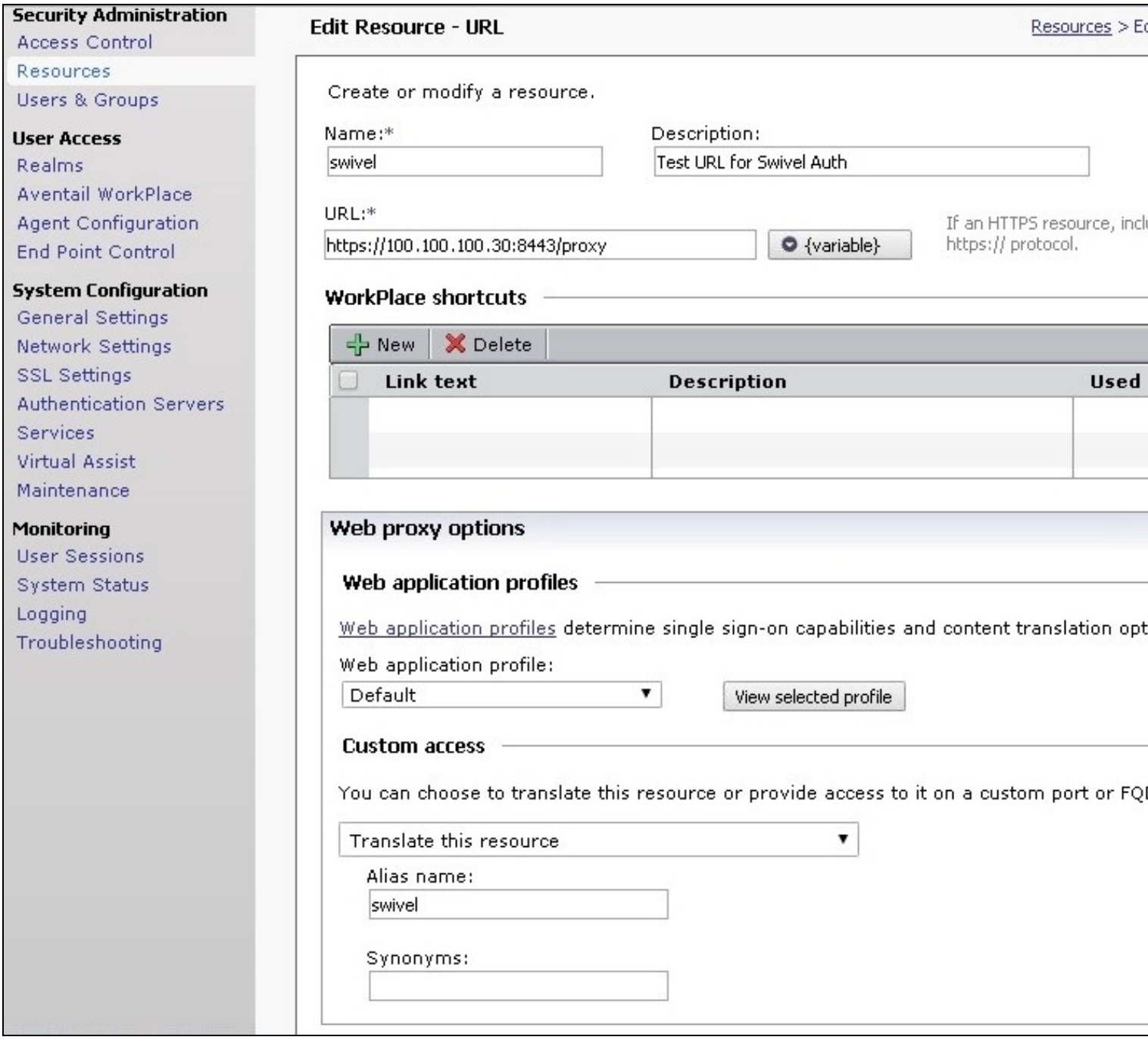
Note: When working with an Aventail Active Passive pair, the Master and Slave may need to be both configured, or shutdown the Slave whilst the master is configured for the changes to be evident.

Swivel sends Security Strings to users via SMS, J2ME (Dual Channel) or through a Turing image (Single Channel). The user extracts their One Time Code (OTC) from the Security String and enters that (preceded by their static Swivel password if they have one) into the SSL VPN log-in page.

If they were using Dual Channel (SMS or J2ME) they would have a security string ready and waiting on their mobile device. For Single Channel, we need some way of presenting a Turing image on the SSL VPN?s sign-in page.

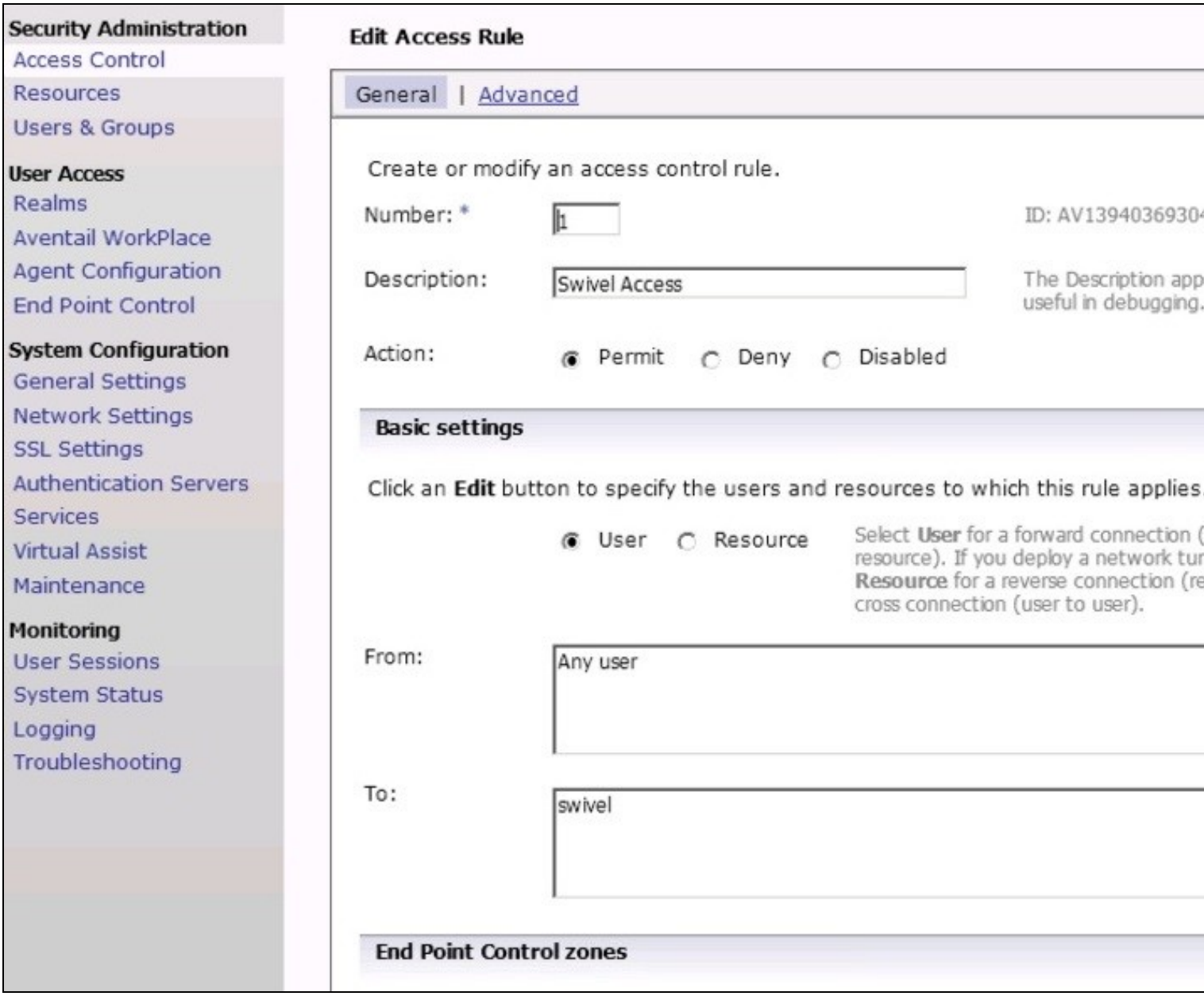
Using the Aventail AMC, it is necessary to create a URL resource for the Swivel virtual or hardware appliance and then make it available to un-authenticated users. It is also necessary to create a custom authentication page to present the ?Turing? button and also the image. The following steps describe how this is achieved.

1. Create a URL resource and give it the name ?swivel? with the URL of the Swivel virtual or hardware appliance. URL = https://swivel_server:8443/proxy for a Swivel hardware or virtual virtual or hardware appliance, for a software only install see Software Only Installation. Do not create a workplace shortcut. Under Custom access select Translate this resource with an Alias = ?swivel?. Creating an alias means the real URL of the Swivel virtual or hardware appliance is hidden from any user attempting to log in.



2. Create an ACL which allows all users access to the resource created in step 1. Select Access Control and New Rule with Permit access for type User

with access from Any User to the Swivel Resource.



3. The Swivel resource is behind and therefore protected by the Aventail appliance. It is necessary to allow un-authentication access to the URL created in step 1, this is NOT the same as adding an ACL.

a. Using an SSH client such as PUTTY or WinSCP connect to the Aventail appliance as ?root? with the admin password.

b. Then using Vi or an editor in WinSCP edit the file : /usr/local/app/mgmt-server/datastore/pending/sysconf/avconfig.xml

c. Find the resource id for the resource you just created (search for ?swivel?): <webURL id="AV1193773540220KE" name="swivel" scope="all_descendants">

d. Then, find the following line: <webAuthRule enabled="true" id="WebSSLNullAuthRule" managed="system">

e. Add your resource id to the ?destinations? block: <destinations_item refId="AV1193773540220KE"/>

f. Restart the management console: /etc/init.d/mgmt-server restart

g. Log in to the management console again and add/edit something; it doesn?t really matter what, you just want to get the ?Pending changes? and then apply the changes.

h. Changes to the avconfig.xml file will not get replicated to a HA secondary appliance so the settings need to made on this appliance. Also, during firmware upgrades the changes to avconfig.xml may not be retained.

4. For the given workplace site it is necessary to create a customised authentication request page. The section below describes this in detail.

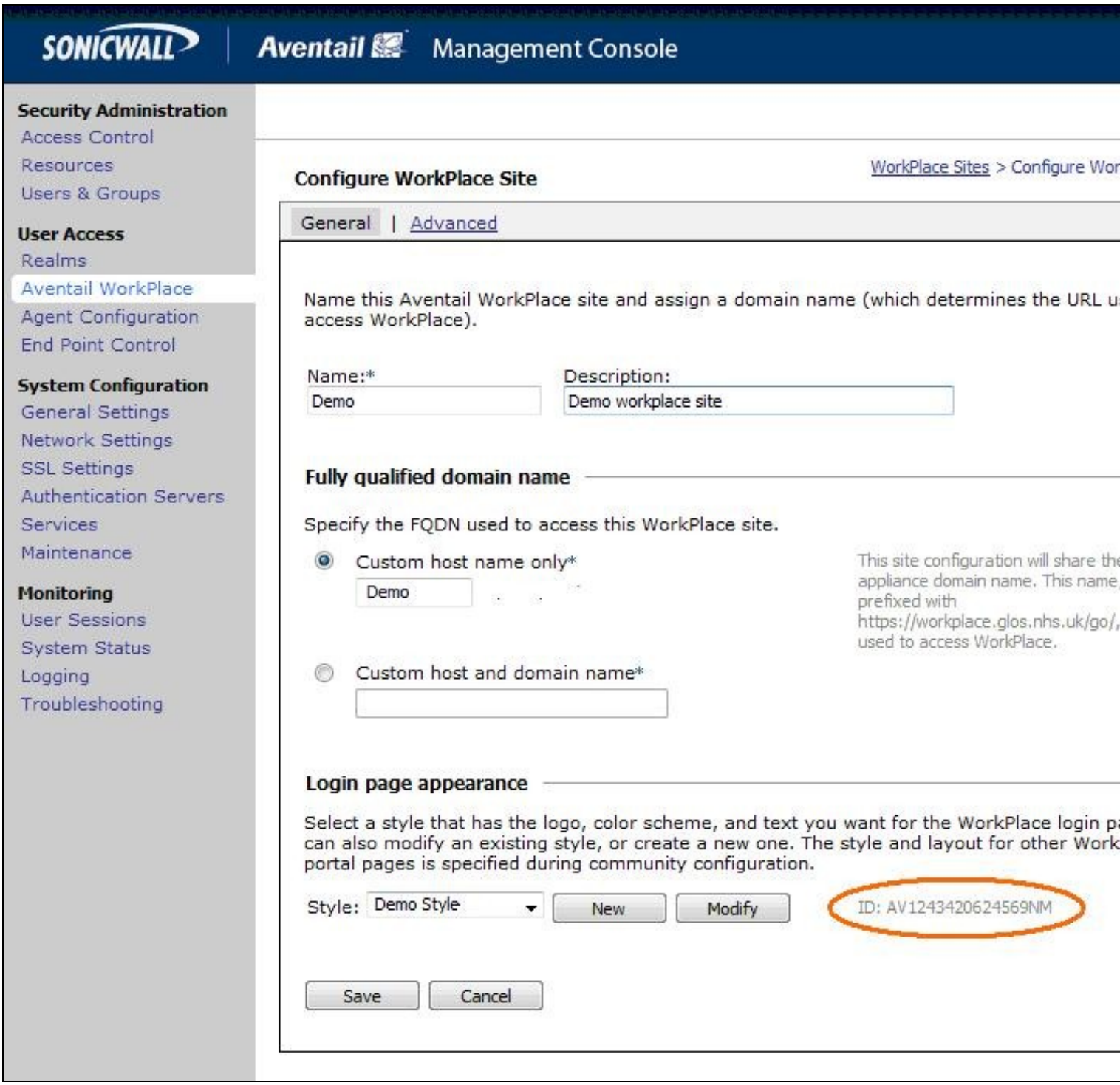
36.4 Creating A Custom Authentication Request Page

In order to have the TURing image displayed on the authentication page it is necessary to create and customise an ?authentication-request.tmpl? file.

In version 10.0.0 and later the default WorkPlace template files contain only plain HTML: the rendering is done using cascading style sheets. The content has also been streamlined with the help of tags that define more general divisions on the workplace portal pages (for example, , , , and so on).

1. For the required workplace, create a new style (or use one already created) to be used only for this workplace. Make a note of the styles ID num. The style needs to be used for the SSL VPN login point for which Swivel authentication will be used.

Configure Workplace and record Style ID



The default WorkPlace template files should be used as a starting point for customized templates, and never edited directly, because your changes will be overwritten the next time you customize WorkPlace in AMC. The default templates are as follows (one for each supported display size):

```
/usr/local/extranet/templates/extraweb.tmpl
```

```
/usr/local/extranet/templates/compact-extraweb.tmpl
/usr/local/extranet/templates/micro-extraweb.tmpl
```

When you create a workplace site, you specify a style for the login pages, which include realm selection, realm error, licensing error, and so on.

Copy the basic template from your v10 appliance: transfer /usr/local/extranet/templates/extraweb.tmpl (using WinSCP, for example) to your local computer. Log in using root and the admin password.

2. Save a copy of the extraweb.tmpl as authentication-request.tmpl.

Insert the following code into the new file directly below

```
<input type=button name=btnTuring value="Show Turing Image" onclick=ShowTuring() class='submitbutton' style="visibility:visible; position:

<img id=imgTuring name=imgTuring style="visibility:hidden;position: relative; left:40;top:70;">

<script language="JavaScript">


// Add on-blur method to username field so that
// TURing image appears automatically
if(document.getElementsByName("data_0")[0] != null) {
  document.getElementsByName("data_0")[0].onblur = function () {ShowTuring();};
}


function ShowTuring() {

sUser=document.getElementsByName("data_0")[0].value;

 if (sUser=="") {
  alert ("Please enter your username first!");
  document.getElementsByName("data_0")[0].focus()
 }  else {
//The IP address below must be the External IP of the Aventail VPN
sUrl="https://FQDN_of_workplace/swivel/SCImage?username=";

//Find the image using Mozilla compatible pproach...
varImg = document.getElementById("imgTuring");

//Set the image SRC and make it visible
varImg.src = sUrl + sUser + "&random=" + Math.round(Math.random()*1000000);
varImg.style.visibility = "visible";

//Alternative approach - show image in Popup
//window.showModalDialog(sUrl + sUser,null,"dialogWidth=305px;dialogHeight=110px;status:no;scroll:no;help:no;")

//Set focus to the OTC input
document.getElementsByName("data_2")[0].focus()
 }
}


</script>
```

The customization first adds a button to the page to allow the user to request a TURing image and a placeholder for the image so that it can be displayed.

<input type=button name=btnTuring value="Show Turing Image" onclick=ShowTuring() class='submitbutton' style="visibility:visible; position: relative; left:50;top:60;width:75;"> When the user presses the TURing button it calls the showTuring function that retrieves the image from Swivel via the alias that has been set up and makes the TURing image visible. The customisation also adds an "onblur" action to the username field. This means that when the user tabs away from the username field a TURing image will be automatically requested.

3. The newly customised authentication-request.tmpl needs to be saved to the correct location on the Aventail. Again using WinSCP, copy the file to the folder /usr/local/extranet/templates/AV(ID identified in Figure 7). The ID folder should have been created automatically when the style was created.

4. Make a change in the Aventail AMC such that ?pending changes? can be applied.

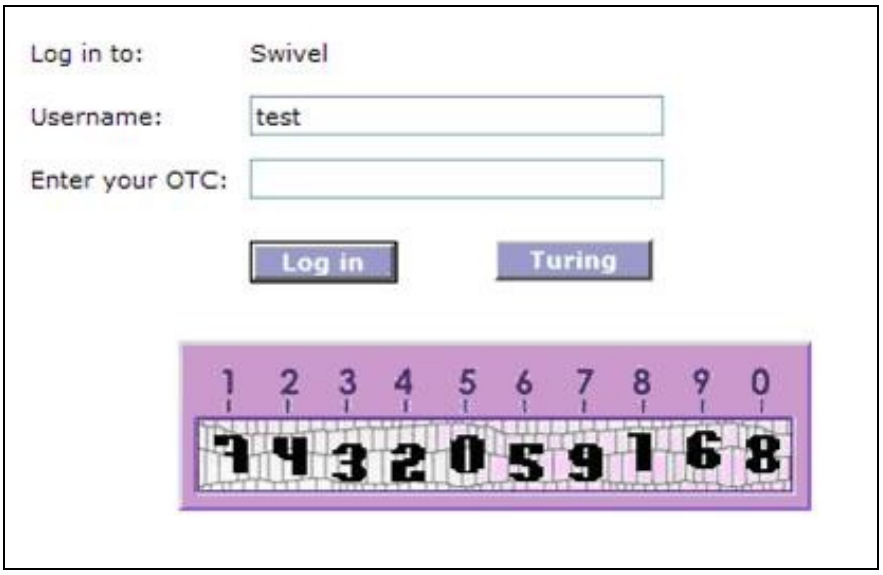
5. The newly configured workplace configuration should now be available.

If your Aventail appliance is part of a HA pair then copy the customised authentication-request.tmpl file across to the backup appliance.

37 Verifying the Installation

Login using the Turing or SMS.

Example of a modified SonicWALL Aventail sign-in page



38 Known Issues and Limitations

None

39 Configuration Options

39.1 Turing Image Size

Change the line:

<img id=imgTuring name=imgTuring style="visibility:hidden;">

to

<img id=imgTuring name=imgTuring width="450" style="visibility:hidden;">

A width of 450 to gives a 50% larger image (300 is standard). Different values may be used.

39.2 Security String Index

To modify the login page to display the required Security String index rather than a TURing image use the following modifications. See also Multiple Security Strings How To Guide

1) The button that is used for TURing needs to be changed to request the index and rather than an image tag a text field is required to display the result.

```
<tr>
 <td>
  <input type=button name=btnTuring value="Get Index" onclick=ShowIndex()
  class='submitbutton' style="visibility:visible;width:100;">
 </td>
 <td >
  Use index : <INPUT class="indextext" TYPE="text" id="indextext" name="indextext" size = "3">
  to select your security string.
 </td>
</tr>
```

Similarly the onblur action should be changed

```
if(document.getElementsByName("data_0")[0] != null) {
   document.getElementsByName("data_0")[0].onblur = function () {ShowIndex();};
}
```

2) The ShowIndex function then needs adding

```
function ShowIndex() {
{
  sUrl="https://FQDN_of_workplace/swivel/SCImage?username="
  sUser=document.getElementsByName("data_0")[0].value;
  if (sUser=="") {
   alert ("Please enter your username first!");
   document.getElementsByName("data_0")[0].focus()
 }
 else
 {
  updateindex(sUrl,sUser);
  document.getElementsByName("data_1")[0].focus()
 }
}

function updateindex(sUrl,sUser)
{
 //this means call the getText function and when callback is called,
 // call setIndex
 getText(sUrl  + sUser, setIndex) + "&random=" + Math.round(Math.random()*1000000);
}

 function getText (url, callback) {
 var request = null;
 //Initialize the request variable.
 if (window.XMLHttpRequest) {
 // Are we working with mozilla?
 request=new XMLHttpRequest();
 }
 else
 {
 //Not Mozilla, must be IE
 request=new ActiveXObject("Microsoft.XMLHTTP");
 }
 if (request==null) {
  //If we couldn't initialize request...
  alert("Your browser doesn't support the Get Index Button, sorry.");
  return false;
  }
   request.onreadystatechange = function() {
   if (request.readyState == 4 && request.status == 200)
   {
     callback(request.responseText);
   }
 }

   request.open("GET", url);
   request.send(null);
}

function setIndex(text){
 index = document.getElementById("indextext");
 if(text.length < 3){
  index.value = text;
 } else {
  index.value = "";
 }
```

```
}
```

39.3 TURing and SMS

To support TURING and SMS Index you need to include both buttons and both sets of scripts.

But not have any onBlur action on the username, as the user may choose either option.

39.4 Manual Turing Display

To stop the automated Turing display remove the **.onblur** entry. Note you would use this where dual channel authentication is required. The starting of a single channel session makes the Swivel server expect a single channel login:

```
// Remove on-blur method to username field so that
// TURing image appears automatically
 if(document.getElementsByName("data_0")[0] != null) {
   document.getElementsByName("data_0")[0] = function () {ShowTuring();};
 }
```

39.5 Automated Turing Display

To automate the Turing display we can add the below lines of code. Note you would not use this where dual channel authentication is required as the starting of a single channel session makes the Swivel server expect a single channel login:

```
// Add on-blur method to username field so that
// TURing image appears automatically
 if(document.getElementsByName("data_0")[0] != null) {
   document.getElementsByName("data_0")[0].onblur = function () {ShowTuring();};
 }
```

Example:

```
<input type=button name=btnTuring value="Show Turing Image" onclick=ShowTuring() class='submitbutton' style="visibility:visible; position:

<img id=imgTuring name=imgTuring style="visibility:hidden;position: relative; left:40;top:70;">

<script language="JavaScript">


// Add on-blur method to username field so that
// TURing image appears automatically
if(document.getElementsByName("data_0")[0] != null) {
  document.getElementsByName("data_0")[0].onblur = function () {ShowTuring();};
}


function ShowTuring() {

{
 sUser=document.getElementsByName("data_0")[0].value;

 if (sUser=="") {
  alert ("Please enter your username first!");
  document.getElementsByName("data_0")[0].focus()
 }

else

{
//The IP address below must be the External IP of the Aventail VPN
sUrl="https://FQDN_of_workplace/swivel/SCImage?username=";

//Find the image using Mozilla compatible pproach...
varImg = document.getElementById("imgTuring");

//Set the image SRC and make it visible
varImg.src = sUrl + sUser + "&random=" + Math.round(Math.random()*1000000);
varImg.style.visibility = "visible";

//Alternative approach - show image in Popup
//window.showModalDialog(sUrl + sUser,null,"dialogWidth=305px;dialogHeight=110px;status:no;scroll:no;help:no;")

//Set focus to the OTC input
document.getElementsByName("data_2")[0].focus()
 }
}
}

</script>
```

40 Troubleshooting

Check the Swivel logs for TURing images and RADIUS requests.

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - Duplicate packet from NAS

This can be caused by the following:

- If the Swivel server sends the reply but it is not received by the access device, the access device may try to resend the RADIUS request. This can be caused by the Access device sending a RADIUS request from an external interface, but not accepting the response through that external interface.

If a red cross appears instead of the TURing image it is likely that a self signed certificate may be preventing the image from appearing. To verify this, in I.E. right click on the red cross and click on properties, copy the URL into the URL bar and see if a certificate error occurs with an image. The URL will be similar to:

virtual or hardware Appliance: https://<VPN URL>:8443/proxy/SCImage?username=test

For a software only install see Software Only Installation

To overcome this install a valid certificate on the Swivel virtual or hardware appliance. Using non SSL communication will likely result in the web browser creating a pop up about SSL and non SSL communications in the web page.

41 Additional Information

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

42 Barracuda SSL VPN Integration

43 Introduction

This document describes steps to configure a Barracuda SSL VPN with Swivel as the authentication server.

Swivel can provide Two Factor authentication with SMS, Token, Mobile Phone Client and strong Single Channel Authentication TURing, Pinpad or in the Taskbar using RADIUS.

To use the Single Channel Image such as the TURing Image, the Swivel server must be made accessible. **The client requests the images from the Swivel server, and is usually configured using a NAT** (Network Address Translation), often with a proxy server. The Swivel appliance is configured with a proxy port to allow an additional layer of protection.

44 Prerequisites

Barracuada SSL VPN 380 or higher. Note the SSL VPN 280 does not support RADIUS authentication.

Barracuda Documentation

Swivel 3.x, 3.5 for RADIUS groups

The Swivel server must be accessible from the Barracuda SSL VPN using RADIUS.

The Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, and security string number, **for external access this is usually through a NAT**.

45 Baseline

Barracuda SSL VPN 2.2.2.203 and 2.2.2.115

Swivel 3.9

46 Architecture

The Barracuda SSL VPN makes authentication requests against the Swivel server by RADIUS.

The client makes TURing requests against the Swivel server using HTTP/HTTPS

47 Swivel Configuration

47.1 Configuring the RADIUS server

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

47.2 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.

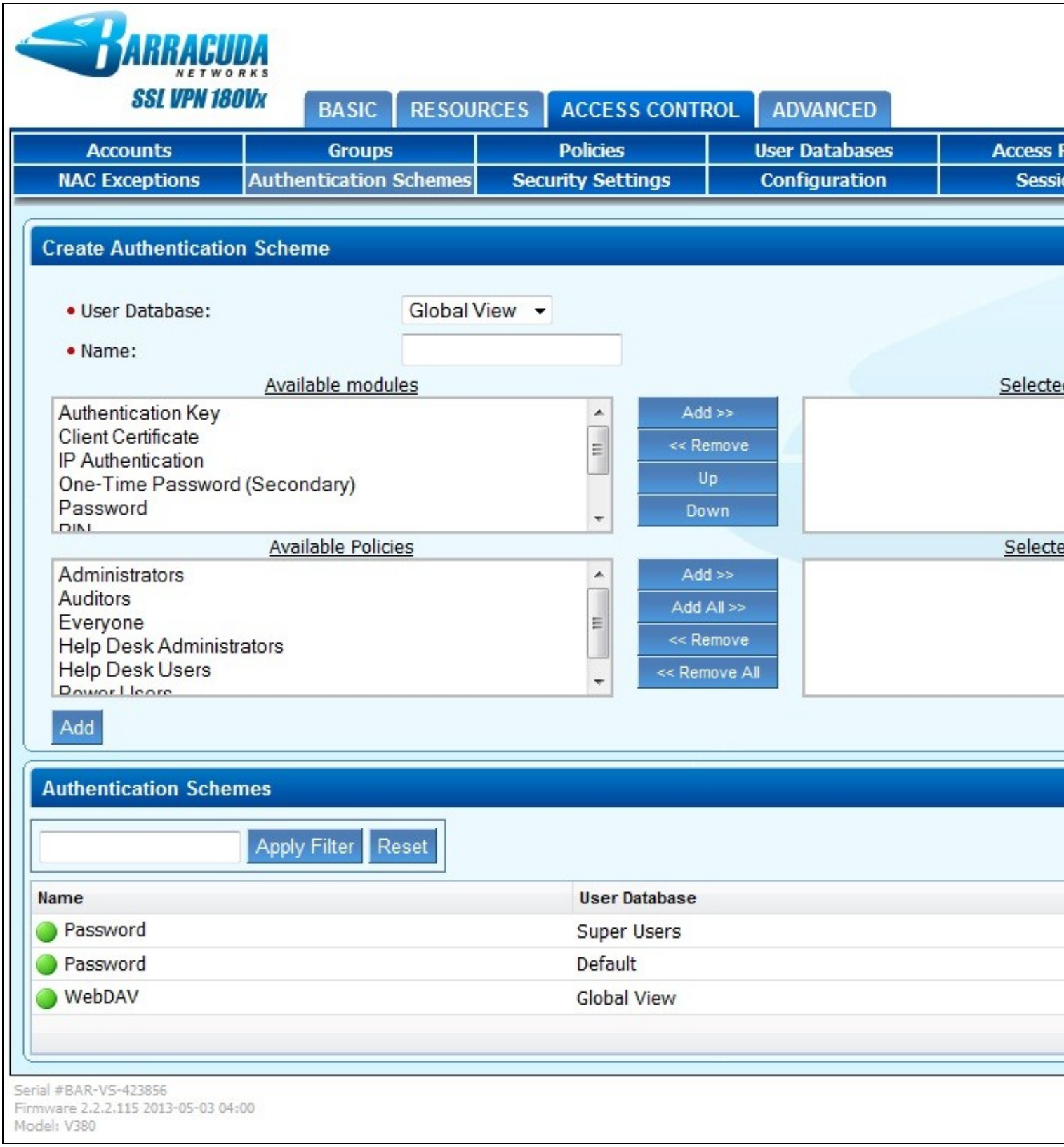
48 Barracuda SSL VPN Configuration

Login to the Barracuda SSL VPN administration console, usually through the ssladmin login.

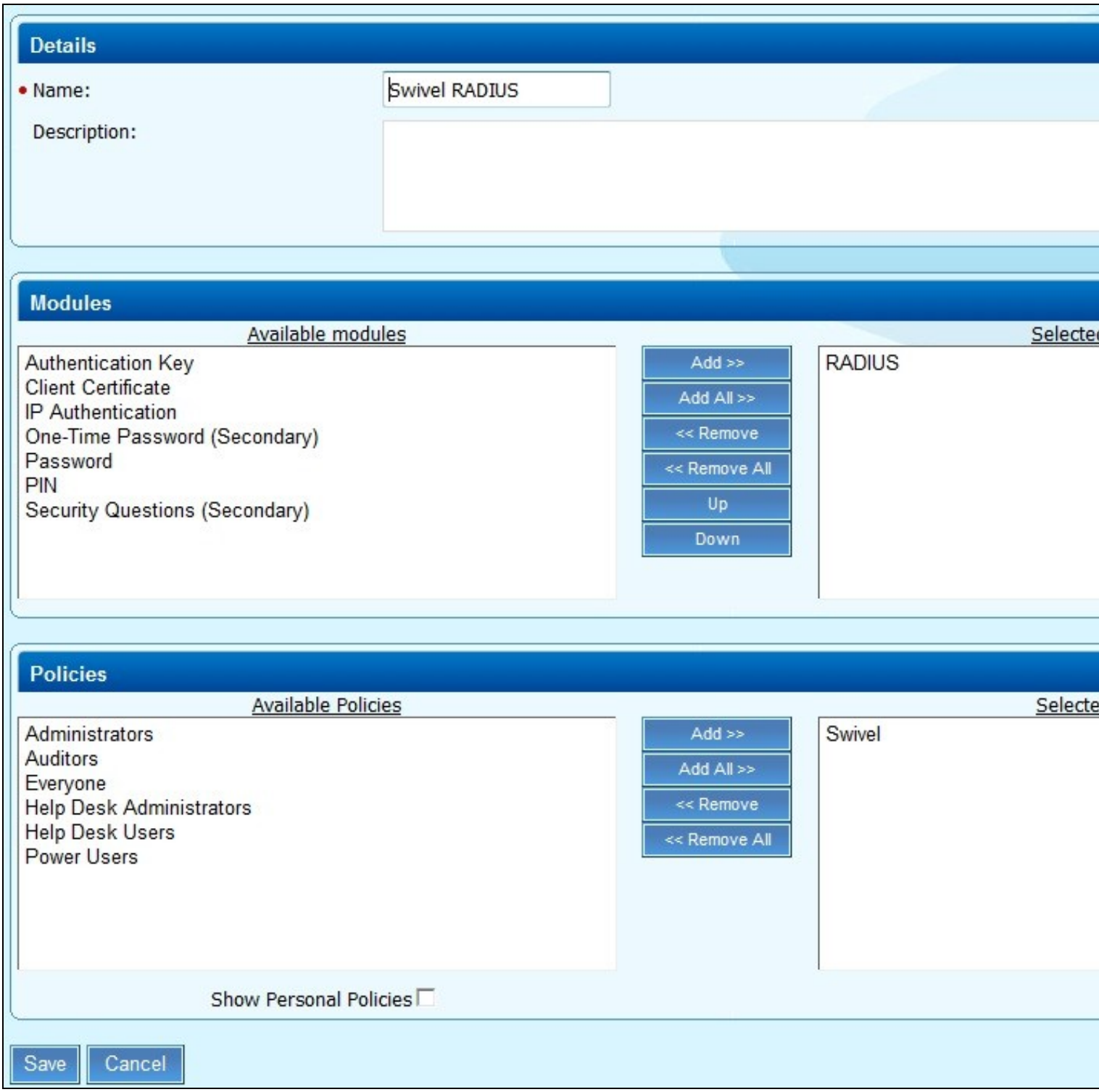
The user must exist as a user on the Barracuda SSL VPN, the user can be created through the Access Control Tab then select Accounts. Other user data sources may be configurable such as AD.

48.1 Create an authentication scheme

From the Access Control tab select Authentication schemes.



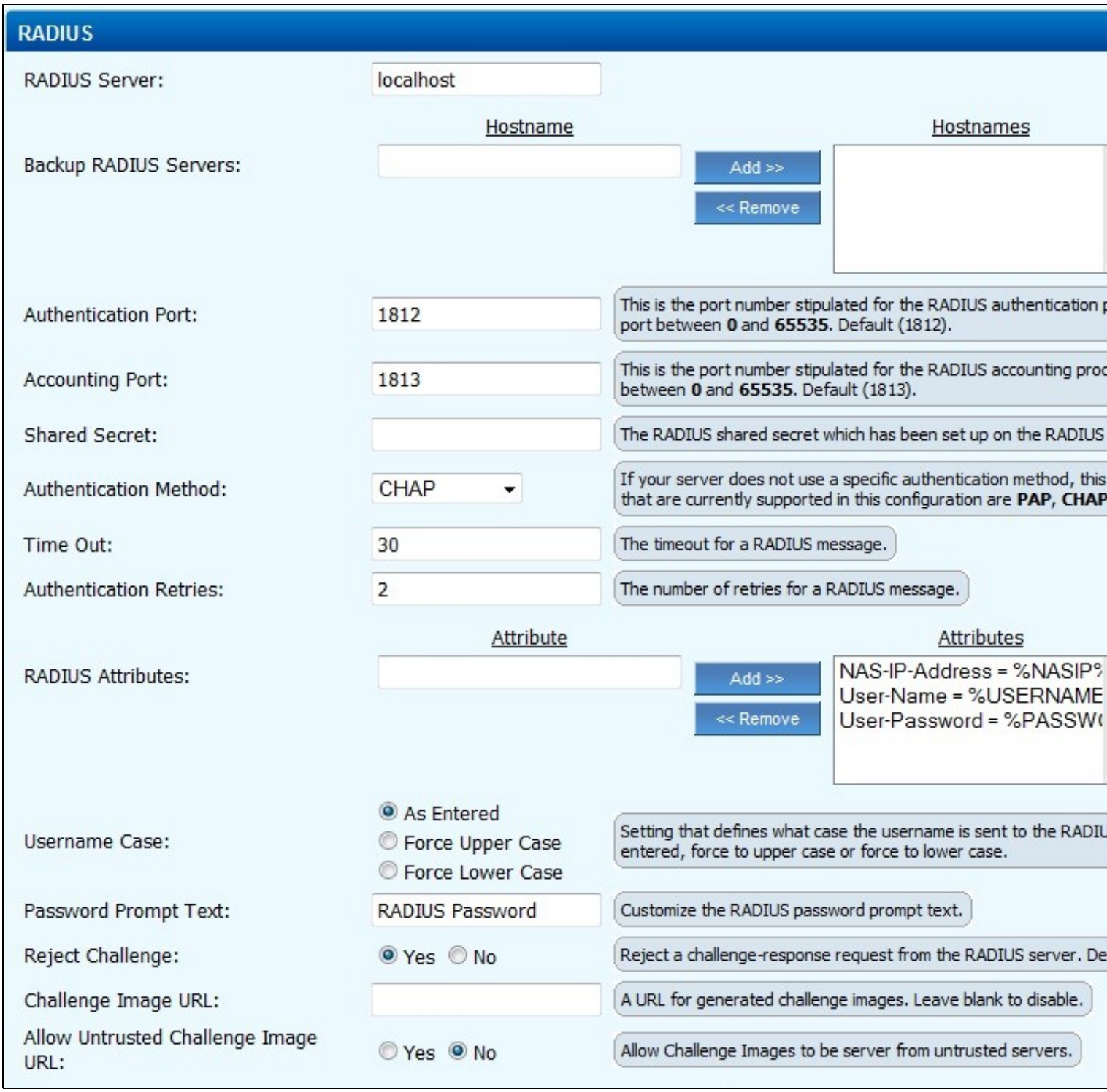
Enter a name for Authentication Scheme, such as **Swivel RADIUS**. From Available Modules select RADIUS then click on Add >>, so it appears on the right as a Selected module., and then select from Available policies the policy required and click Add >>. When complete click Add. A default policy can be used, in this example it is using a custom policy created under Access Control/Policies.



If required move the **Swivel RADIUS** authentication scheme to the top of the list, the top entry is the default entry presented to the user at login, click More to change the priority.

48.2 Barracuda RADIUS Configuration

On the SSL VPN administration console select the Access Control tab then select configuration.



Enter the following information:

RADIUS Server: Swivel RADIUS server hostname or IP (Note do not use the Swivel VIP address if this is being used, but the real IP address, see VIP on PINsafe Appliances).

Backup RADIUS Servers: Additional Swivel RADIUS instances as required.

Authentication Port: The Swivel server RADIUS authentication port, default 1812.

Accounting Port: The Swivel server RADIUS accounting port, default 1813.

Shared Secret: The shared secret entered into the NAS entry on the Swivel server.

Authentication Method: Use PAP for Challenge and Response/Two Stage Authentication and mobile clients.

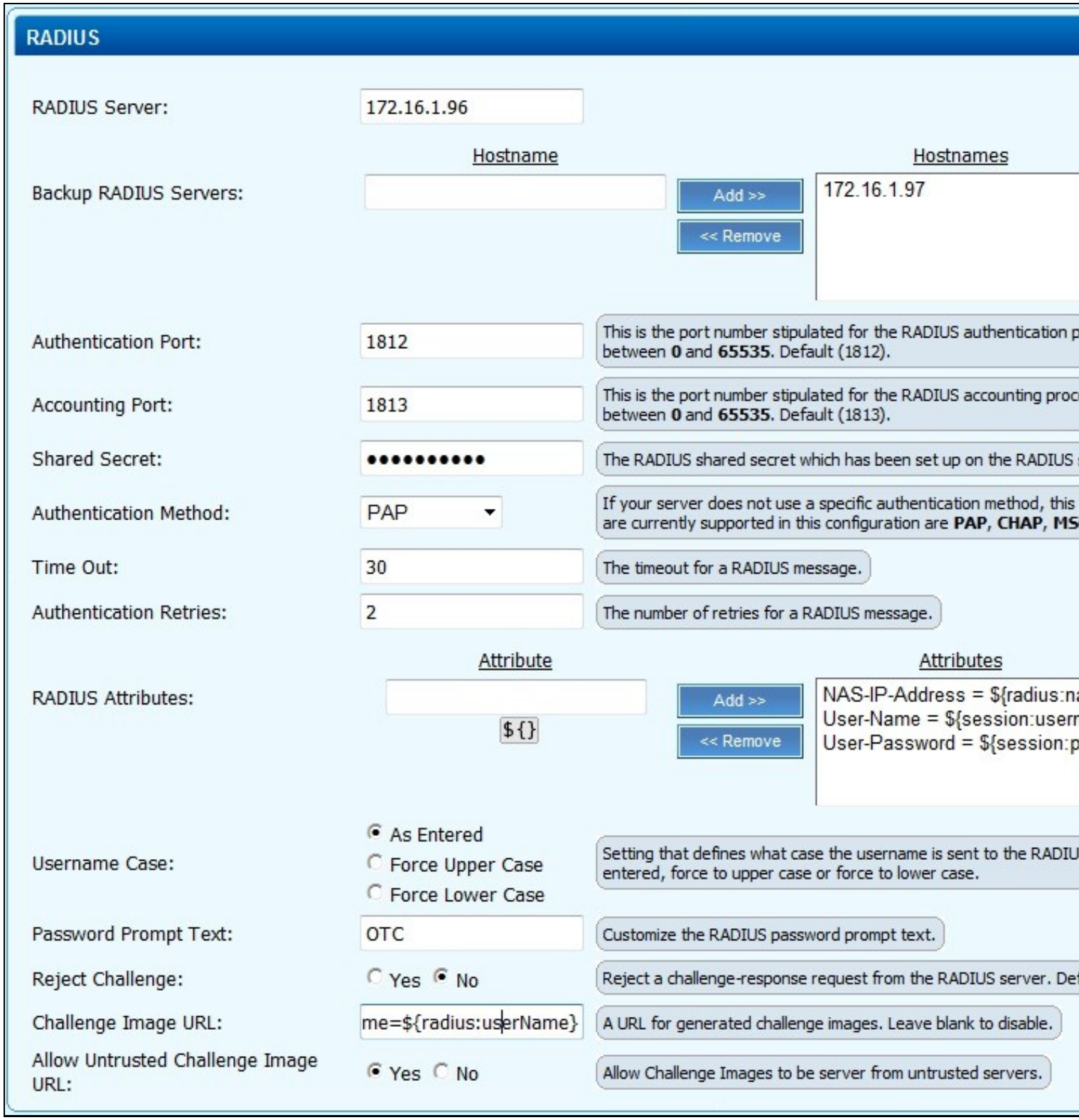
Password Prompt Text: The text to be displayed in the login field, usually set to OTC or One Time Code.

Reject Challenge: Set to No if Two Stage Authentication/Challenge and Response is to be used.

Challenge Image URL: Enter Swivel server details for graphical images to be used for authentication.

See options below for different configuration options.

Allow Untrusted Challenge Image URL: Set to Yes.



Save the RADIUS settings.

48.3 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.

48.4 Additional Configuration options

48.4.1 Additional RADIUS configuration Options: Single Channel TURing graphical image

This allows the graphical single channel TURing image to be displayed to the user for authentication. If this is not required, such as if SMS and Mobile Phone Client authentication is to be used, then this step should be skipped and the **Challenge Image URL:** left blank.

To configure the single channel graphical image set **Challenge Image URL:** to:

For an Appliance

```
https://Swivel_server_public_hostname:8443/proxy/SCImage?username=${radius:userName}
```

For a software only install see Software Only Installation

Allow Untrusted Challenge Image URL: Set to Yes.

Save the RADIUS settings.

48.4.2 Additional RADIUS configuration Options: Multiple String delivery index display

When a user logs in the user can be displayed an image telling them which of their security strings to use for authentication. See also Multiple Security Strings How To Guide

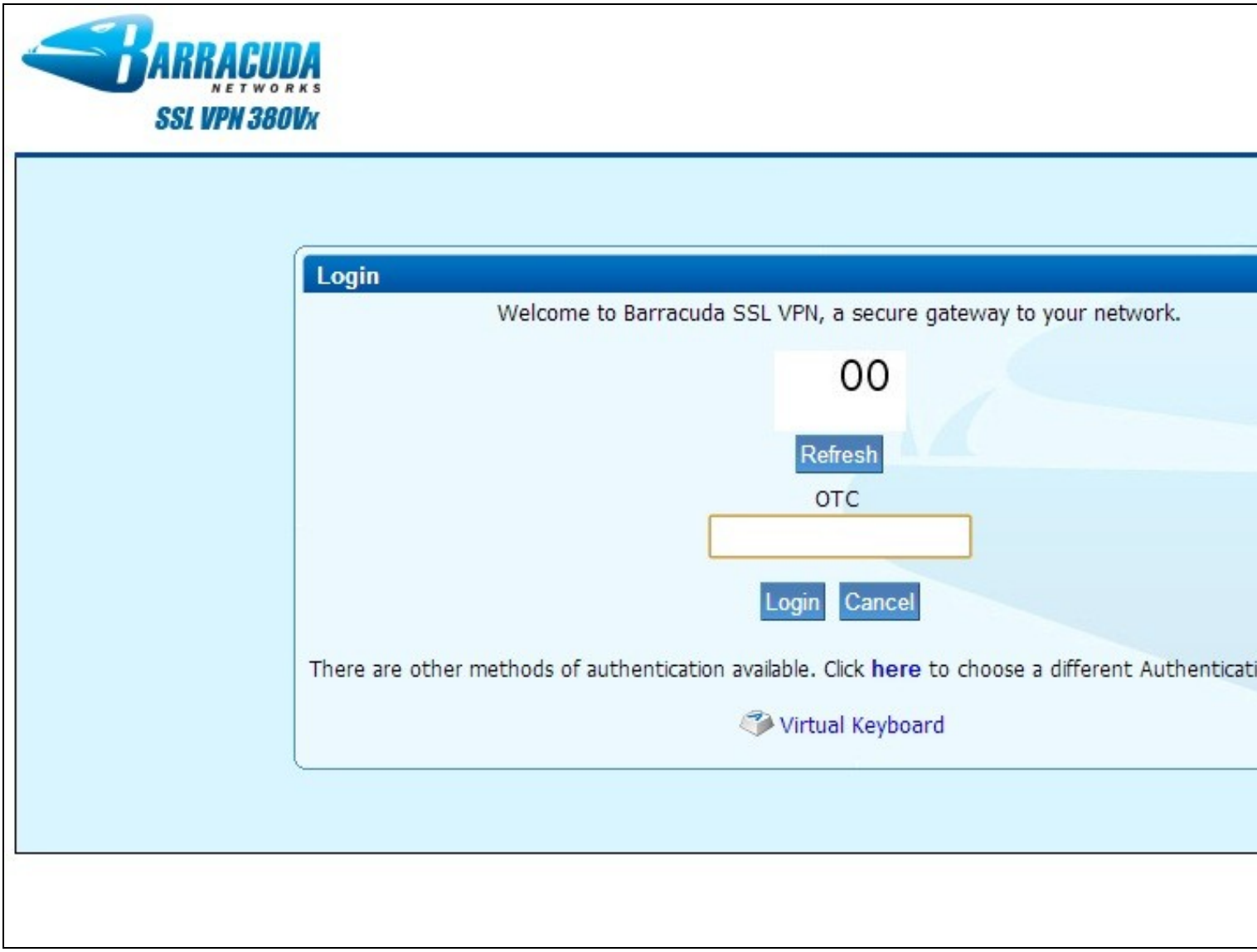
Set **Challenge Image URL:** to:

For an Appliance

```
https://Swivel_server_public_hostname:8443/proxy/DCIndexImage?username=${radius:userName}
```

For a software only install see Software Only Installation

Save the RADIUS settings.



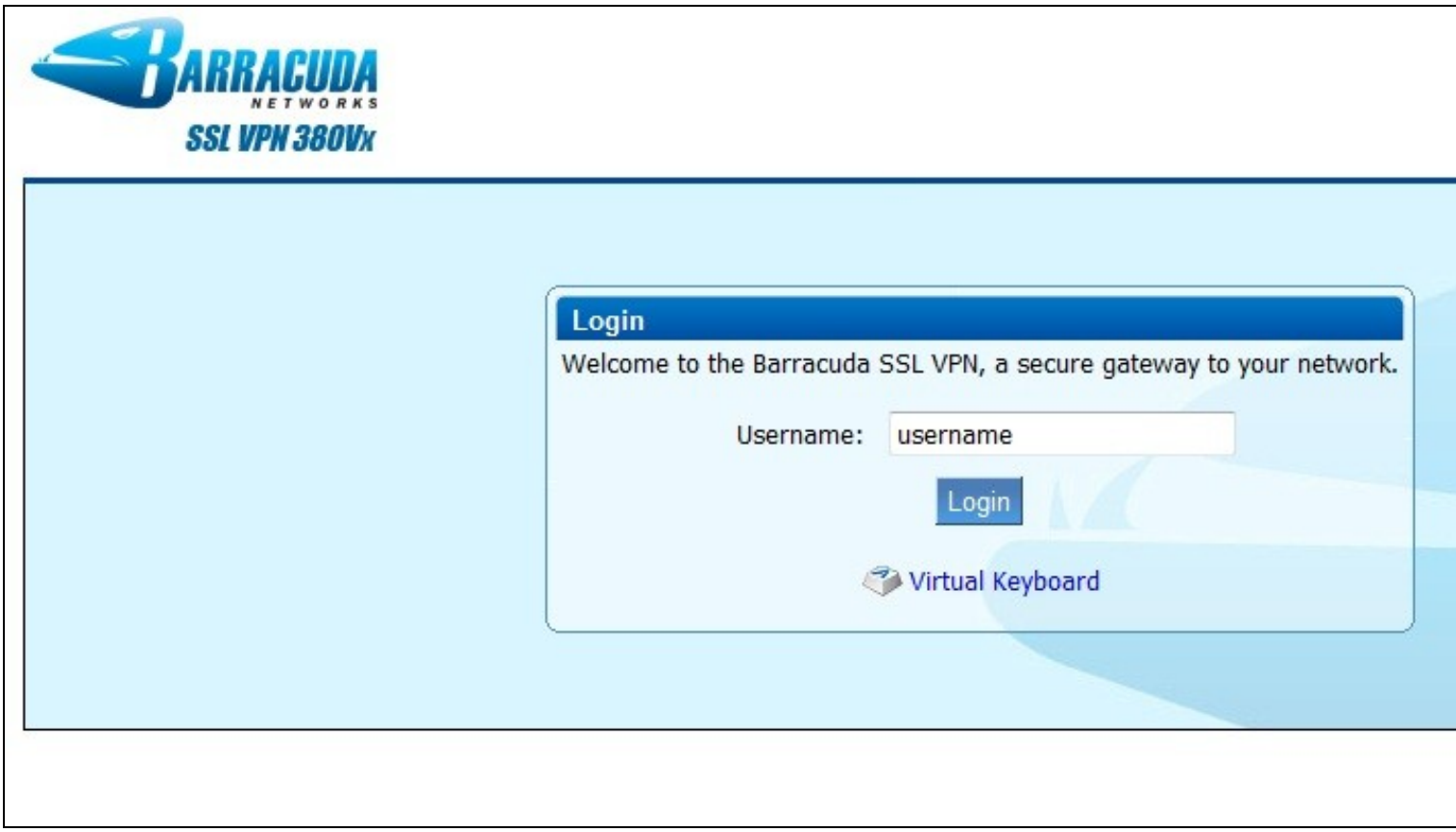
48.4.3 Additional RADIUS configuration Options: Two Stage Authentication

This allows the user to enter a username, then on the second screen a password and then on the third screen will be required to enter their One Time Code. Note that where the graphical TURing image or other image is used, then this will be displayed on the second and third screens even though it is not required on the second screen. See also Two Stage Authentication How to Guide

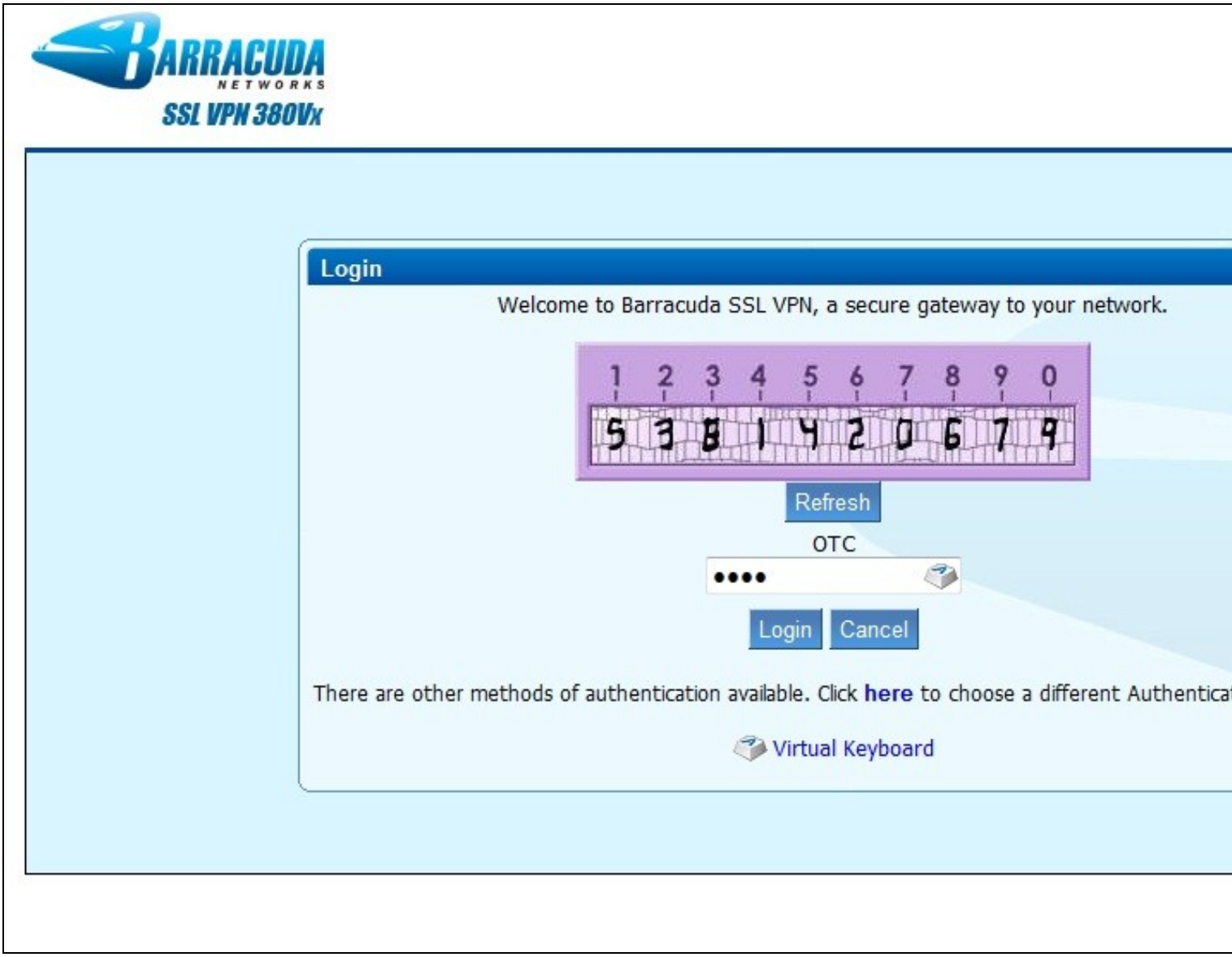
This requires the Barracuda SSL VPN setting **Reject Challenge:** to be set to No if Two Stage Authentication/Challenge and Response is to be used, and **Authentication Method:** should be set to PAP, save the RADIUS settings. On the Swivel administration console the RADIUS/NAS/Two stage authentication needs to be set to Yes, then click Apply. The user also needs to have a repository password, see Password How to Guide.

49 Testing

Select the Barracuda SSL VPN login page, enter a username, then select login.



Enter the One Time Code and click login.


BARRACUDA
NETWORKS
SSL VPN 380Vx
Login
Welcome to Barracuda SSL VPN, a secure gateway to your network.
1 2 3 4 5 6 7 8 9 0
5 3 8 1 4 2 0 6 7 9
Refresh
OTC
Login
Cancel
There are other methods of authentication available. Click here to choose a different Authentica
Virtual Keyboard

50 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

51 Known Issues and Limitations

Two Stage authentication will display an image at each stage.

Change PIN is not currently supported to redirect to a Swivel Change PIN page.

52 Additional Information

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

53 Bluecoat ProxySG Integration

Bluecoat Proxy SG Guide

54 Bomgar

55 Introduction

This document describes the steps to configure Bomgar with Swivel as the authentication server. Swivel can provide Two Factor authentication with SMS, Token, Mobile Phone Client, It is not currently possible to embed the TURing or Pinpad within the login page/client but these can be provided instead by Taskbar or User Portal for strong Single Channel Authentication.

56 Prerequisites

Bomgar Account

Bomgar Documentation

Swivel 3.x, 3.5 or higher for RADIUS groups

To use the Single Channel Image such as the TURing Image, the Swivel server must be made accessible and the security string provided through the Taskbar, User Portal or other web page, usually through a NAT.

57 Baseline

Bomgar Product Version 14.2.2, Product Build 51805, API Version 1.12.0

Swivel 3.10.1

58 Architecture

The Bomgar software makes authentication requests against the Swivel server by RADIUS.

59 Swivel Configuration

59.1 Configuring the RADIUS server

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

59.2 Configuring Two Stage Authentication

The Bomgar client software supports Two Stage Authentication. It is suggested to initially configure just with an OTC and if Two stage authentication is required, configure this once everything has been tested and proven to be working.

See Challenge and Response How to Guide

59.2.1 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.

59.3 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

60 Bomgar Configuration

The following document provided by Bomgar outlines the integration setting on Bomgar: Bomgar RADIUS Integration.

60.1 Test the RADIUS authentication

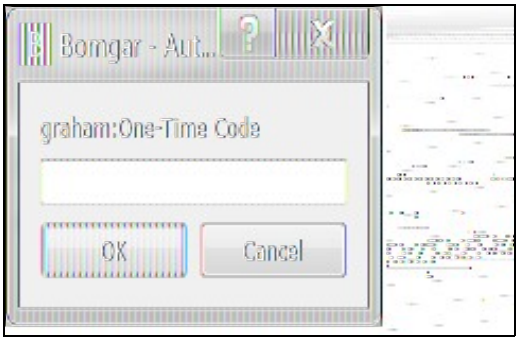
The Bomgar configuration has a test tool, and at this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Either using the test tool or through the the web login page, and enter Username and 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 OTP prompt 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, and is contactable.

If this works then the client software login can be tested.

Bomgar Client login



Bomgar client login uisng Two Stage Authentication



60.2 Optional

61 Testing

62 Additional Configuration Options

63 Troubleshooting

64 Known Issues and Limitations

None

65 Additional Information

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

66 Category:CheckPoint

67 Category:Cisco

68 Category:Citrix

69 Cyberoam UTM SSL VPN

70 Introduction

This document describes steps to configure a Cyberoam UTM firewall with integrated SSL VPN and PINsafe as the authentication server for authentication using SMS, Mobile Phone Client or the PINsafe Taskbar utility. It is not possible to embed the graphical single channel image directly into the login page.

70.1 Prerequisites

Cyberoam CRxxx (except CR15i and CR15wi as these do not have SSL VPN support)

Cyberoam Firmware 10.x

PINsafe 3.x

70.2 Baseline

Cyberoam CR25i firmware 10.01.0 build 739

PINsafe 3.8

70.3 Architecture

The Cyberoam CR25i makes authentication requests against the PINsafe server by RADIUS. PINsafe can also verify the AD or other supported repository password where required.

71 Swivel Configuration

71.1 Configuring the RADIUS server

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

If Tight Integration is to be used with RADIUS groups then ensure RADIUS Groups is set to YES.



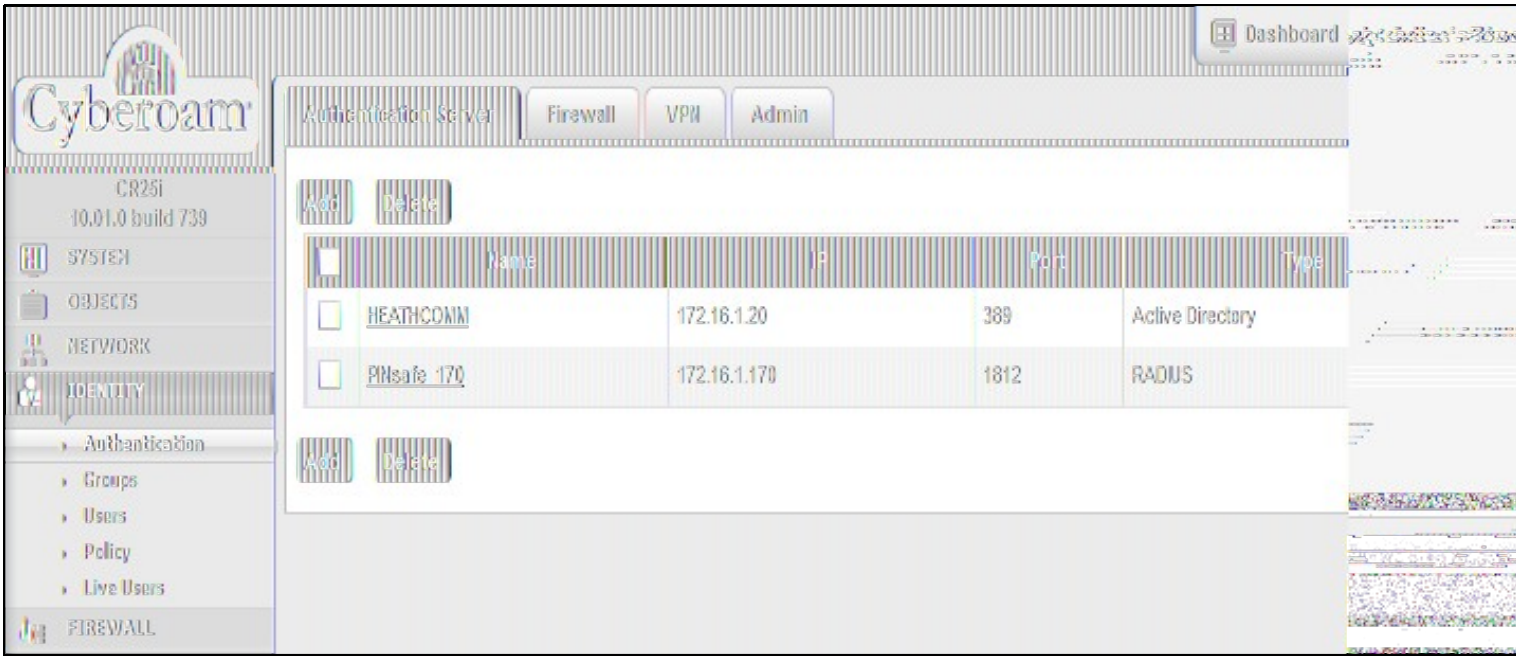
71.2 PINsafe Dual Channel Authentication

See Transport Configuration

72 Cyberoam CR25i Configuration

72.1 Define a RADIUS server on the Cyberoam

On the Cyberoam CR25i Administration console select Identity, then Authentication and the Authentication Server Tab, then click on Add.



Enter the PINsafe RADIUS server authentication details as follows:

- Server Type: RADIUS Server
- Server Name: Descriptive name for the PINsafe server
- Server IP: PINsafe server IP address
- Authentication Port: usually 1812
- Shared Secret: A secret password also entered on the PINsafe RADIUS NAS entry
- Integration Type: Loose Integration or Tight Integration as described below:

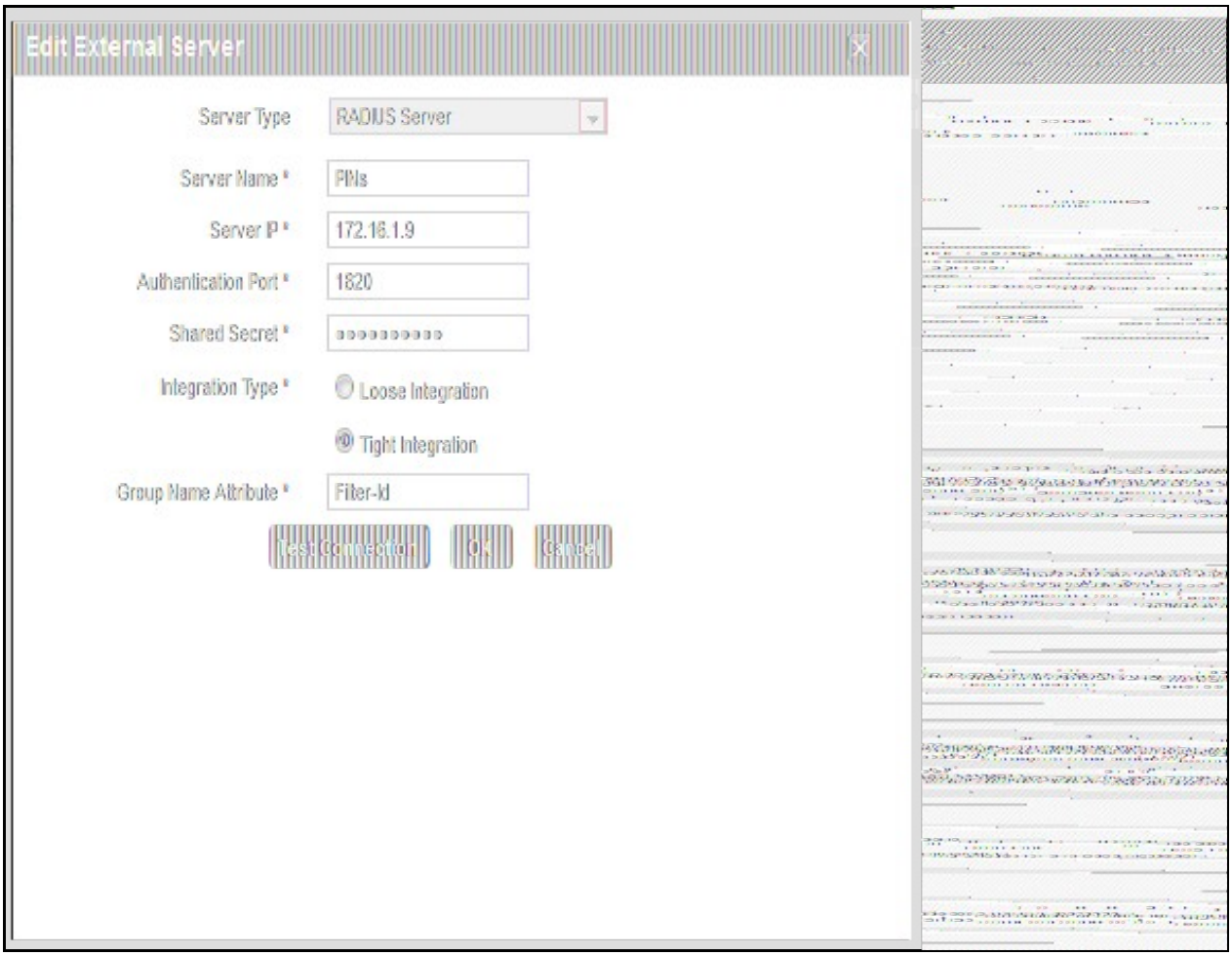
72.1.1 Loose Integration

With loose integration, Cyberoam does the Group management and does not synchronize groups with RADIUS server when user tries to logon. By default, users will be the member of Cyberoam default group irrespective of RADIUS Server group. Administrators can change the group membership. If Loose Integration is used, new users will be added to the default user group on the Cyberoam.

72.1.2 Tight Integration

With Tight integration, Cyberoam synchronizes groups with the PINsafe RADIUS Server every time the user tries to logon. Hence, even if the group of a user is changed in Cyberoam, on each subsequent login attempt, the user logs on as the member of the same group as configured on the PINsafe RADIUS Server. In this case group membership of each user is as defined in the RADIUS Server. The PINsafe RADIUS server needs to be configured to use RADIUS groups.

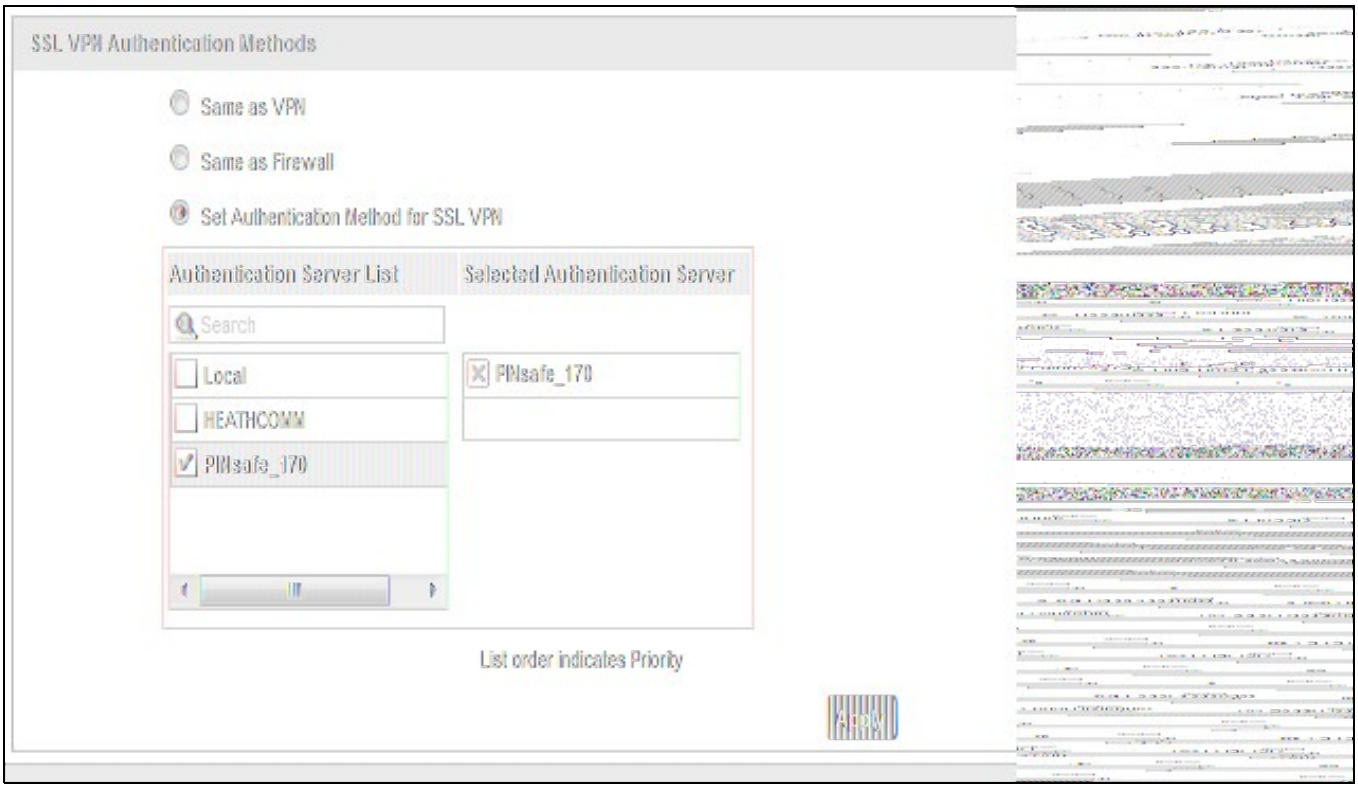
Note: when creating a SSL VPN policy, a user needs to login to the Captive Portal first, which creates the RADIUS user on the Cyberroam. They can then login to the SSL VPN portal



72.2 Cyberoam SSL VPN Authentication Methods

On the Cyberoam Administration console select Menu Identity, then Authentication then the VPN tab and select the Set Authentication Method for SSL VPN. All authentication servers that have been configured on the unit is shown on the left side. So the PINsafe RADIUS server added in the previous step should show up here. Tick the server to select it. It will then be shown in the list on the right side. It is possible to select more than one server if you have an active/active PINsafe configuration.

Note is is not possible to check authentication against multiple authentication types, the first authentication method that matches the user will be used. To configure authentication with multiple authentication servers see Additional Cyberoam Configuration Options below.



72.3 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.

72.4 Additional Cyberoam Configuration Options

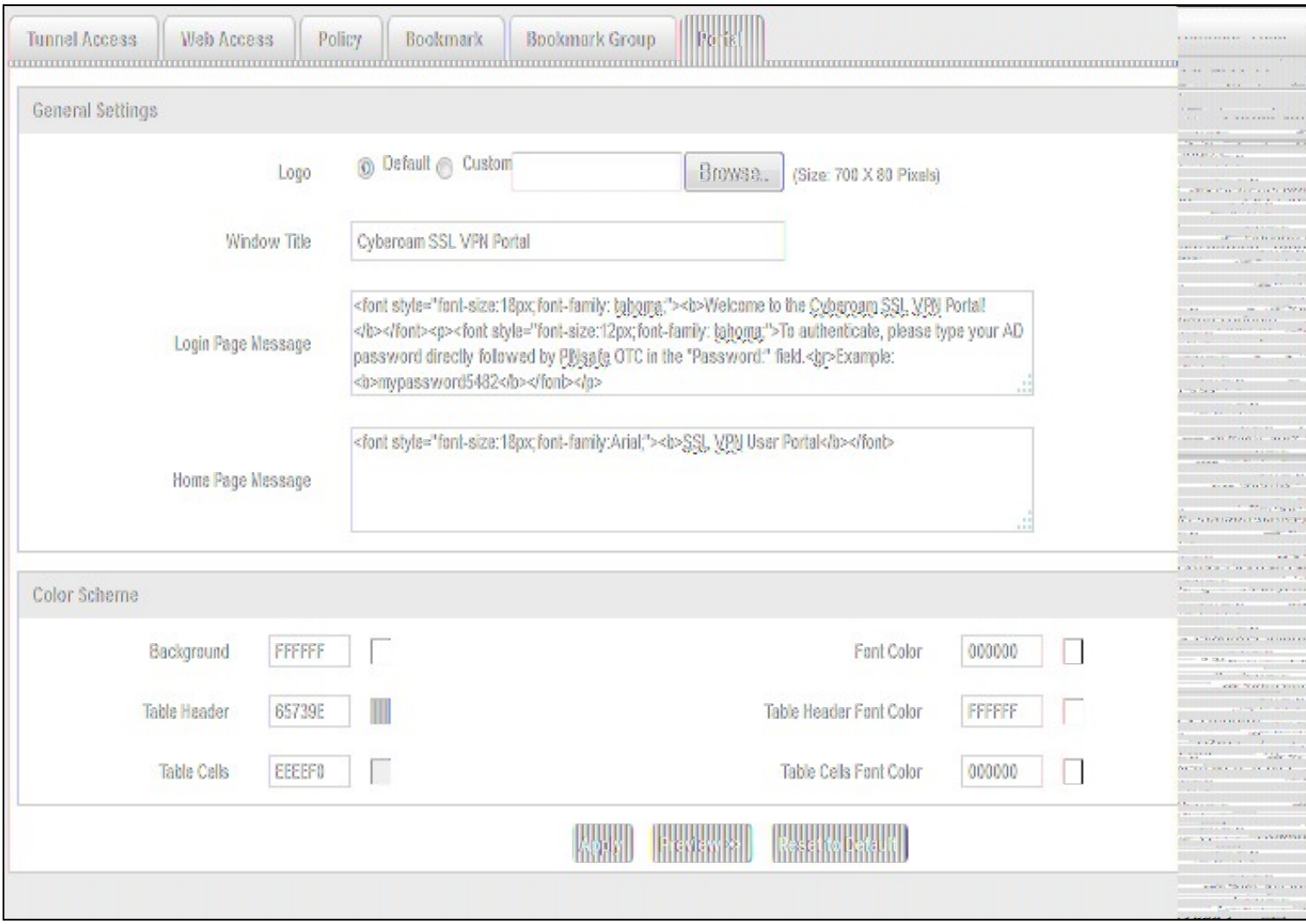
72.4.1 Configuring Authentication with AD Password and OTC

PINsafe can be configured to Check the password of supported repositories such as Active Directory. To do this the Check Password with repository must be enabled on the PINsafe server. PINsafe 3.7 and earlier have this as a global setting affecting all users, to select this option on the PINsafe Administration Console select Policy then Password, for PINsafe 3.8 onwards, it is defined by each NAS, under RADIUS then NAS. For more information see the Password How to Guide

The Password must be entered followed directly by the OTC on the login page by the user, e.g. passwordnnnn

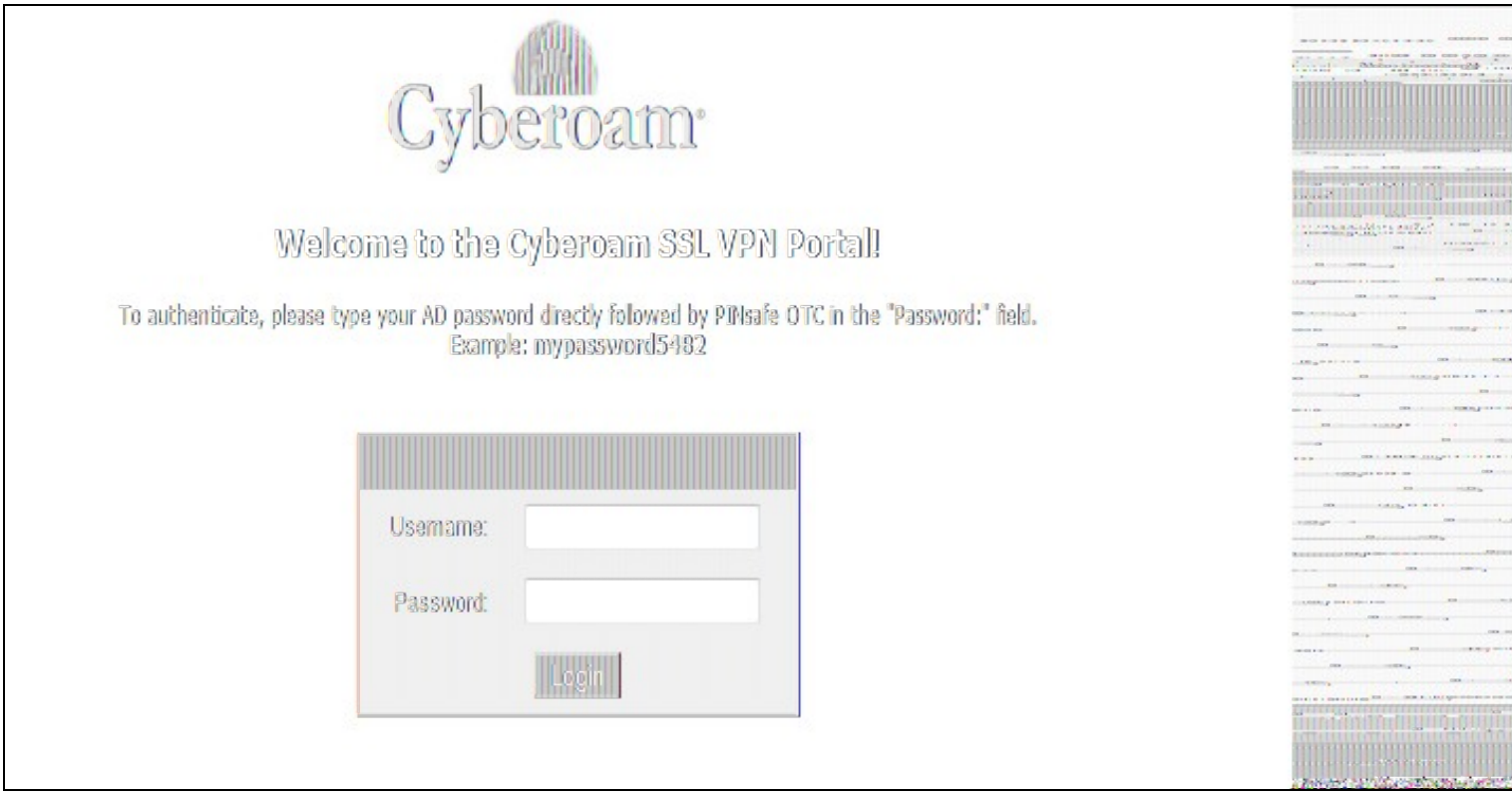
72.4.2 Modifying the Cyberoam login page

The Cyberoam login page can be modified to display different text and colours. To do this, on the Cyberoam Administration console select VPN, then SSL then select the Portal Tab. The below example shows modification for explianing how to add AD password and One Time Code.



72.5 Testing

Test authentication using a dual channel Security String or an image from the PINsafe Taskbar utility. The below example shows the combination of AD password with OTC for authentication.



72.6 Troubleshooting

Check the PINsafe logs for RADIUS requests.

72.7 Known Issues and Limitations

Dual Channel authentication and Taskbar only

72.8 Additional Information

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

73 Ericom PowerTerm WebConnect

74 Introduction

This article describes how to integrate Swivel with the PowerTerm WebConnect by Ericom using SMS, Mobile Client and the Taskbar utility. It is not possible to embed the Single Channel within the login page.

75 Prerequisites

Swivel 3.3

PowerTerm WebConnect

76 Baseline

Swivel 3.9

77 Architecture

Ericom PowerTerm WebConnect authenticates users by using RADIUS authentication against Swivel.

78 Installation

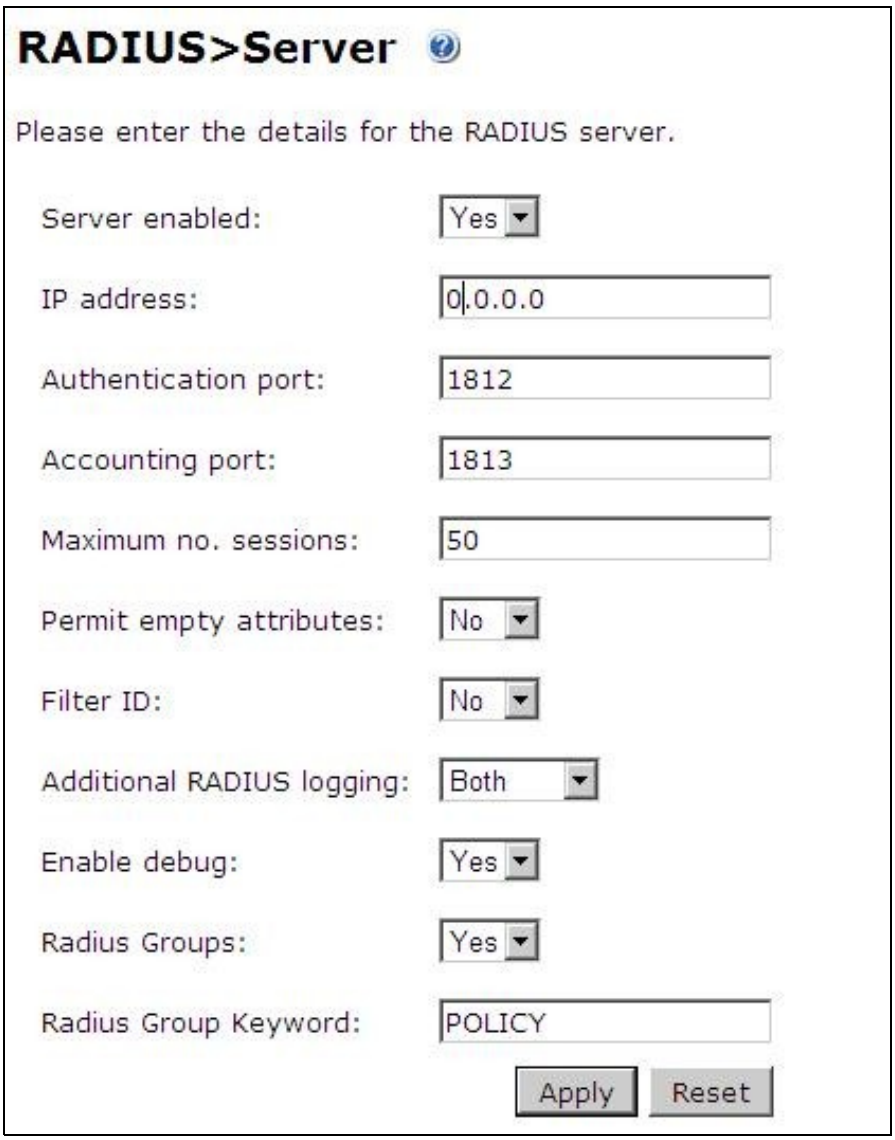
78.1 Swivel Integration Configuration

78.1.1 Configuring the RADIUS server

Configure the RADIUS settings using the RADIUS configuration page in the Swivel Administration console by selecting RADIUS Server. To turn on RADIUS authentication set **Server Enabled** to YES. The Host or IP address is the interface which will accept RADIUS requests, leave this blank (or use 0.0.0.0) to allow RADIUS requests on any interface.

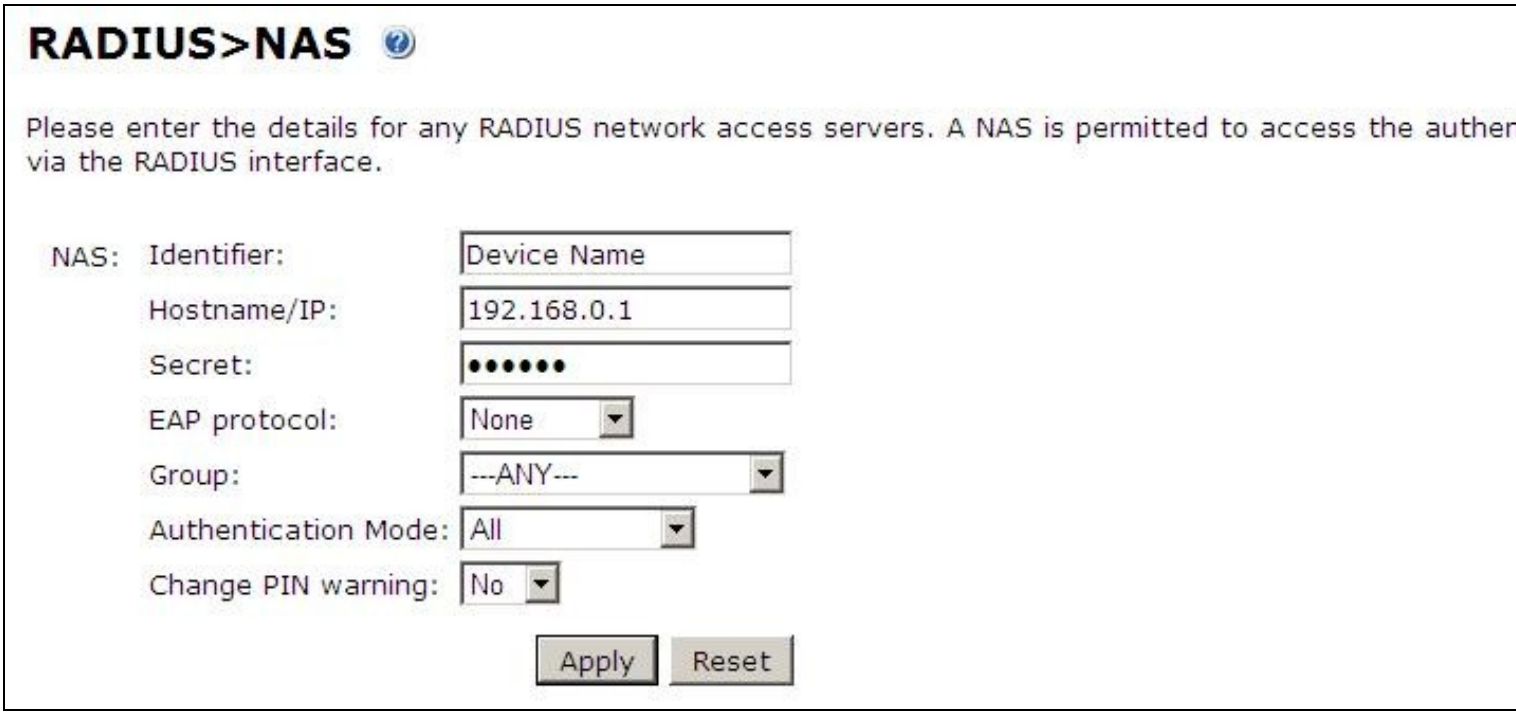
For troubleshooting RADIUS debug can be enabled together with the debug log option, see Debug how to guide

Note: for appliances, the Swivel VIP should not be used as the server IP address, see VIP on PINsafe Appliances



78.1.2 Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the Swivel Administration console. Enter a name for the VPN server. The IP address has been set to the IP of the VPN appliance, and the secret ?secret? assigned that will be used on both the Swivel server and VPN RADIUS configuration.



You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP are supported. All users will be able to authenticate via this NAS unless authentication is restricted to a specific repository group.

78.2 Ericom PowerTerm WebConnect Integration

78.2.1 RADIUS Server Configuration

Launch the PowerTerm WebConnect Administration Console and go to the Main Configuration (Files | Configuration | Main).

In the [ConnectionPoint=Internet] section set the option AuthenticationMethod=Radius.

This setting specifies that connections to this Connection Point will be authenticated with RADIUS.

Configure settings for the RADIUS connection

Radius_server Address of the Swivel RADIUS server

Radius_port (UDP) port that the Radius server is listening on. Default: 1812

Radius_sec_timeout timeout to wait for response from the Radius server. Default: 2

Radius_retries number of times to retry sending of the authentication request if a timeout occur. Default: 3

Radius_secret RADIUS server?s secret password as entered in the NAS section of Swivel.

Restart the PowerTerm WebConnect Server service.

78.2.2 Configuring Applications

Go to applicable published application?s Advanced section (applicable applications are those that will be used by users authenticating with RADIUS). Uncheck the option Use WebConnect User Credentials. Place %u in the Username field, and %X?Network Password? in the Password field.

Uncheck the option ?Use Default Domain?

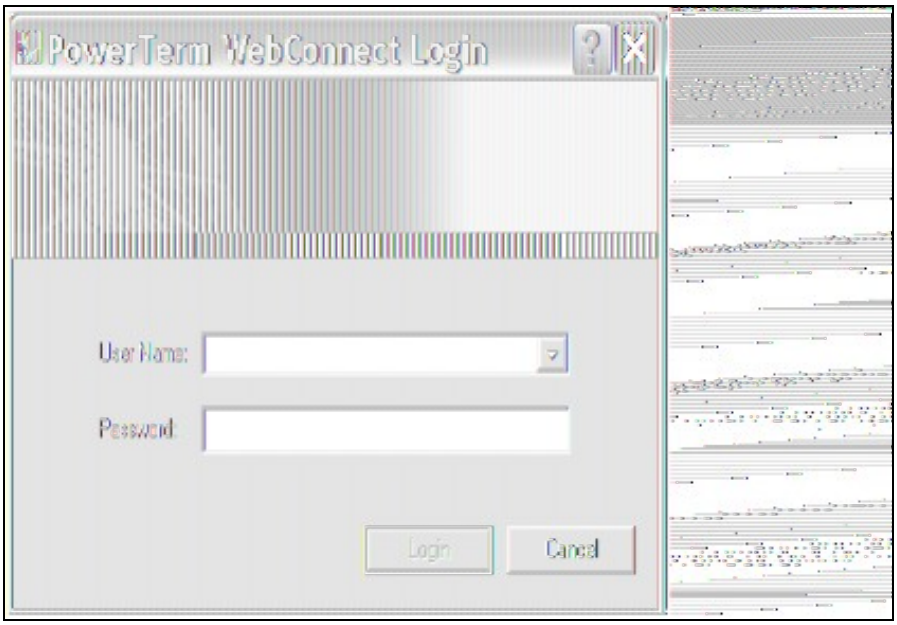
NOTE: Network Password should be entered exactly as is, do not replace the text with a user?s password. There needs to be a space between - ?Network? and ?Password?



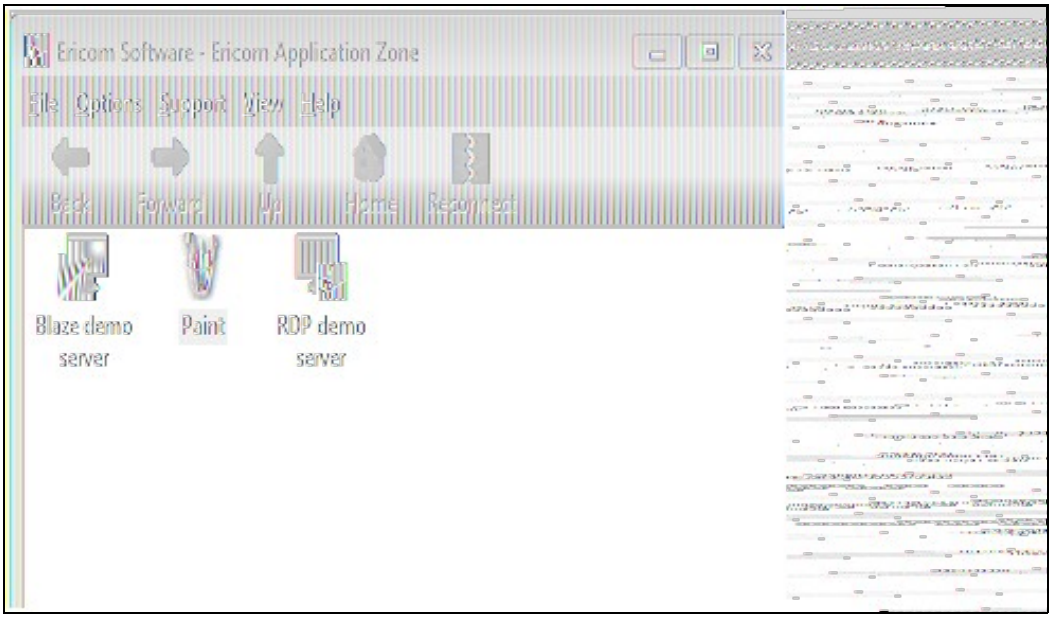
78.3 Additional Installation Options

79 Verifying the Installation

When users launch the Application Zone they will see the following screen, should log in with their username and Swivel One Time Code.



If the authentication is successful, the Application Zone will open displaying the users applications.



The first time the user launched an application, they will be prompted for their network password, as shown below.



The application will then open.

80 Uninstalling the Swivel Integration

Remove the RADIUS authentication for applications, check the option Use WebConnect User Credentials and remove the RADIUS server settings.

81 Troubleshooting

82 Known Issues and Limitations

83 Additional Information

84 Category:F5

85 Fortinet Fortigate Integration

86 Introduction

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

87 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.

88 Baseline

Fortinet 3.x

Fortinet 4.x

Fortinet 6.x

Swivel 3.x

Swivel 4.x

89 Architecture

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

90 Swivel Configuration

90.1 Configuring the RADIUS server

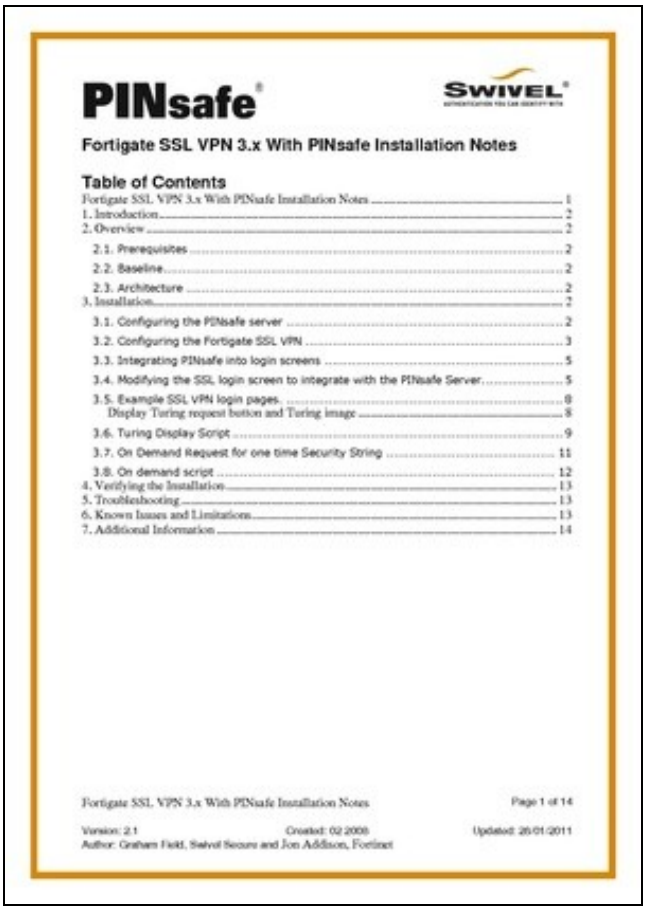
On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

90.2 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.

91 Fortinet Fortigate Configuration

91.1 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

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

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

91.2 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)

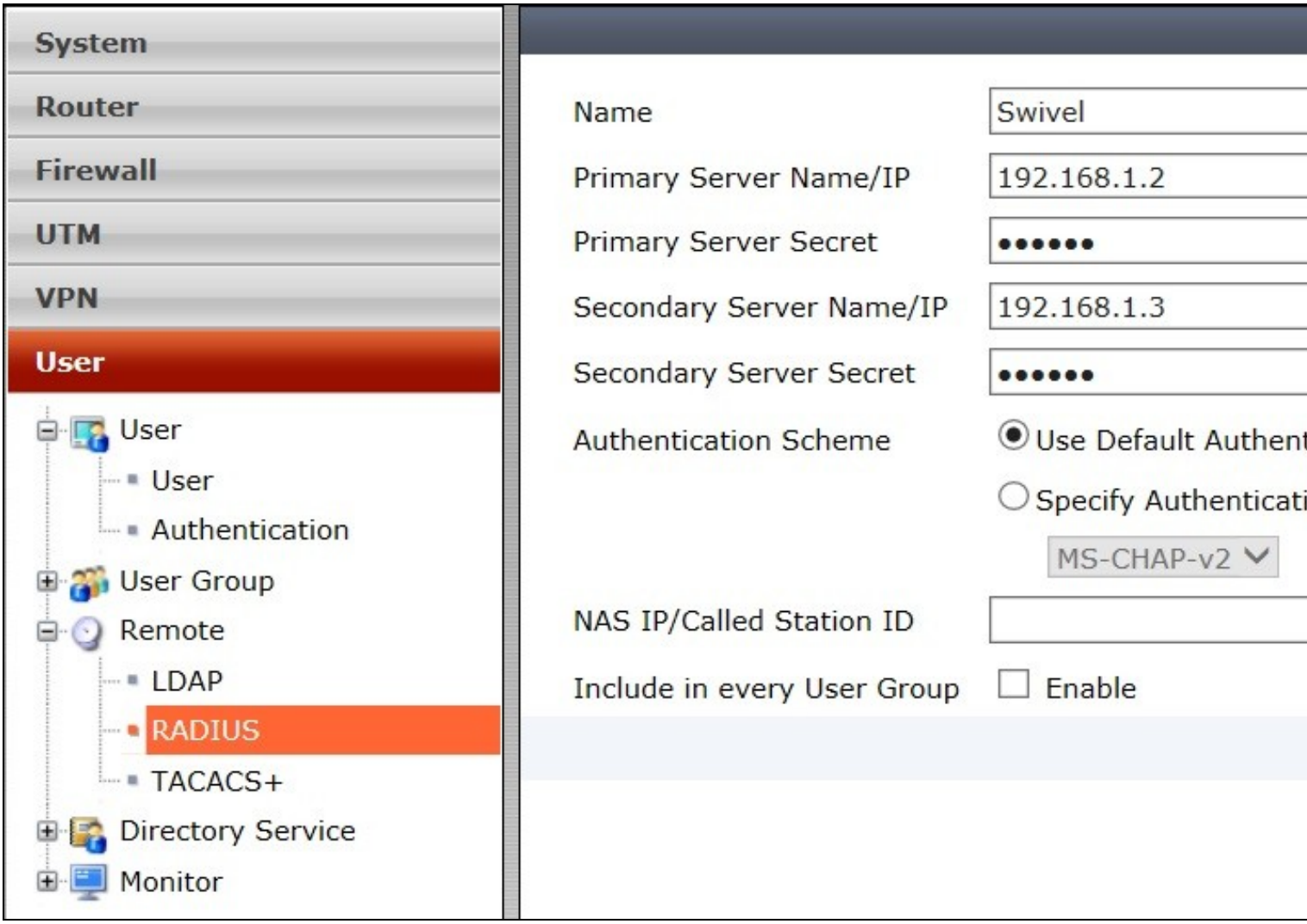
Primary Server Secret The shared secret entered on the Swivel RADIUS NAS

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

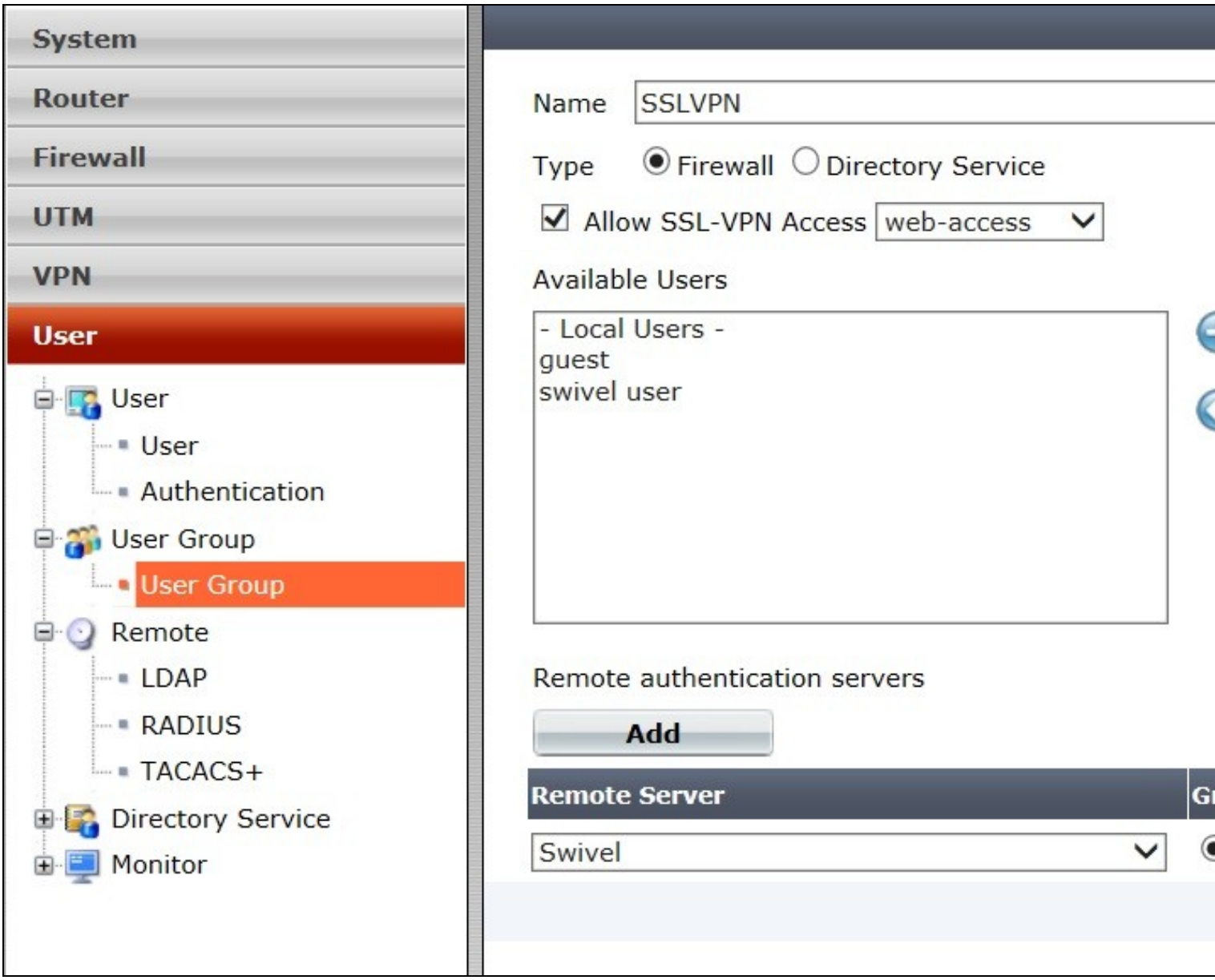
Authentication Scheme leave as Use Default Authentication Scheme unless Mobile App authentication or Check Password With Repository is used, in which case this should be set to use PAP.

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.

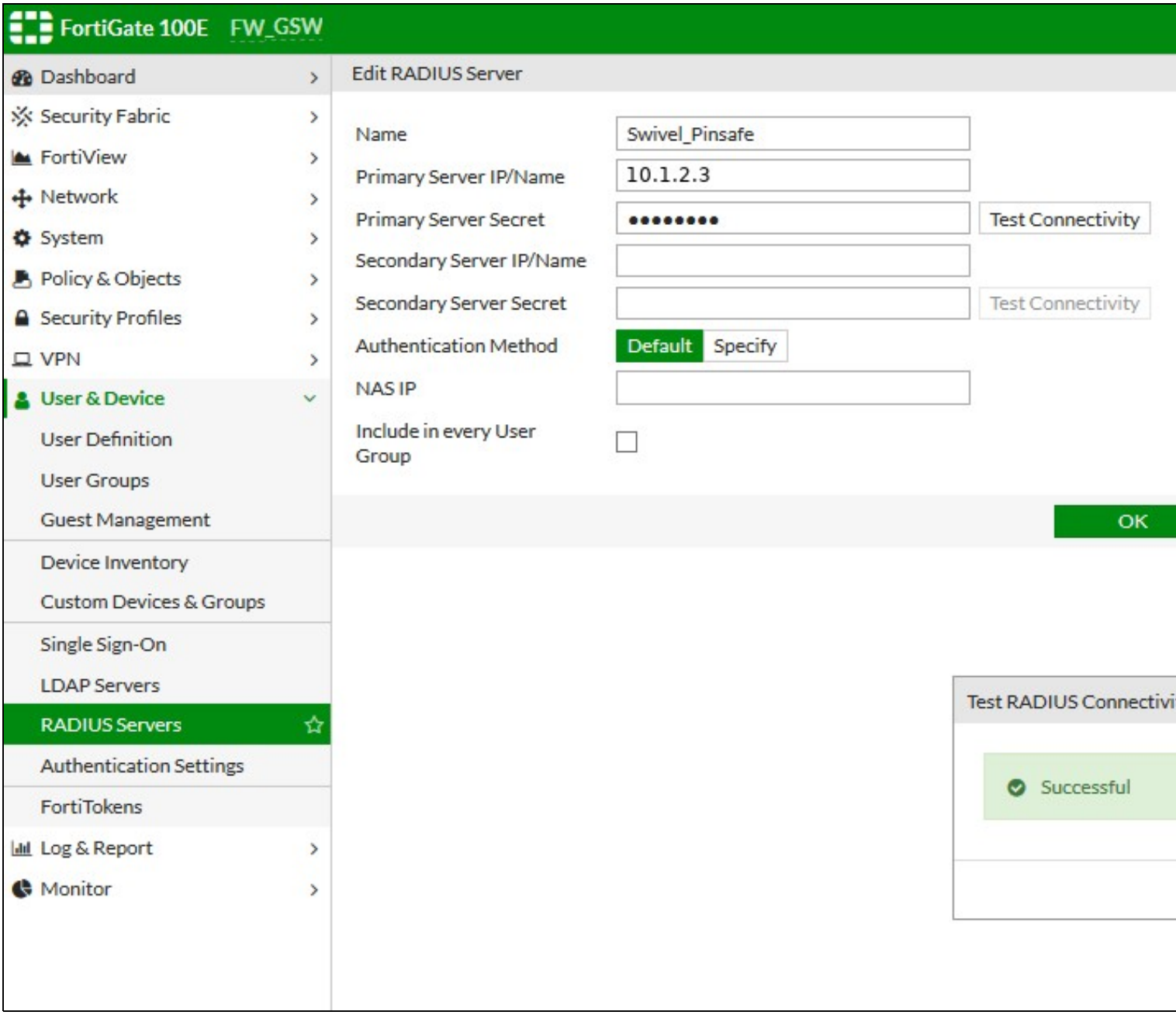
When multiple authentication servers are used, the Fortigate will use the username and password or One Time Code against each starting with local, until a successful authentication is made.



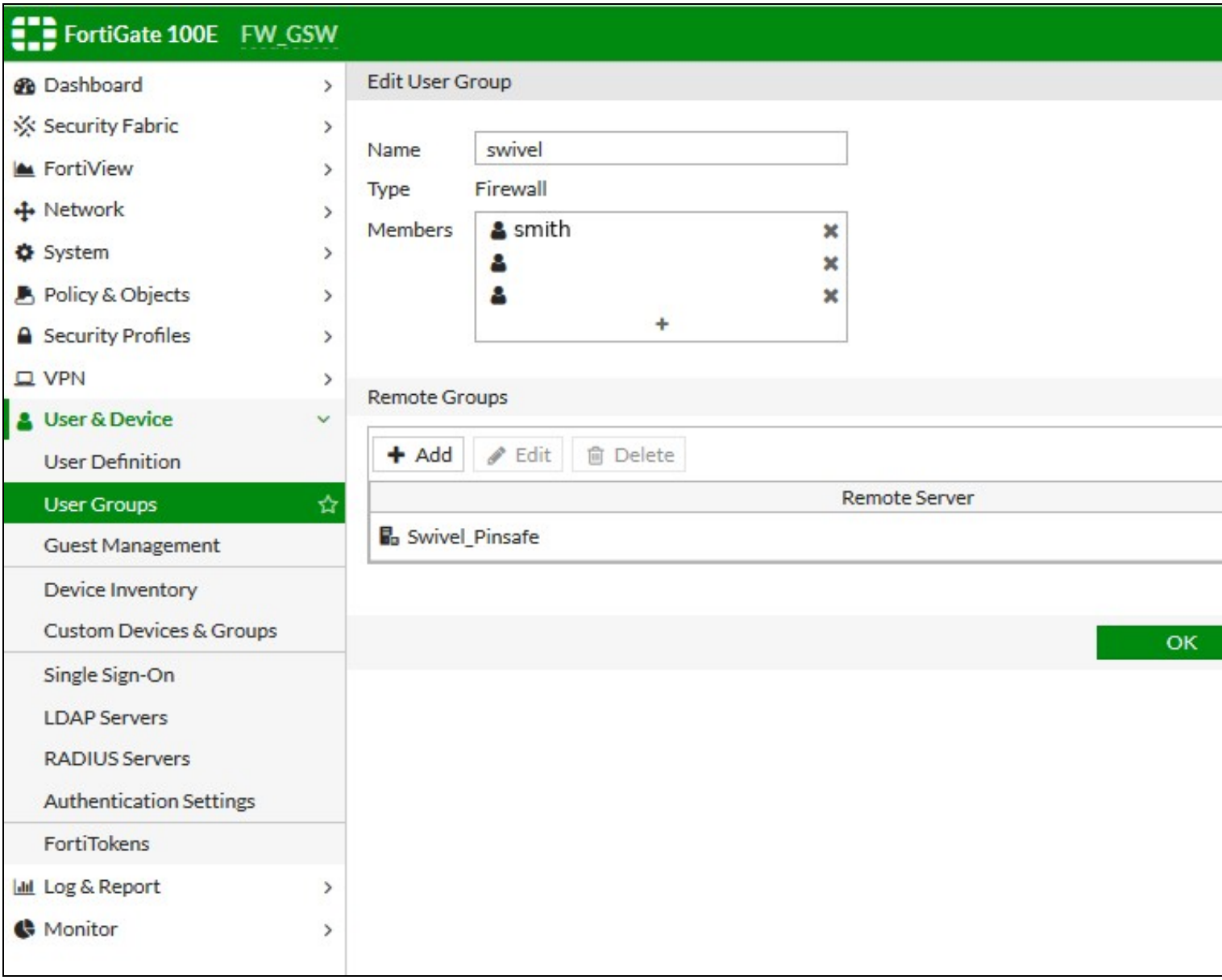
91.3 Fortinet Fortigate Version 6.x Integration guide

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.

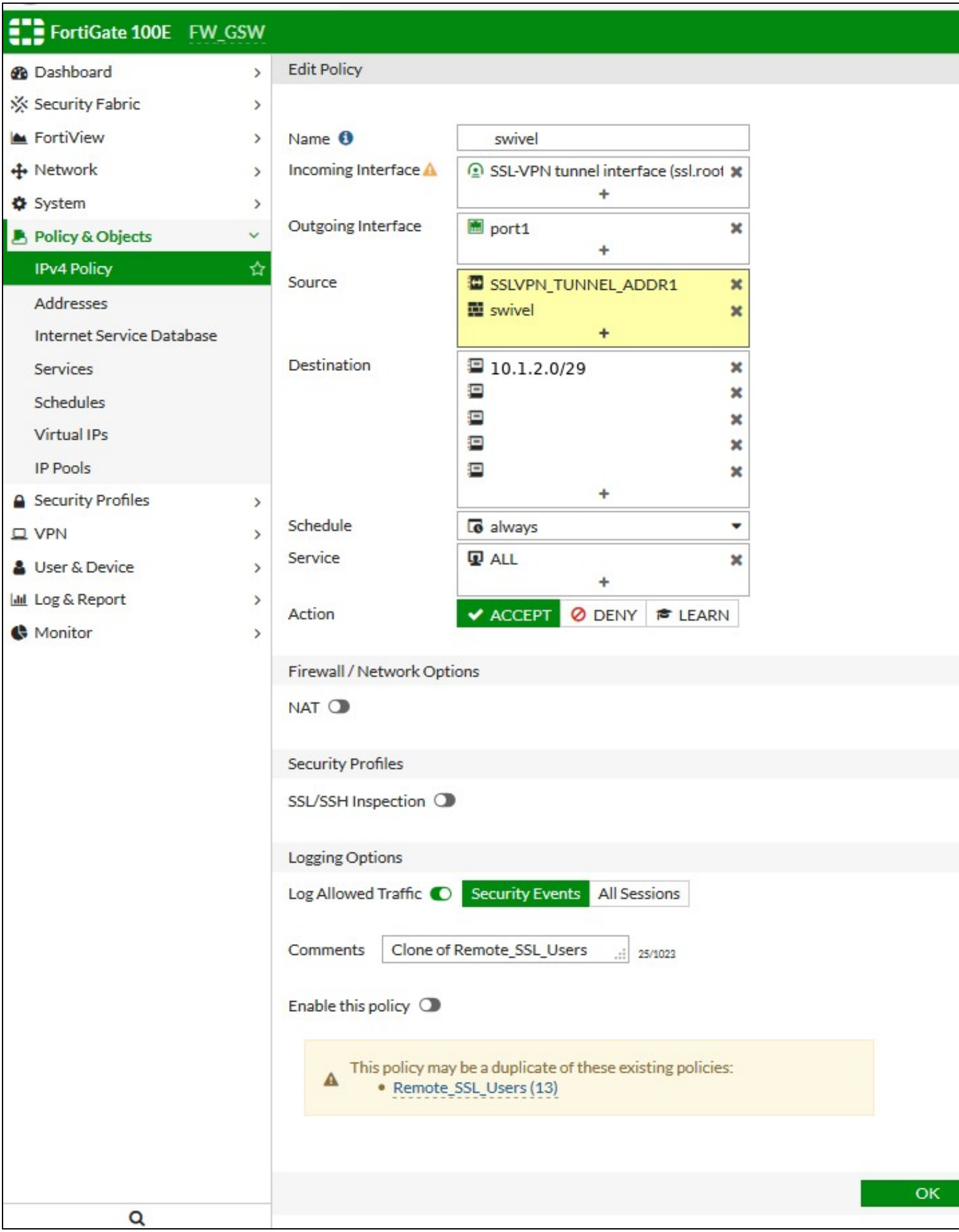
For further information regarding Fortinet FortiOS 6: https://docs.fortinet.com/uploaded/files/4328/fortios-v6.0.0-release-notes.pdf



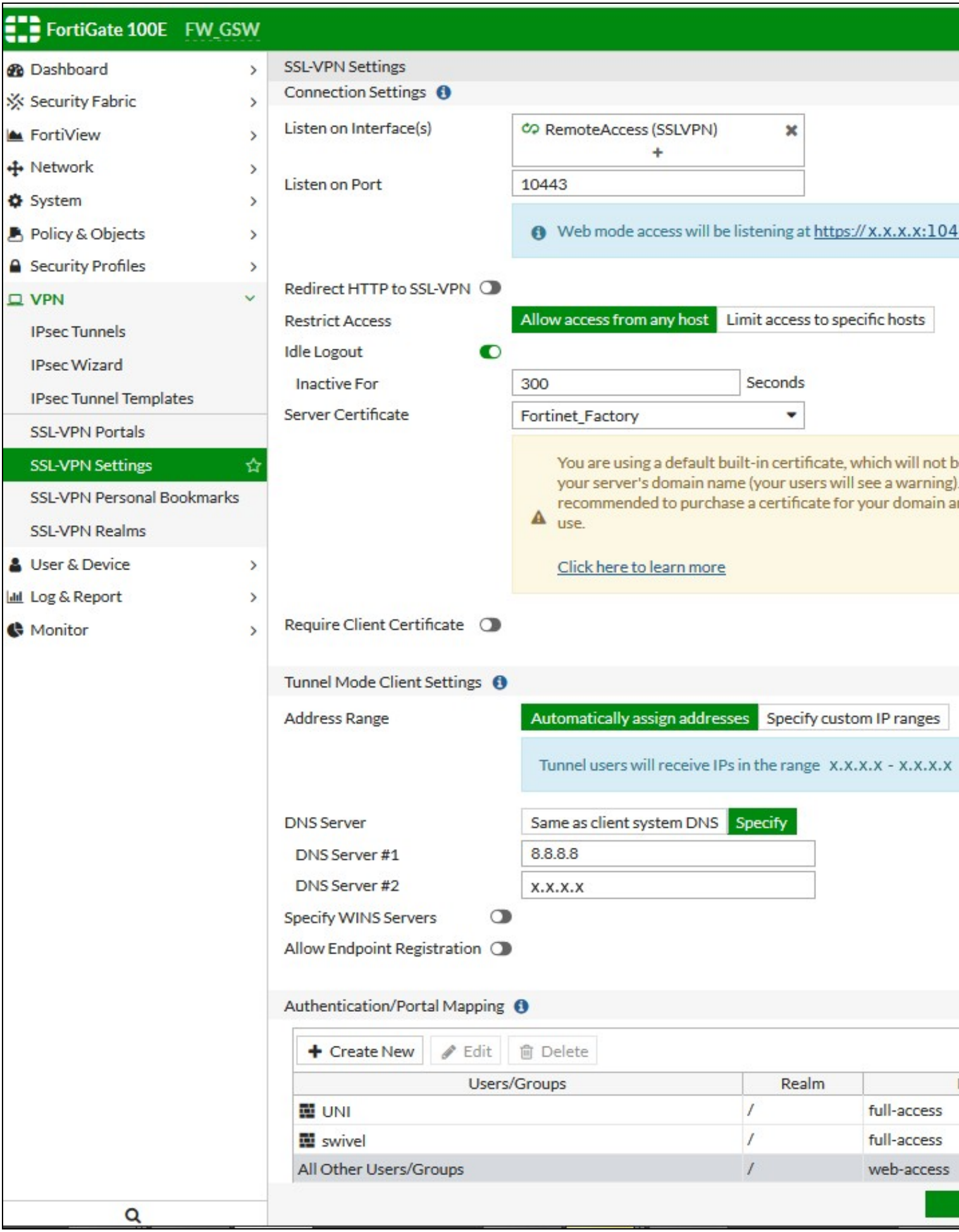
Select Radius Servers, create a Swivel Radius Server to bind to the the Appliance and test the connection. After create a user group for Swivel.



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

91.4 Test the RADIUS authentication

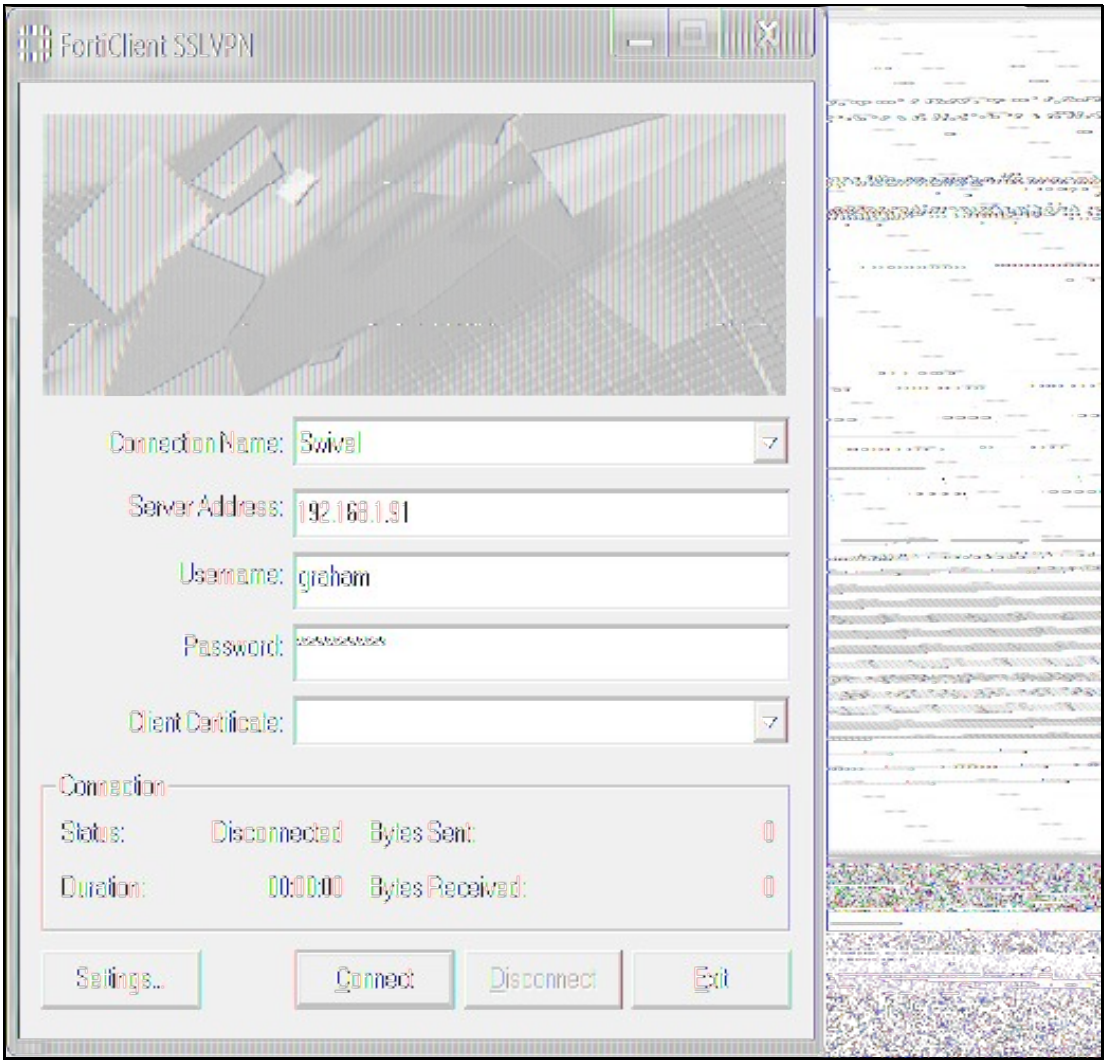
At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select 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.

92 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

92.1 Forticlient

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



92.2 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:

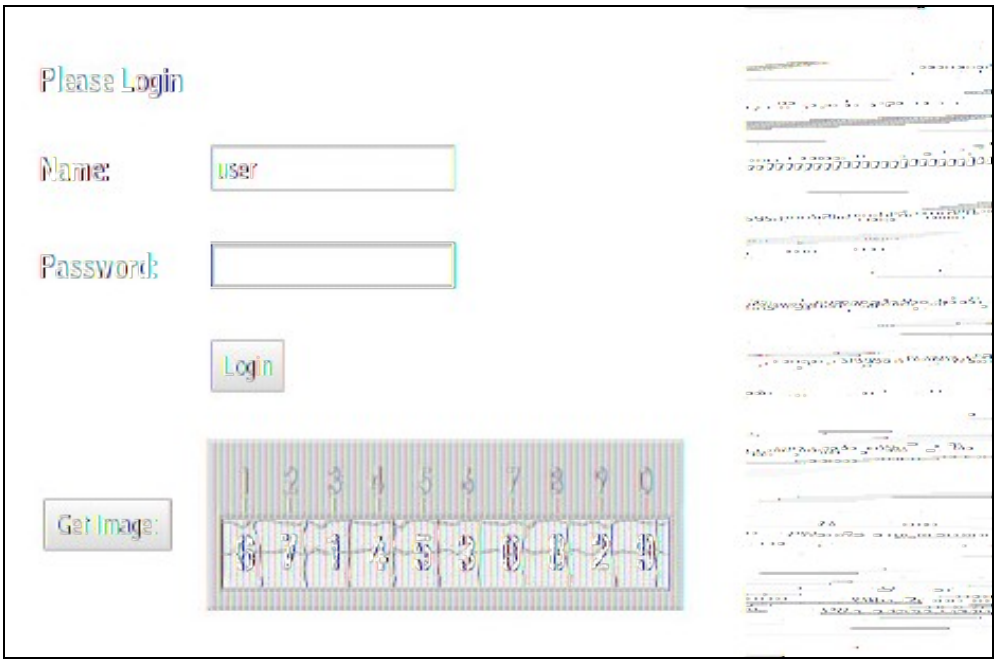
var sUrl="https://192.168.1.3:8443/proxy/SCImage?username=";

For a software only install see Software Only Installation

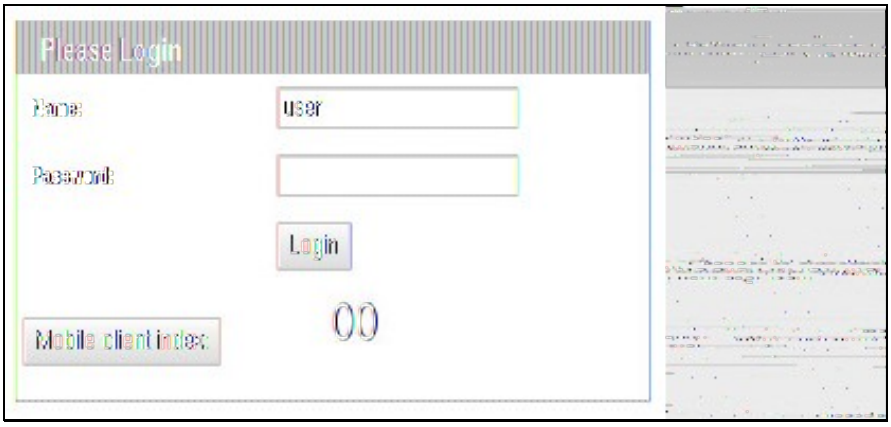
93 Testing

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



94 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

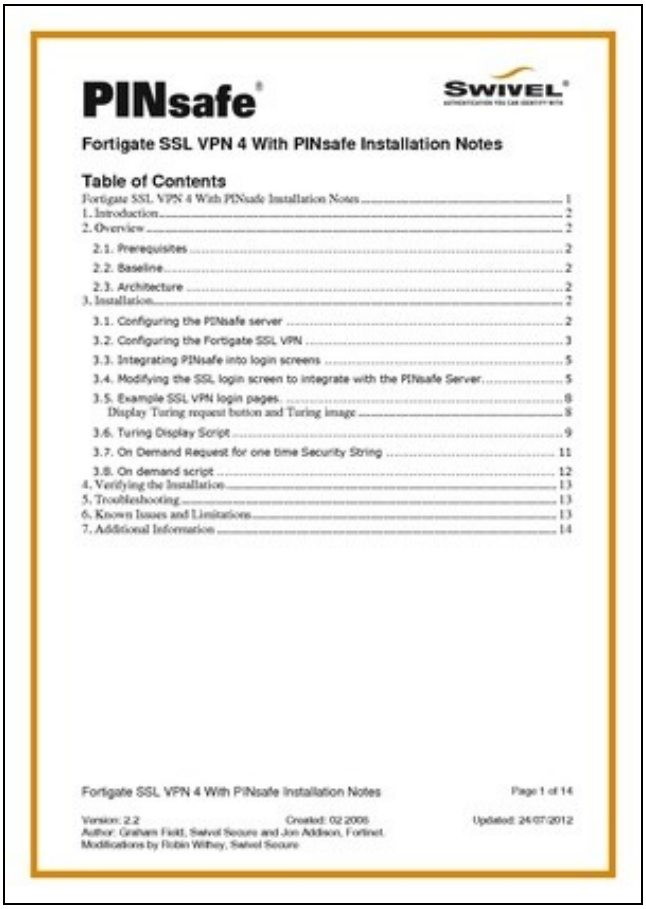
Login page modifications absent

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.

95 Known Issues and Limitations

None

96 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

Fortigate SSL VPN 4 With PINsafe Installation Notes Page 1 of 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

97 Category:Google

98 HOB Remote Desktop VPN

99 Introduction

This document outlines the integration of PINsafe with the HOB Remote Desktop VPN.

100 Prerequisites

PINsafe 3.x

HOB RD VPN WebSecureProxy

If the graphical single Channel image is to be used, then the image must be accessible by the client from the internet, this is usually done by a NAT to the PINsafe server.

HOB RD VPN WebSecureProxy PINsafe Integration files

101 Baseline

PINsafe 3.7

HOB RD VPN WebSecureProxy 2.2 0108

102 Architecture

Users connect to the HOB RD VPN WebSecureProxy login page and enter their username and One Time Code. The authentication information is sent to the PINsafe server by RADIUS. RADIUS ChangePIN and Two Stage Challenge and Response authentication are also supported through RADIUS.

103 Swivel Configuration

103.1 Configuring the RADIUS server

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

103.2 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.

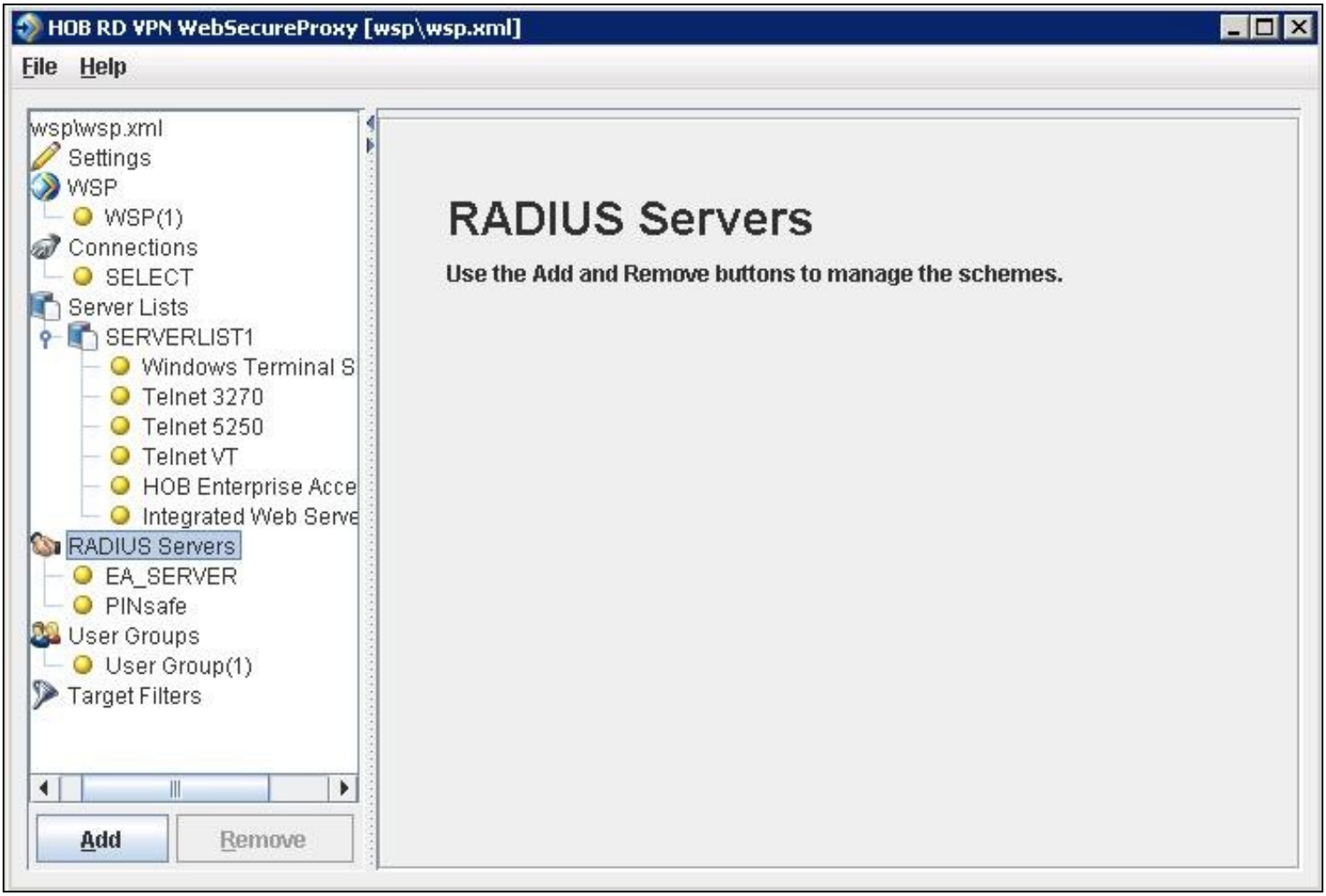
103.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

104 HOB RD VPN WebSecureProxy Integration

104.1 Create a RADIUS Server

On the HOB RD VPN WebSecureProxy Administration Configuration select RADIUS Servers then Add.



Enter the details for the PINsafe RADIUS server, the following information is required:

Name: A descriptive name such as PINsafe

Host IP Address: The hostname or IP address of the PINsafe server

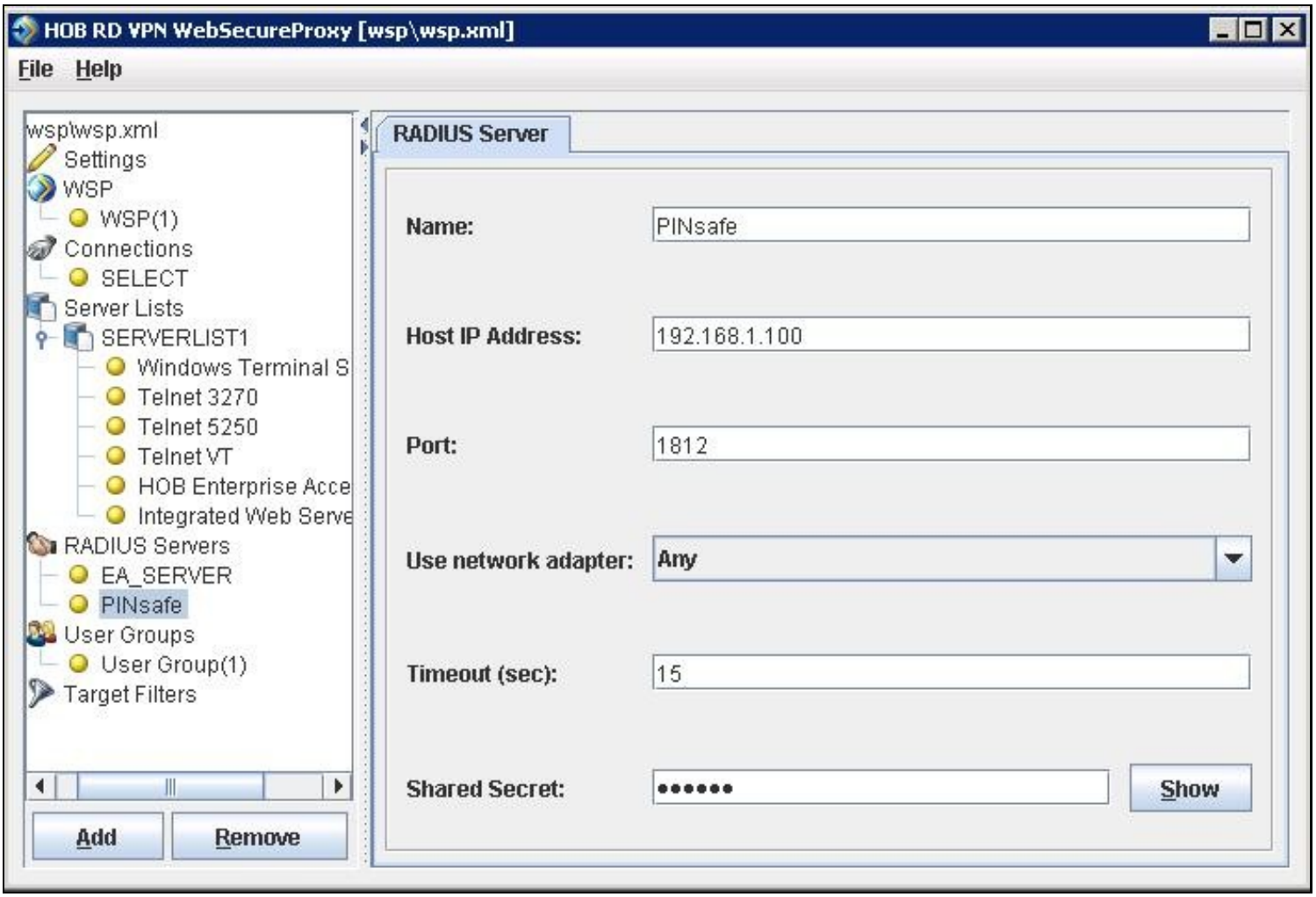
Port The port used for RADIUS authentication on the PINsafe server, usually 1812

Use network adapter: The network adapter from which authentication requests are sent from.

Timeout (sec): The length of time to wait for a RADIUS authentication attempt fails.

Shared Secret: A value that is also entered and must match on the PINsafe RADIUS NAS.

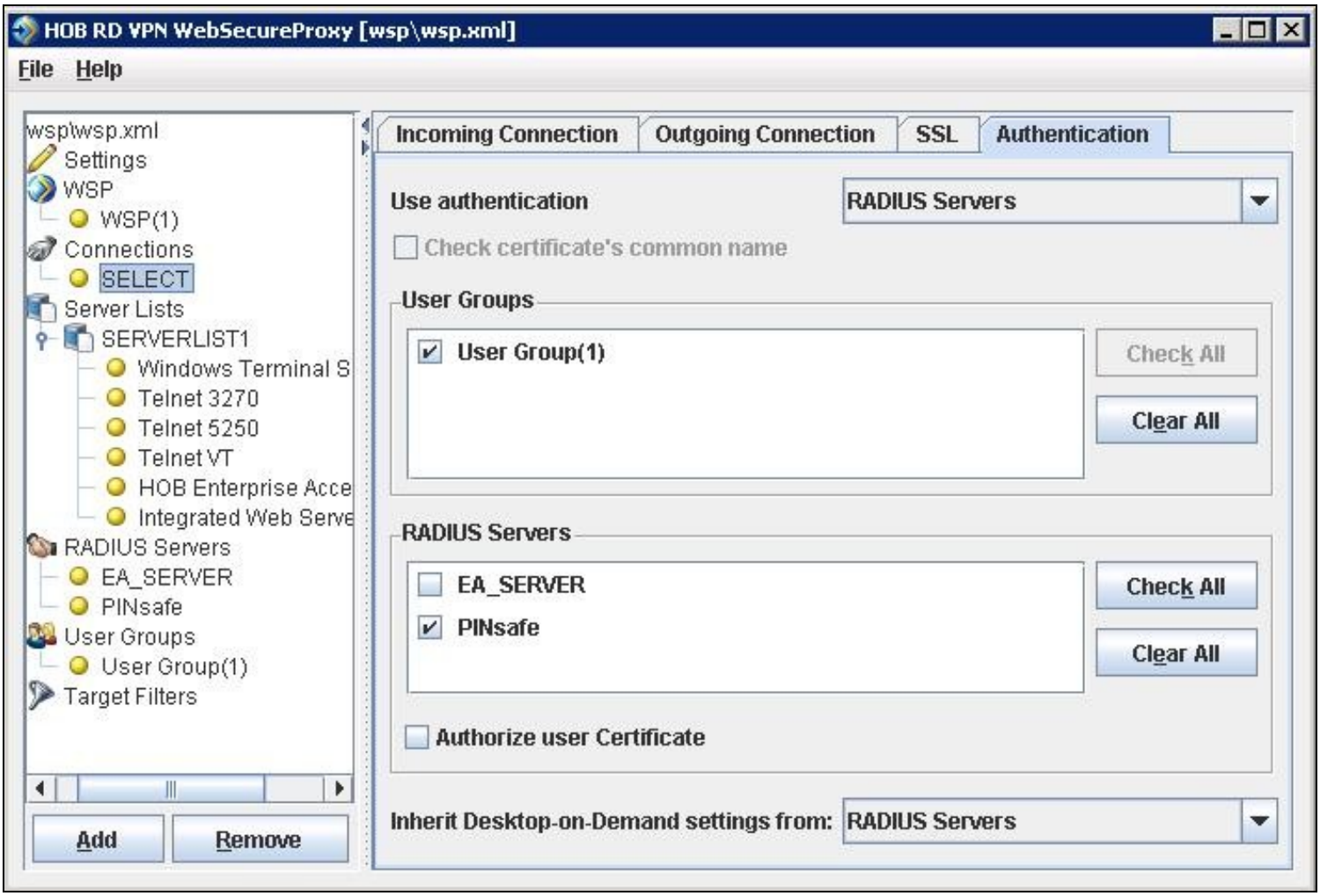
When complete click on File, then Save. For settings to take affect the HOB WebSecureProxy may need to be restarted.



104.2 Assign the PINsafe RADIUS server to a Connection

On the HOB RD VPN WebSecureProxy Administration Configuration select Connections, then the name of the required connection, then select the Authentication tab. Set the Use authentication to RADIUS and ensure that the PINsafe RADIUS server is selected.

When complete click on File, then Save. For settings to take affect the HOB WebSecureProxy may need to be restarted.



104.3 Additional Installation Options

104.3.1 Single Channel, Index and Message request

The HOB RD VPN WebSecureProxy will now be configured to allow authentication for Dual channel such as SMS and mobile phone applet. To configure additional options such as the graphical single channel image, and the security string index the login page must be modified. See also Multiple Security Strings How To Guide

Edit the pinsafe.js file and change the IP address of the PINsafe server to be that of the public NAT address of the PINsafe server.

```
pinsafeUrl = "http://192.168.1.100:8443/proxy/";
```

For a Swivel virtual or hardware appliance this will usually need to be: pinsafeUrl = "https://192.168.1.100:8443/proxy/";

For a software only install see Software Only Installation

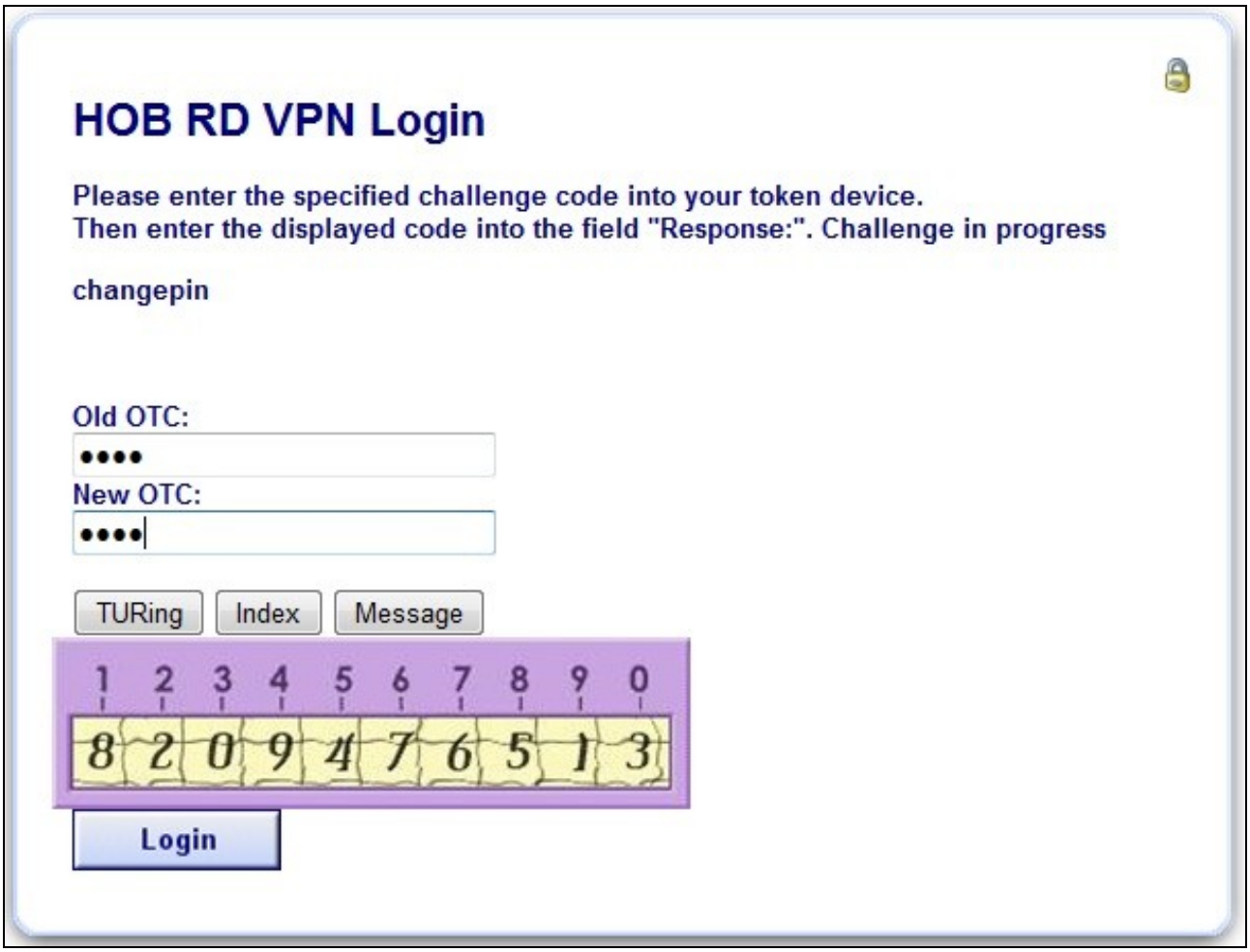
Backup the original files and then upload the modified files and login pages to the Hob RD VPN server, <path to install>\HOB\rdvpn\www\login

The default installation path is: c:\Program Files\HOB\rdvpn\www\login

For changes to the login page to take effect the HOB WebSecureProxy may need to be restarted.

104.3.2 Change PIN

To enable ChangePIN, on the PINsafe administration console select RADIUS/NAS then set ChangePIN Warining to Yes. Upload the modified login pages as detailed above. When a user is required to change their PIN they are automatically redirected to the ChangePIN page. Remember that the PIN number is never entered during the changePIN process, instead old and new one time codes are entered. A user may use SMS or tthe mobile phone to change their PIN. If a PINsafe password is being used, they must use <password><OTC>.



104.3.3 Challenge and Response and Two Stage Authentication

To enable Challenge and Response and Two Stage Authentication:

1. Upload the modified login pages as detailed above.

2. On the PINsafe administration console select RADIUS/NAS then set Two Stage Auth to Yes.

3. On the PINsafe administration console select RADIUS/Server and set Use Challenge/Response to Yes.

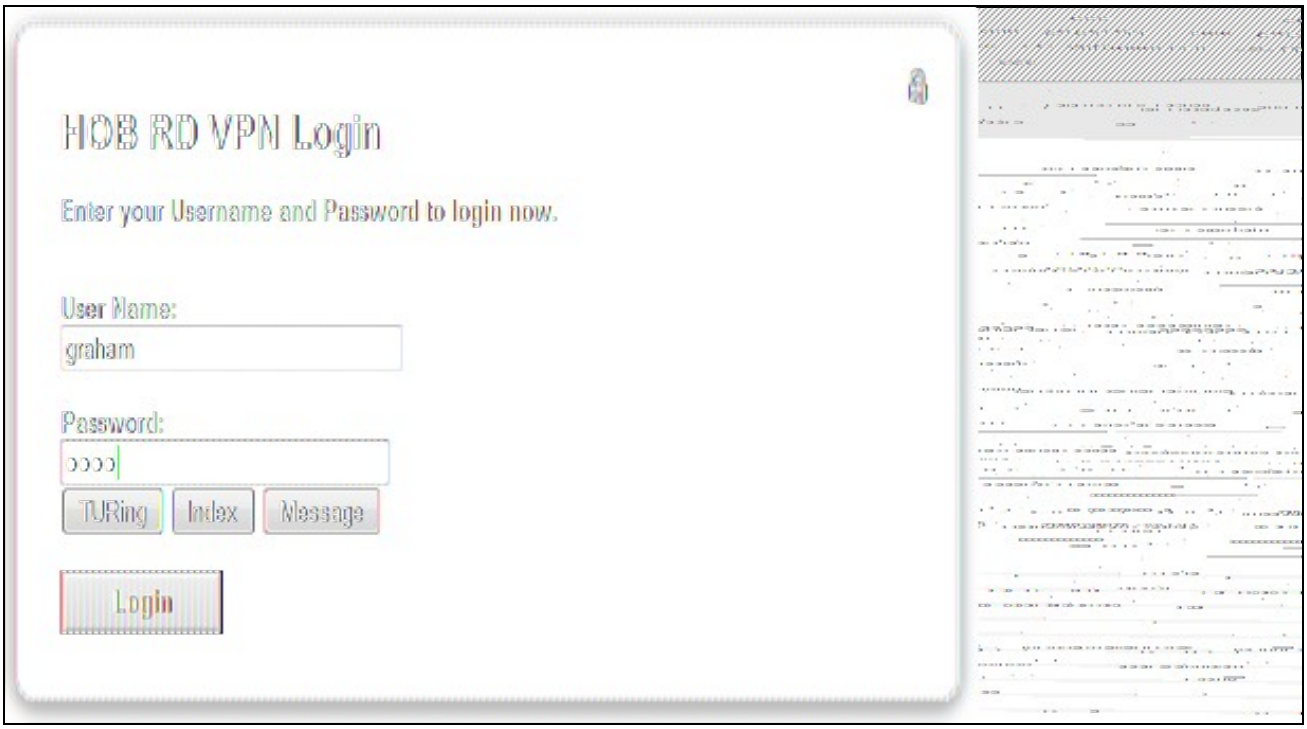
4. On the PINsafe administration console select Policy/Password and set Require Password to Yes, and Check Password with Repository to Yes. In PINsafe 3.8 this option is located under RADIUS/NAS.

When a user logs in they will be prompted to enter their password, and if correct will be redirected to another page where they can enter their one time code. The Challenge and Response option allows the user to be sent an SMS message on a correct password being entered.

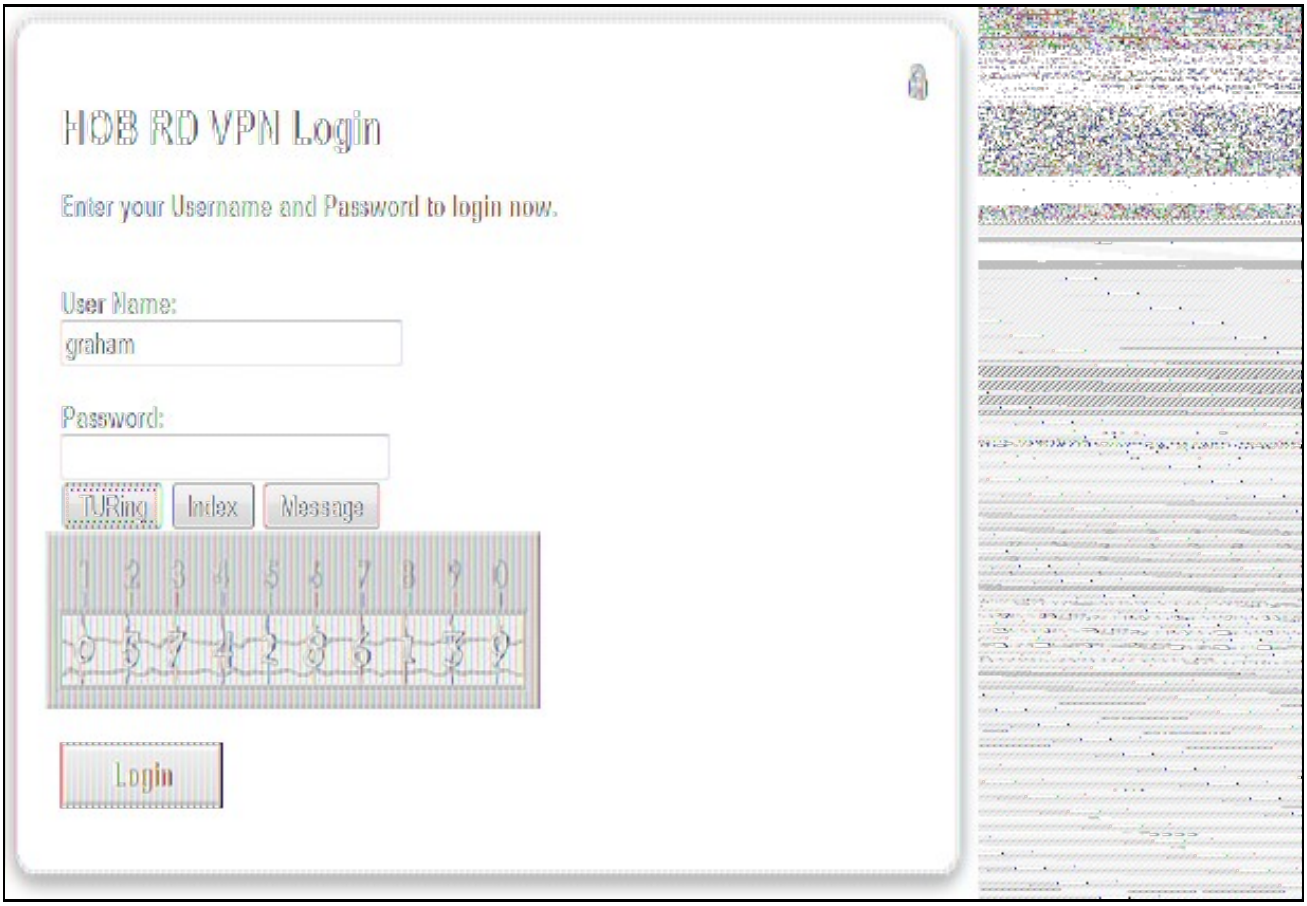
105 Verifying the Installation

Attempt a login using the username and One Time Code.

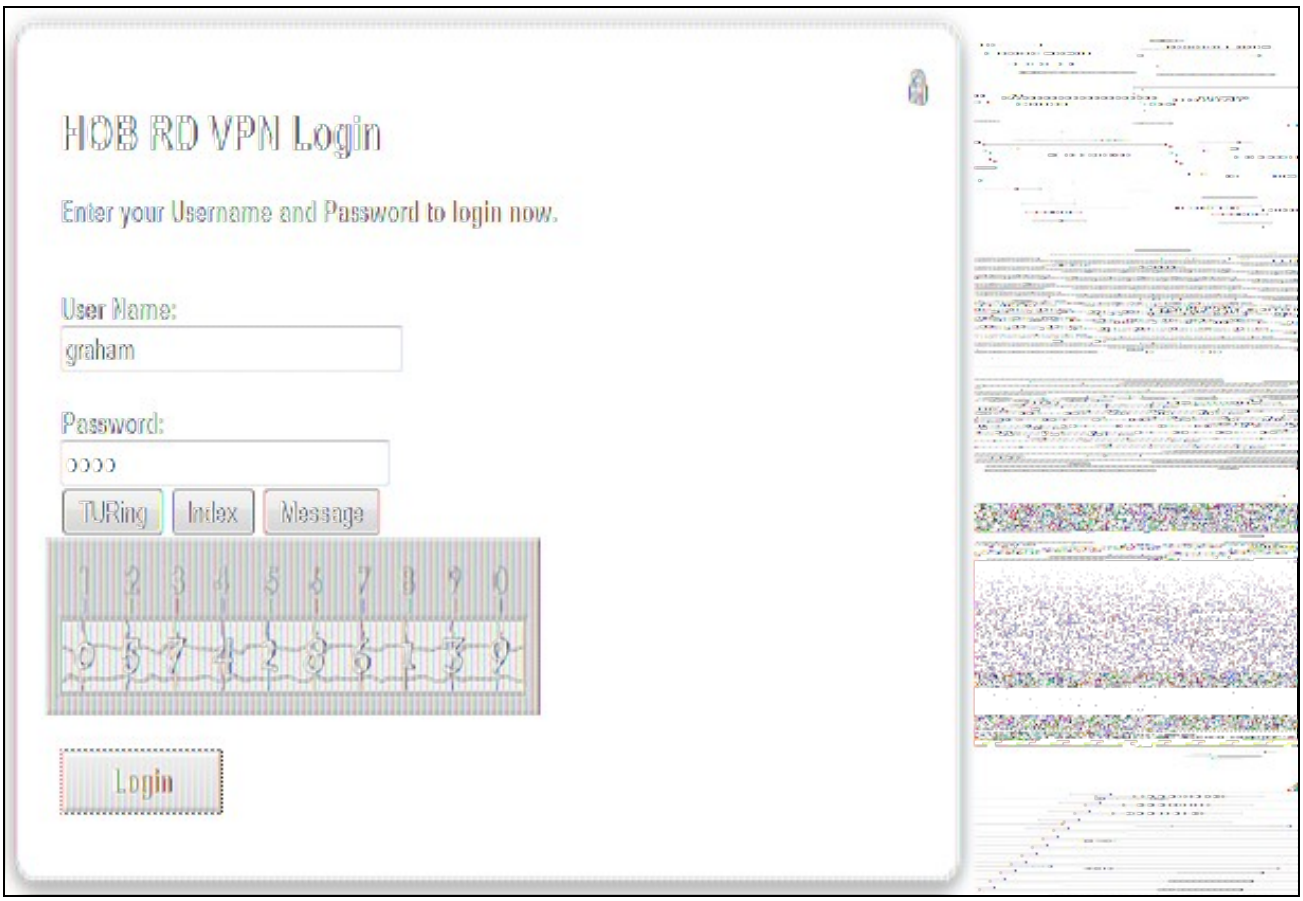
For the dual channel login using SMS or mobile phone applet, enter the username, and then the One Time Code. Do not click on the TURing button. If the Message button has been added, then this can be used to request a new SMS message after the username has been entered.



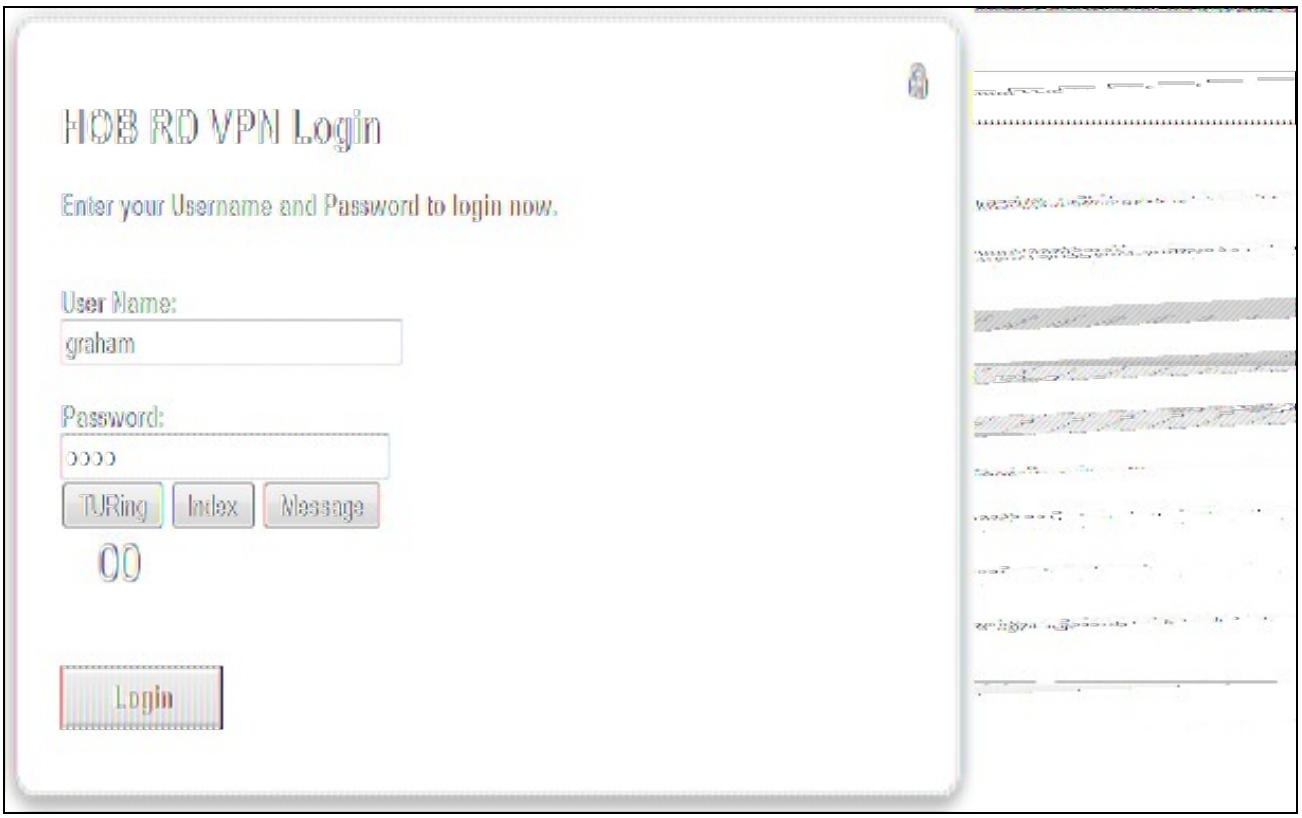
For the Single Channel authentication enter username and click on TURing.



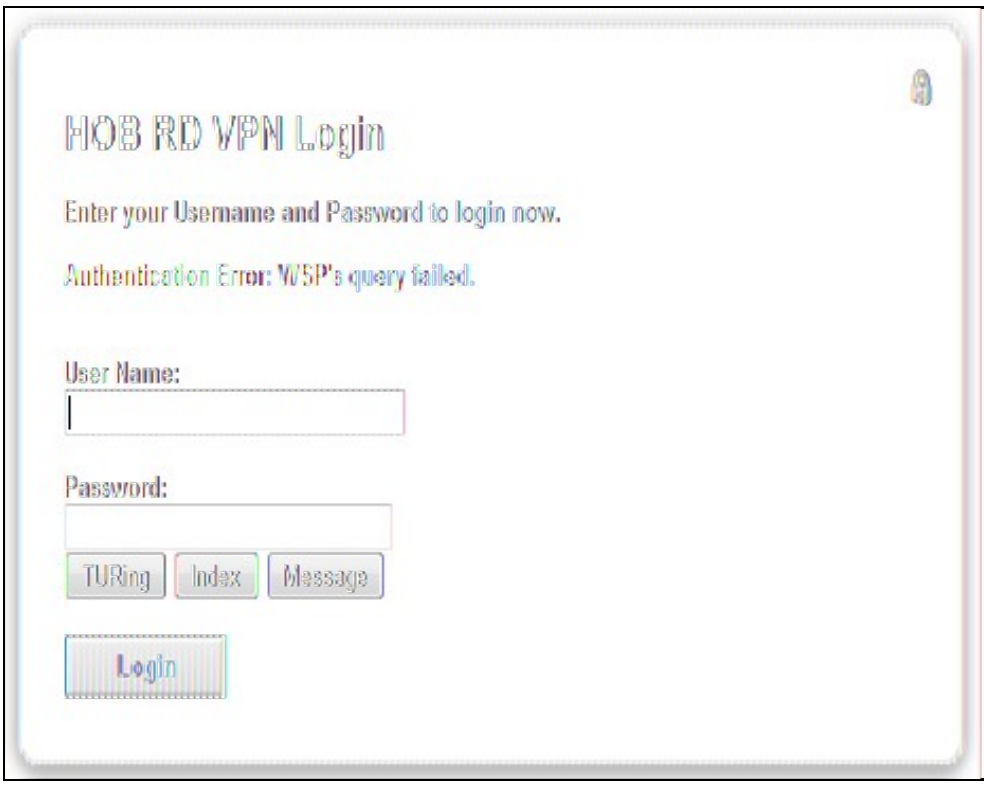
Enter the One Time Code then click on login.



If multiple Security Strings are being sent by SMS, then the string index can be requested to tell the user which security string should be used. Enter the username then click on Index. Enter the one time code associated with that number.



Verify that entering an incorrect one time code fails an authentication.



106 Uninstalling the PINsafe Integration

Copy the original files back on the HOB RD VPN server, and remove the PINsafe RADIUS server from the HOB RD VPN WebSecureProxy. Remove the PINsafe RADIUS server entry under RADIUS Servers.

107 Troubleshooting

Check the PINsafe logs for error messages. Specifically look for RADIUS requests to see if they are reaching the PINsafe server and Session Started messages to verify Single Channel images are being requested where used.

108 Known Issues and Limitations

109 Additional Information

110 Category:Joomla

111 Category:Juniper

112 Category:Mcafee

113 Meraki

113.1 Overview

Meraki is a cloud-based managed wi-fi solution. http://www.meraki.com/

This article explains how you can add Swivel Authentication to the wifi authentication process.

The integration is possible because Meraki allows for two features:-

- RADIUS Authenetication
- The ability to direct a user to a specified URL

113.1.1 Security

The wireless connection uses PAP as the authentication method when you are using the Sign-on Splash page feature. With PAP, user credentials are sent in plain text. However, in a Meraki network, user credentials are encrypted in an SSL tunnel when sent from the clients web browser to the Meraki Cloud Controller. The Meraki Cloud Controller acting as the RADIUS client sends the username and password along with other connection specific data in a RADIUS Access-request to the PINsafe RADIUS server you specified in Dashboard. For security, the Meraki Cloud Controller encrypts the password using the RADIUS shared secret and an XOR function. This ensures the users password is never transmitted in plain text.

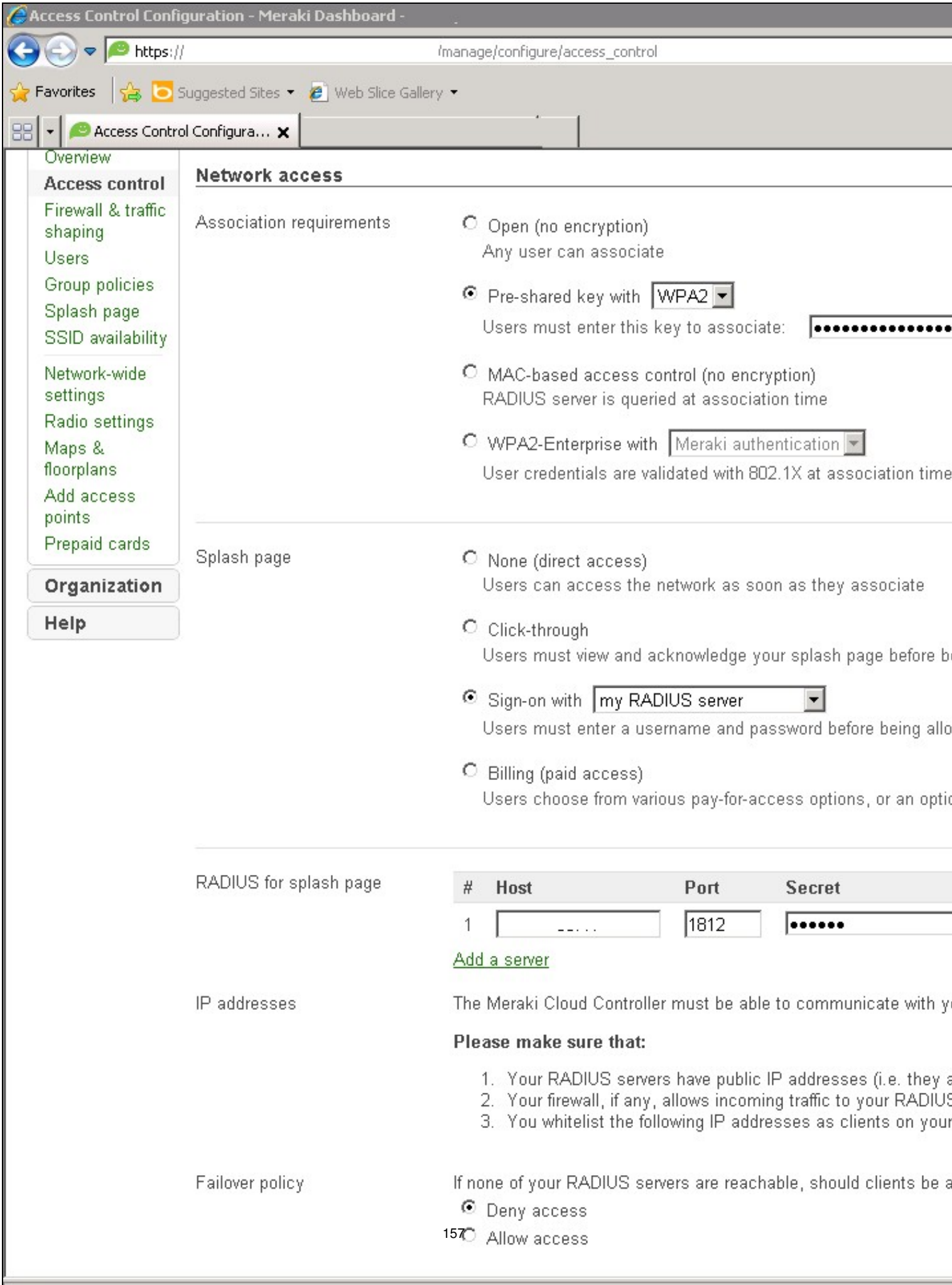
113.2 Meraki Configuration

There are two settings specifc to this integation, setting RADIUS for authentication and setting the url of the custom login page.

Firstly on the access control page you need to specify that authentication to this network will be via RADIUS. You need to enter the host name/ip address of the Swivel server and enter a shared secret.

Note that the Swivel server needs to be accessible on the RADIUS port via the internet for the integration to work.

Also you need to create a NAS entry on the Swivel Server that matches that of the Meraki entry. The Meraki config page lists the possible source IP addresses.


Access Control Configuration - Meraki Dashboard -
https://
/manage/configure/access_control
Favorites
Suggested Sites
Web Slice Gallery
Access Control Configura...
Overview
Access control
Firewall & traffic shaping
Users
Group policies
Splash page
SSID availability
Network-wide settings
Radio settings
Maps & floorplans
Add access points
Prepaid cards
Organization
Help
Network access
Association requirements
Open (no encryption)
Any user can associate
Pre-shared key with WPA2
Users must enter this key to associate:
MAC-based access control (no encryption)
RADIUS server is queried at association time
WPA2-Enterprise with Meraki authentication
User credentials are validated with 802.1X at association time
Splash page
None (direct access)
Users can access the network as soon as they associate
Click-through
Users must view and acknowledge your splash page before b
Sign-on with my RADIUS server
Users must enter a username and password before being allo
Billing (paid access)
Users choose from various pay-for-access options, or an optio
RADIUS for splash page
Host Port Secret
1 1812
Add a server
IP addresses
The Meraki Cloud Controller must be able to communicate with y
Please make sure that:
1. Your RADIUS servers have public IP addresses (i.e. they a
2. Your firewall, if any, allows incoming traffic to your RADIUS
3. You whitelist the following IP addresses as clients on your
Failover policy
If none of your RADIUS servers are reachable, should clients be a
Deny access
Allow access

You can test this setup using the test button on the Meraki configuration page. If this is set-up correctly you should see a authentication failure in the Swivel logs and a the status change or OK on the Meraki configuration screen, as shown in the screen shot above.

Now the redirect to the login page needs to be set up.

The key setting is to set the Custom splash page URL to a web page that can perform the Swivel authentication.

This page can be a page hosted on the Swivel Appliance (e.g. under webapps2) or Swivel Server, but can be any page that can collect the credentials required for the authentication.



Users
Group policies
Splash page
SSID availability
Network-wide settings
Radio settings
Maps & floorplans
Add access points
Prepaid cards
Organization
Help

Fluid (mobile friendly) new
Classic
Plain

Custom themes

Copy of Classic

Create something new

Custom splash URL

Or provide a URL where users will be redirected:
http:// /login/login-meraki.jsp

What is this?

Customize your page

Message

Splash logo

No logo

Upload a logo

Splash language: English

Splash behavior

Splash frequency: Every half hour

What is this?

Where should users go after the splash page?
- The URL they were trying to fetch
- A different URL:

Save Changes

© 2012 Meraki, Inc. Privacy

113.3 Custom Login Page

When the user attempts to access a URL via the wifi network, they will be re-directed to the custom splash page.

As part of this redirection the following parameters will be passed

- The login_url: The URL to which the login-form needs to be posted
- The continue_url: The url the user was trying to access
- username The users username

The login form must extract these parameters from the request.

Post the username and password (or one-time code) to the login URL, also passing the continue URL.

If a user needs to supply a password and a one-time code, the login form also needs to concatenate the password and one-time code into a single password field.

An example extract of a login page is shown below. The full page is available to download.File:Meraki.zip. Not you will need to supply a suitable header.gif

```
<form method="POST" align="center" onsubmit="combine()" action="<%=grant_url%>">
 <table width="600" align="center">
 <tr>
  <td colspan="2"><image src="./header.gif"></td>
 </tr><tr>
  <td colspan = "2"> <h1>Welcome to Meraki WiFi</h1> </td>
 </tr><tr>
      <th>Username:</th><td><input type ="text" name="username" id="username" onblur="showTuring()" value="<%=username%>" /></td>
      </tr><tr>
      <th>Password:</th><td><input type ="password" id="adpassword" name="adpassword" /></td>
      </tr><tr>
      <th>OTC:</th><td><input type ="password" name="otc" id="otc" /></td>
      </tr><tr>

      <td><input type = "hidden" name="gr" value="<%=grant_url%>"/> </td>
      </tr><tr>
      <td><input type="hidden" name="success_url" value="<%=continue_url%>" /></td>
      </tr><tr>
        <td><input type="hidden" name="password" id="password" /></td>
</tr><tr>
      <td></td><td><input type="submit" value="Login" /><input type="button" onclick="showTuring()" value="New Image" /></td></tr><tr>
          <tr><td colspan="2">Unauthorised access to this network constitutes a breach of the Computer Misuse Act 1990.<br />n</td></tr>

          <% if (grant_url != null) { %>
      <input type="hidden" name="success_url" value="<%=URLEncoder.encode(continue_url)%>" /><%}%></td>
          </tr><tr>

          <th colspan="2"><image id="imgTuring" style="display:none" /></th></tr></table>
    </form>
```

114 Category:Microsoft

115 Category:Mobile

116 Netgear

117 Introduction

This article explains how to integrate the Netgear SSL VPN product set with PINsafe. This article has been created based on the Netgear FVS336G v2 Product. It is assumed that other products that support Banner Text in the same way (such as the SRX5308) can be integrated in the same way. The Netgear FVS336G v2 Product allows a proxy to be created to PINsafe by creating access through a firewall rule.

Note that a firmware upgrade maybe required to support this integration.

118 Baseline

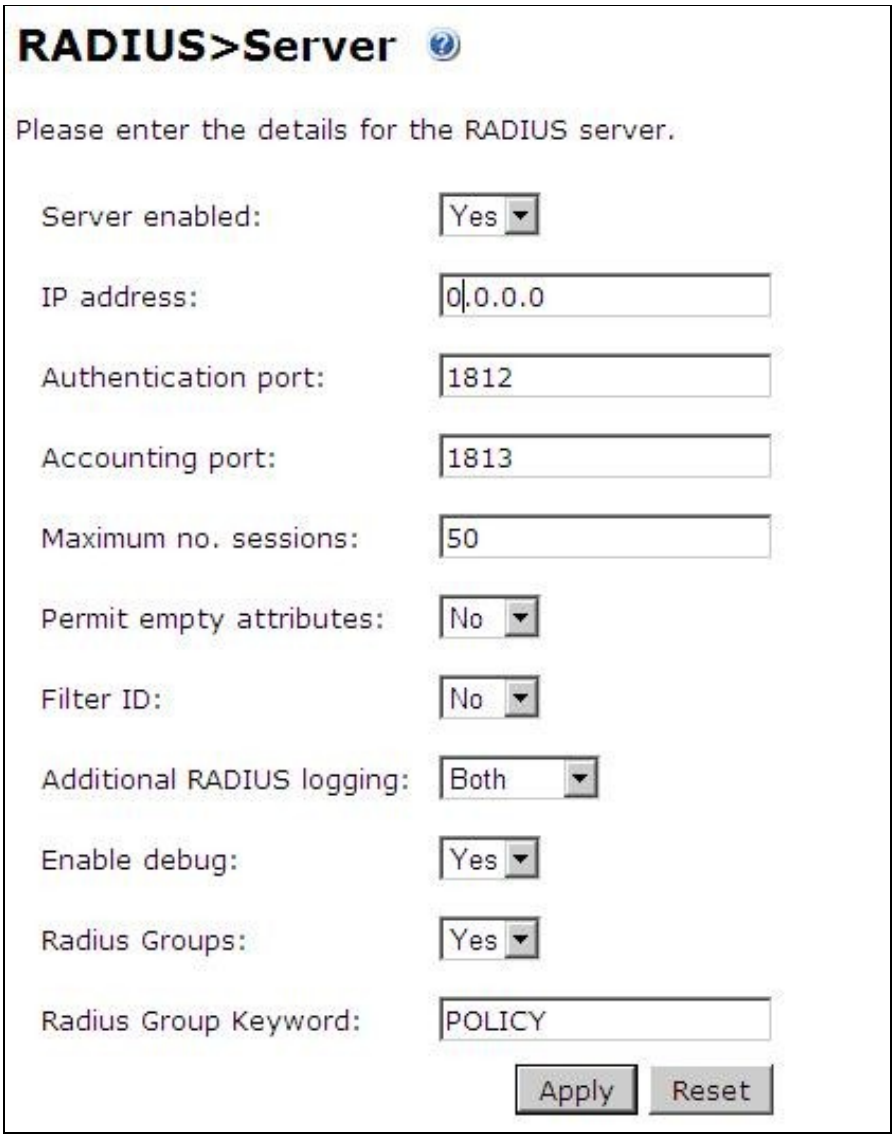
This integration is based on FVS336G v2, Firmware 3.0.7-13 and 3.0.7-24 with PINsafe Version 3.8

119 PINsafe configuration

119.1 Configuring the RADIUS server

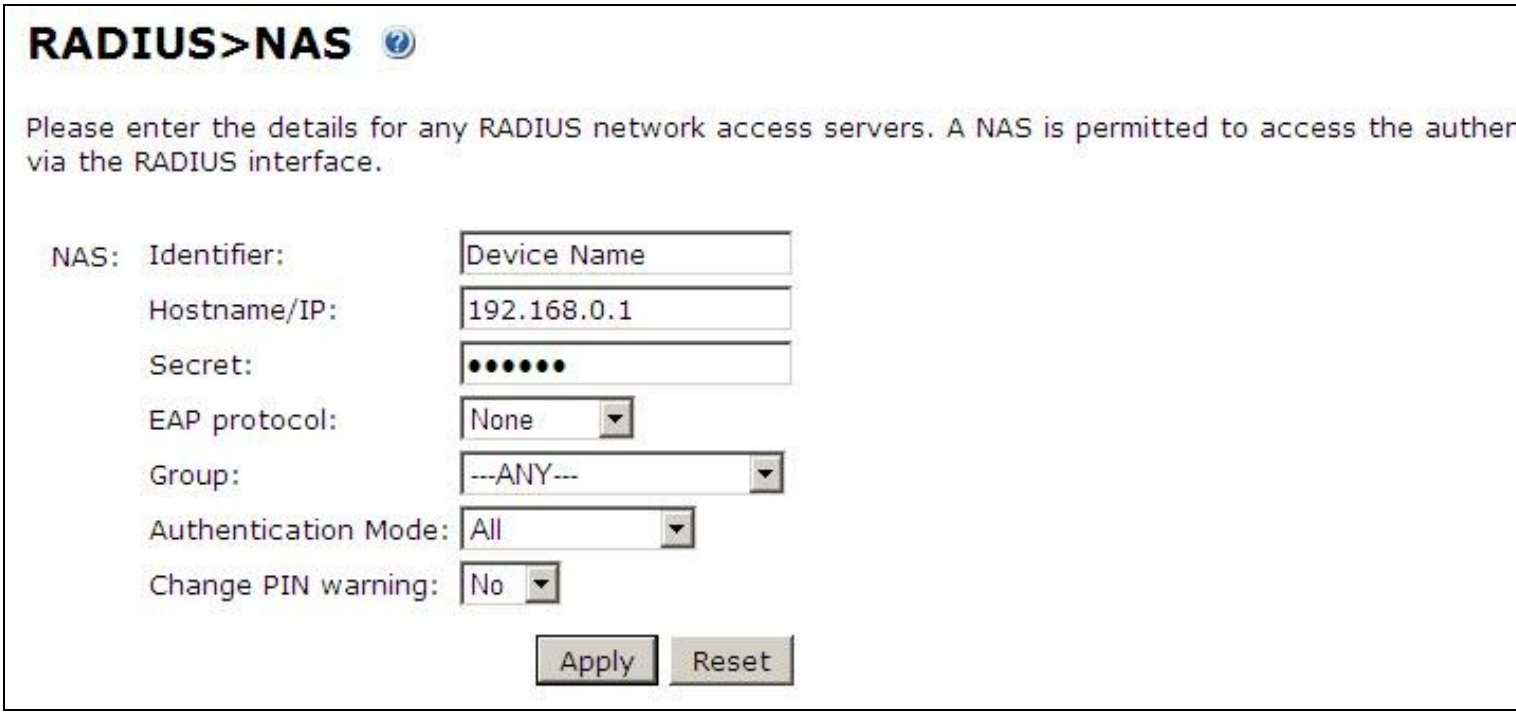
Configure the RADIUS settings using the RADIUS configuration page in the PINsafe Administration console. In this example (see diagram below) the RADIUS Mode is set to ?Enabled? and the HOST IP (the PINsafe server) is set to 0.0.0.0. (leaving the field empty has the same result). This means that the server will answer all RADIUS requests received by the server regardless of the IP address that they were sent to.

Note: for virtual or hardware appliances, the Swivel VIP should not be used as the server IP address, see VIP on PINsafe Appliances



119.1.1 Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the PINsafe Administration console. Enter a name for the Netgear SSL VPN server server. The IP address has been set to the IP of the Netgear SSL VPN server, and the secret ?secret? assigned that will be used on both the PINsafe server and Netgear SSL VPN configuration.



You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP will be supported. All users will be able to authenticate via this NAS unless to restrict authentication to a specific repository group.

119.1.2 Enabling Session creation with username

The PINsafe server can be configured to return an image stream containing a TURing image by presenting the username via the XML API or the SCImage servlet.

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

To test your configuration you can use the following URL using a valid PINsafe username:

Virtual or hardware appliance

https://PINsafe_server_IP:8443/proxy/SCImage?username=testuser

For a software only install see Software Only Installation

For further information see Single Channel How To Guide

119.1.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

120 Netgear Configuration

120.1 Configuring the Domain

To create a portal whereby users have to use PINsafe in order to authenticate, you need to configure a domain on the Netgear SSL VPN.

To do this go to the Users -> Domain page and create a new Domain.

For this Domain, set it to use RADIUS PAP and enter the IP address of the PINsafe server and set the shared secret. Then set the domain to use the Portal pages created previously.

On the PINsafe server ensure that the RADIUS server is enabled and create a NAS entry for the Netgear SSL VPN.

Now when a user goes to the login page they can select the PINsafe domain created.

The credentials they submit will be submitted to PINsafe via RADIUS and if correct access will be granted.

120.2 Single Channel TURing Integration

This is not required where dual channel authentication through SMS, Mobile Client is used.

120.2.1 Create a Firewall Access Rule

Create a rule to allow traffic from the WAN to the Swivel virtual or hardware appliance. The Netgear device will proxy the request. Since this will open up a port to PINsafe from the WAN, it is recommended to use a Swivel virtual or hardware appliance with its proxy port protection on port 8443, and/or configure an IP filter to prevent access to the administration console. See Filter IP How to Guide On the Netgear Prosafe Administration Console select Security/Firewall/LAN WAN Rules then below Inbound Services click on the *add* button and create a rule to allow traffic with the following settings:

Service Name: HTTP (You may need to create a port for 8080 or 8443)

Action/Filter: Allow Always

LAN Server IP Address: PINsafe server IP address

LAN Users:

WAN Users: ANY

Destination WAN1

Bandwidth Profile: None

An entry should appear in the Inbound Services

120.2.2 Modify the Login Page

This section explains how to modify the SSL Login page to include a TURing image. **Note that the banner text is limited to 256 Characters, the example shown is approx 250 characters, so no additions should be made and using a long pinsafe host name may cause issues**

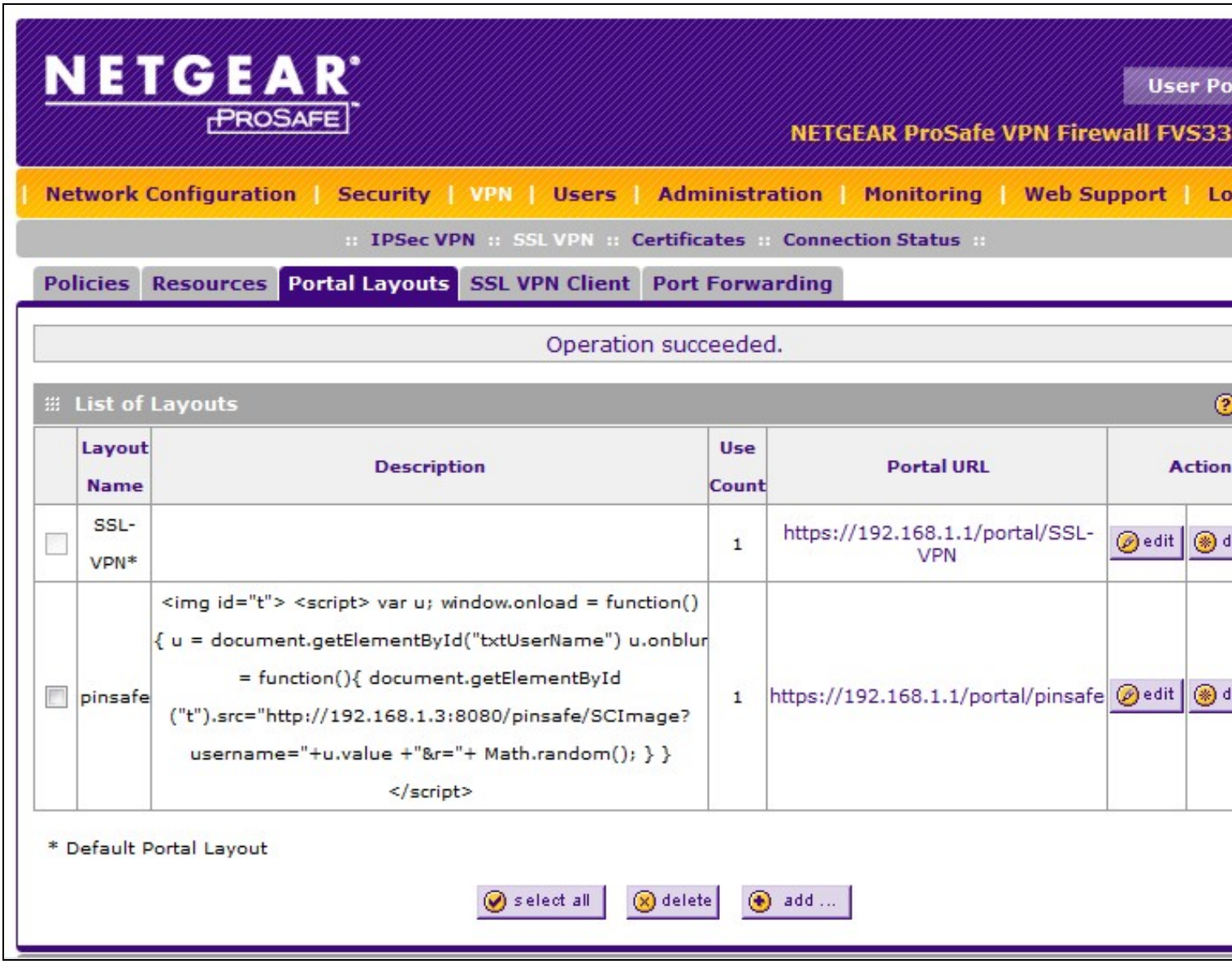
To create the PINsafe login page go to the VPN -> SSL VPN -> Portal Layouts and create a new portal layout.

In the Banner Text section of the portal layout page, enter the following text

```
<img id="t">
<script>
var u;
window.onload = function(){
u = document.getElementById("txtUserName");
u.onblur = function(){
document.getElementById("t").src="http://192.168.1.3:8080/pinsafe/SCImage?username="+u.value +"&r="+Math.random();
}
}
</script>
```

Replacing 192.168.1.3 with the IP address of you PINsafe server. Note that there is a maximum of 256 characters allowed for this so if you PINsafe hostname is long, you may need to removed the "&r="+Math.random() text to compensate.

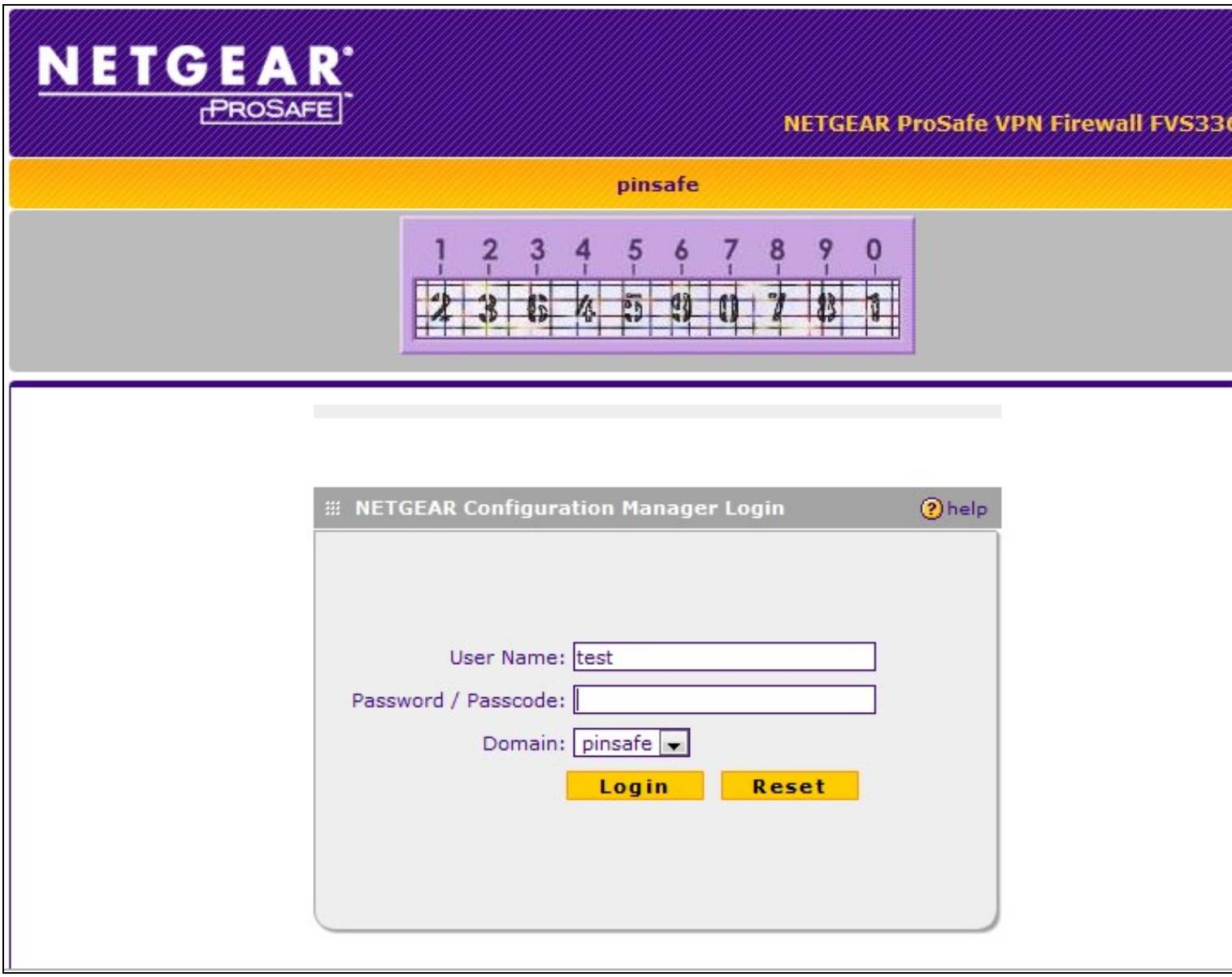
Also note if you are integrating with a virtual or hardware appliance the format will be https on port 8443, and it will be /proxy instead of /pinsafe



Once this portal page is complete you can test that the image is being included correctly by navigating to the login page, in this example https://192.168.1.1/portal/pinsafe.

A similar modification can be completed to request a dual channel image (replace SCImage with DCMessage) or request the index of the security string to be used (replace SCImage with DCIndexImage)

The image should appear when you tab away from the username field.



120.3 Additional Configuration Options

The login can be configured to use AD by using Check Password with Repository on PINsafe. The user would enter the AD password followed by the One time Code, example: ADPasswordOTC password9573. Use of this requires PAP authentication.

See Password_How_to_Guide#Check_password_with_repository

120.4 Known issues

The length of text within the banner may vary between versions, a slightly shorter version of the text without the random number to ensure the image is not cached is given below:

```
<img id="t">
<script>
var u;
window.onload = function(){
u = document.getElementById("txtUserName")
u.onblur = function(){
document.getElementById("t").src="http://192.168.1.3:8080/pinsafe/SCImage?username="+u.value;
}
}
</script>
```

121 Netilla Integration

Netilla Integration Guide

122 Nortel VPN Integration

Nortel VPN Gateway

Integration Guide

Version 1.0 March 2009

123 Introduction

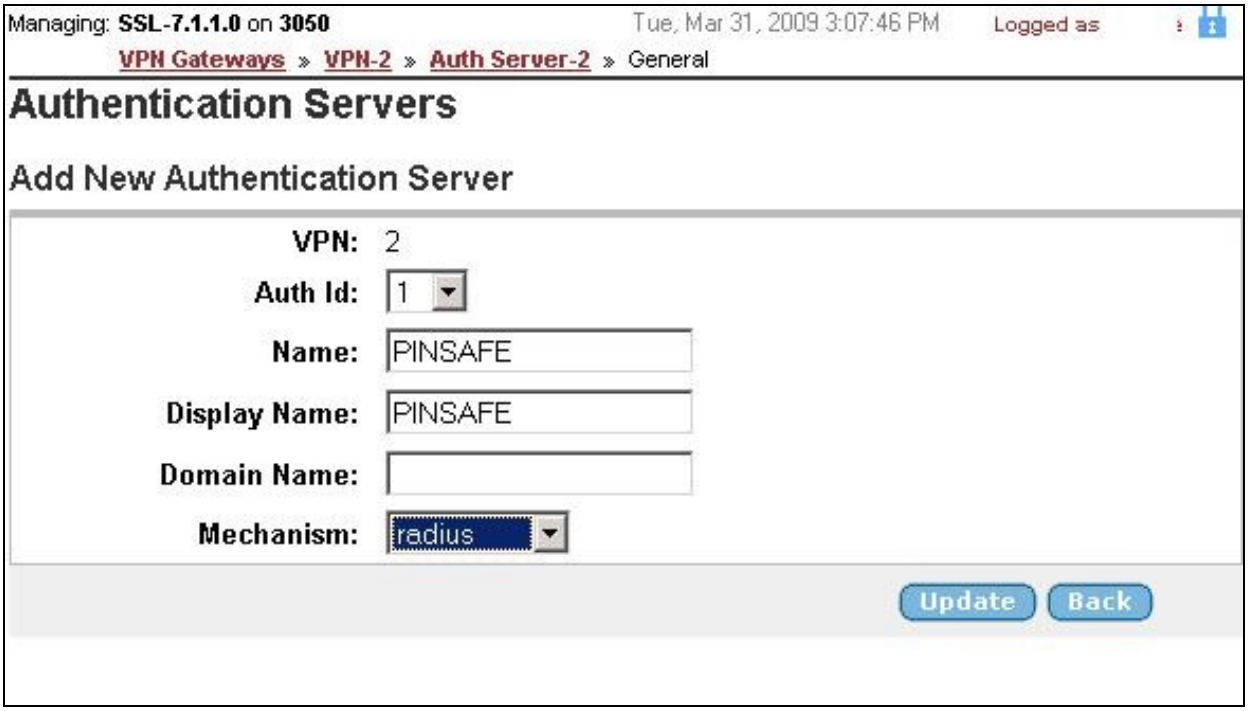
This document describes how to integrate PINsafe with the Nortel VPN Gateway. The integration is based on Nortel 3050 Release 7.1.1.0 This guide covers the Nortel integration only and does not cover the general steps required for configuring the VPN Gateway. This integration requires the PINsafe server to be available from the internet. An appliance install can use the proxy to protect the PINsafe server in this respect.

124 RADIUS Integration

The main integration required is to get the Nortel VPN Gateway to use RADIUS for authentication and to use PINsafe as its RADIUS server.

To do this on the VPN Gateway Config screen select the VPN Gateway you wish to integrate with PINsafe and then select the Authentication option.

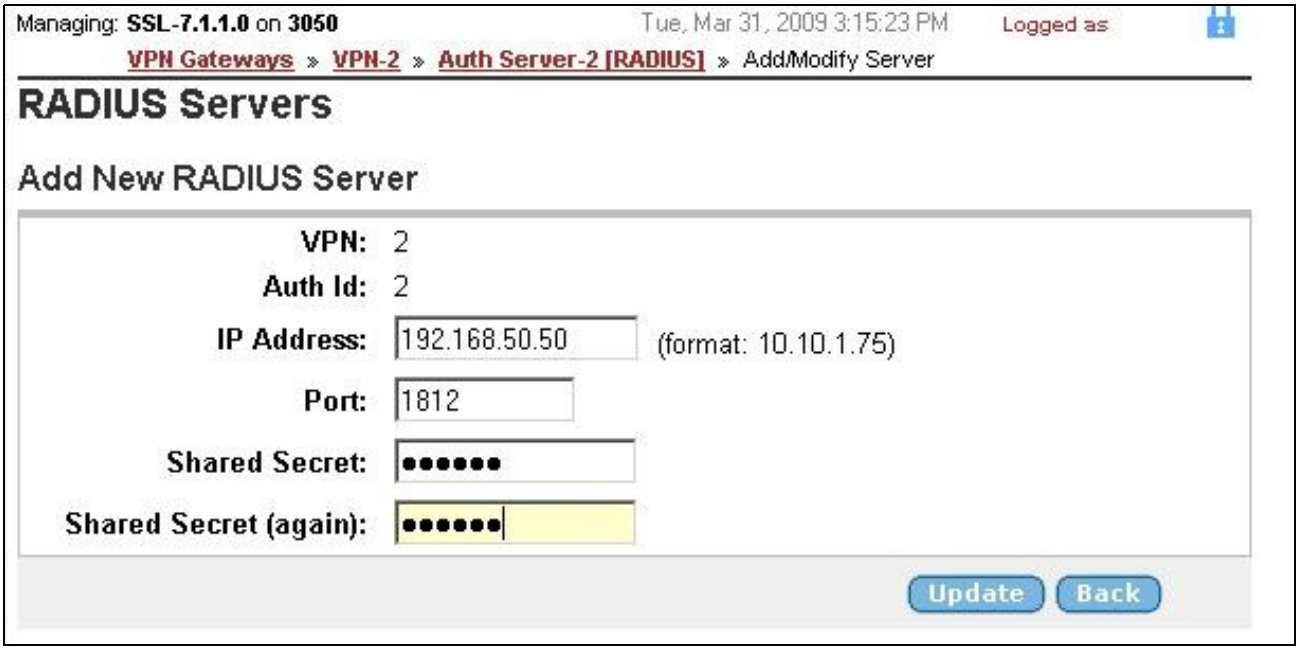
A new authentication server needs to be created. To do this select the Add option and create a new Authentication Server called PINSAFE. The domain name can be left blank.



Then select Update.

Once this stage has been completed the authentication server you have just added will appear on the Authentication Servers screen. Select the server to configure the details. The only essential element is on the Servers tag.

Select this tag and enter the details of the PINsafe server on this screen and click Update.



You must now click Apply on the top right of the screen for these changes to take effect

The VPN is now configured to use PINsafe for authentication. The Nortel allows multiple authentication servers to be defined, if you only wish to use PINsafe then on the Authentication Order tab ensure that it is the only server defined.

You now need to configure PINsafe to accept authentication requests from the Nortel VPN gateway

To do this ensure that the RADIUS server is active and running on the same ports as defined on the Nortel VPN gateway. A NAS then needs to be added that has entries for IP address and shared secret that match those of the Nortel VPN Gateway.

The value for IP address that you need to enter may need to match that of the VPN host defined on the Config ? Hosts screen on the VPN.

125 TURING Integration

The Nortel VPN Gateway supports login page customization and this allows a TURing image to be requested and displayed on the logon page to allow seamless integration between PINsafe and the Nortel VPN Gateway.

This is achieved by going to the VPN Gateway ? Portal page and selecting the Login tab.



The html code required to include the TURing image can then be inserted. A sample is shown below.

```
<script language="JavaScript">
function addButton(e){
var t = document.getElementById('f');
var d = t.getElementsByTagName('td');
d[3].innerHTML = '<input name="user" id="user" size="20" type="text" onblur = "ShowTuring()">';
var i = d.length - 1;
var h = d[i - 1].innerHTML;
d[i-1].innerHTML = h + '  <input type=button name=btnTuring value="Get Another Image" onclick=ShowTuring()>';
var ta = t.getElementsByTagName('table')[0];
r = ta.insertRow(2);
c1 = r.insertCell(0);
c2 = r.insertCell(1);
c1.innerHTML = ' ';
c2.innerHTML = '<img id=turing style="visibility:hidden;">';
r = ta.insertRow(3);
c1 = r.insertCell(0);
c2 = r.insertCell(1);
c1.innerHTML = ' ';
c2.innerHTML = '<font color="red">* Case Sensitive<br></font>';>
}

function ShowTuring() {
ppText = document.getElementById("ptext");
if(ppText != null){
 ppText.innerHTML = "One-Time Code:";
}
var img = document.getElementById("turing");
var usr = document.getElementById("user").value;
var imgUrl = "http://83.111.60.59:81/pinsafe/SCImage?username=";
if (usr=="") {
 alert ("Please enter your username first!");
 document.getElementById("user").focus();
}else{
 //Set the image SRC and make it visible
 var t = document.getElementById('f');
 var d = t.getElementsByTagName('td');
 img.src = imgUrl + usr + "&random=" + Math.ceil(10000*Math.random());
 img.style.visibility = "visible";
 }
}
</script>
```

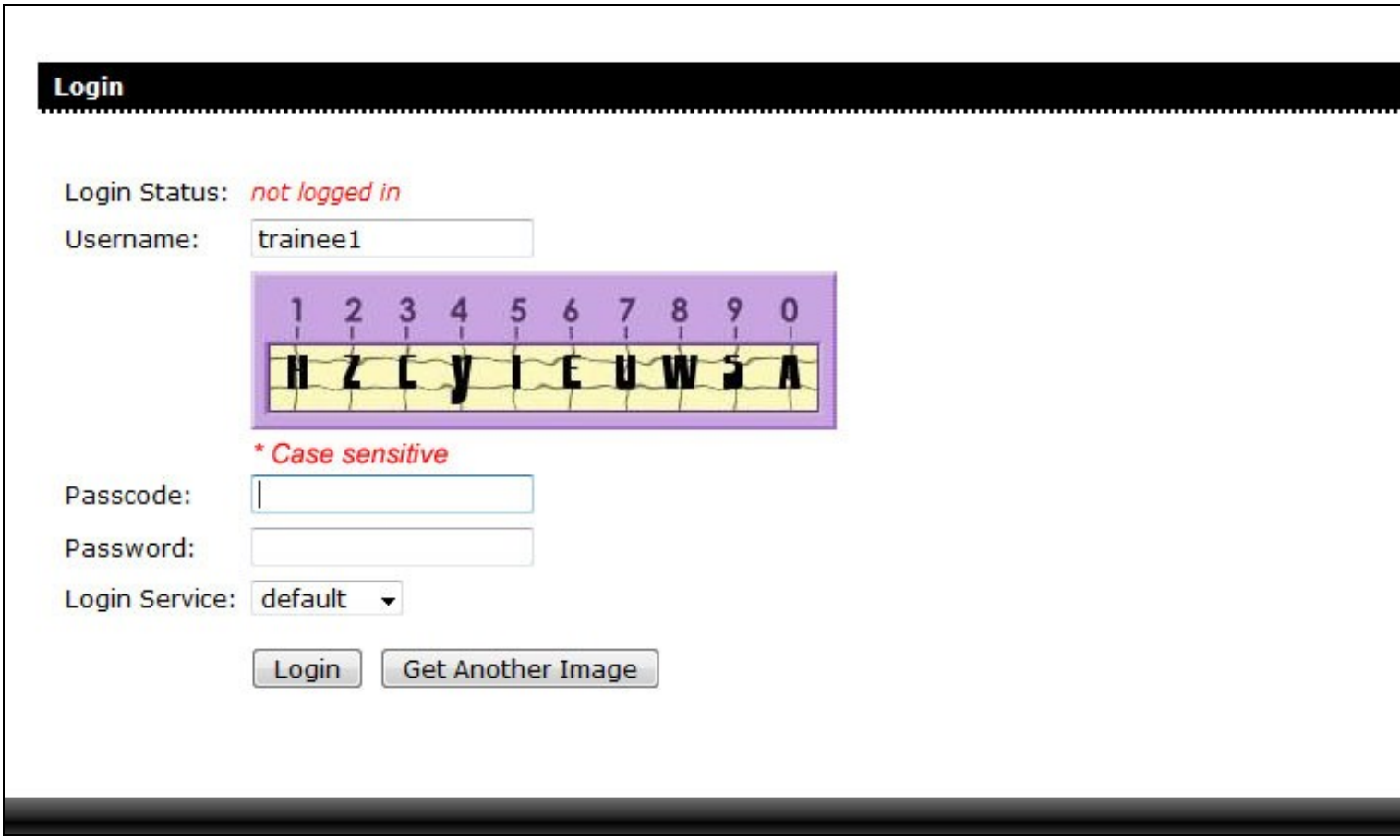
```
<script  language="JavaScript" type="text/javascript">
window.onload = addButton;
</script>
```

The url http://pinsafe:8080/pinsafe/SCImage?username= needs to be changed to match the IP address of the PINsafe server. Note that for an appliance this is likely to be in the format https://pinsafe:8443/proxy/SCImage?username=

Once these changes have been inserted click UPDATE.

You must now click Apply on the top right of the screen for these changes to take effect

You can then view the modified page by going to the ip address associated with the VPN on the Config ? VPN Screen.



126 Notes

This integration requires the PINsafe server to be available from the internet. An appliance install can use the proxy to protect the PINsafe server in this respect.

To test the integration ensure that there is a user that exists on both PINsafe and the VPN Gateway and check the PINsafe logs to see that it is receiving the authentication requests.

127 Category:Open ERP

128 OpenVPN integration

128.1 Introduction

This article describes how to integrate an existing OpenVPN server with PINsafe, to allow VPN authentication with a Username and One Time Code (OTC) using SMS, mobile phone clients, and the Taskbar. The Single Channel TURing image is not directly displayed within the login.

128.2 Prerequisites

- Linux OpenVPN server installation.
- PINsafe installation with network port UDP 1812, accessible from OpenVPN server device.
- OpenVPN Client

128.3 Baseline

The Swivel integration was tested with the following versions

Linux OpenVPN server CentOS/RHEL openvpn-2.2.0-3.el6.rf.x86_64

OpenVPN Client 2.1 rc19

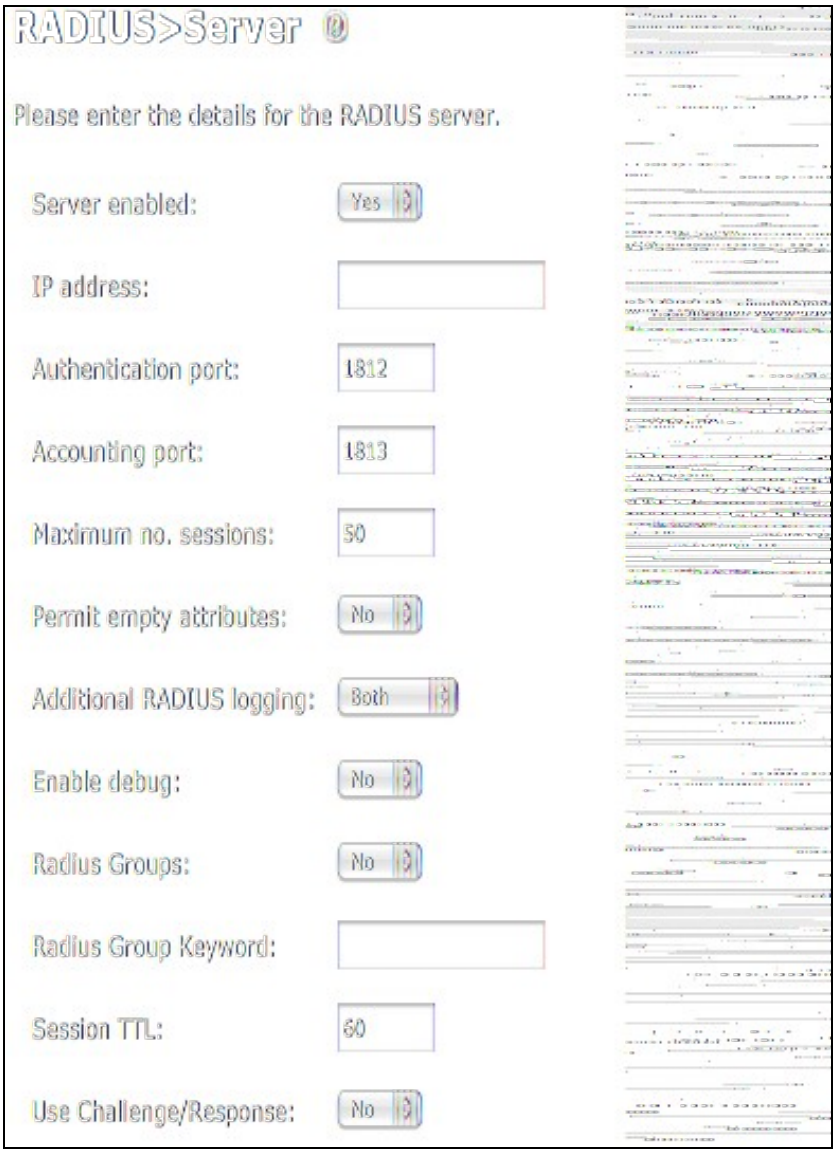
Swivel 3.8

128.4 Integration

128.4.1 PINsafe Integration

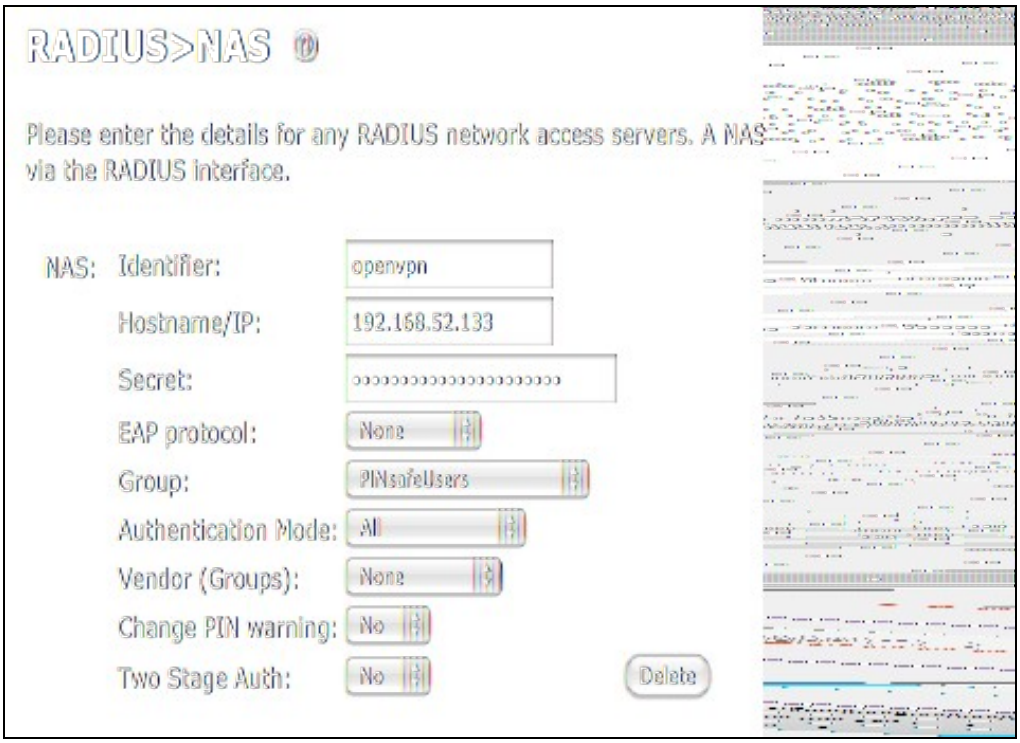
On the Swivel appliance

1.-) Configure and enable RADIUS Server:



Set the option *Server Enabled* to Yes

2.-) Create a new NAS (Network Access Server)



- **Identifier:** Descriptive name of the openvpn server (hostname)
- **Hostname/IP:** OpenVPN Server IP address (as seen by PINsafe. Note if any NAT is required)
- **Secret:** Same secret password set in openVPN file /etc/pam_radius.conf
- **Group:** The PINsafe group permitted to authenticate

128.4.2 OpenVPN Server Integration

In the **OpenVPN Server device** (assumed to be a RHEL/CENTOS), the package **pam_radius** RPM should be installed.

To achieve that run the command *"yum install pam_radius"*.

Edit the openvpn configuration file. By default this file should be **/etc/openvpn/openvpn.conf**.

Add the line:

```
plugin /usr/share/openvpn/plugin/lib/openvpn-auth-pam.so openvpn
```

IMPORTANT UPDATE In OpenVPN Server openvpn-2.2.1-1.el6.x86_64 the plugin location changes to **/usr/lib64/openvpn/plugin/lib/openvpn-auth-pam.so**. It is hihgly recommended to perform a search for file **openvpn-auth_pam** to ensure everything will work smooth.

Edit the file **/etc/pam_radius.conf** and add a line with next format:

```
IP_Pinsafesecret   timeout
```

where:

IP_Pinsafe is the IP address where PINsafe installation is.

secret is the password that will be used for the RADIUS communication with PINsafe RADIUS Server.

timeout is the time in seconds that will be defined to wait until a connection attempt with pinsafe server is terminated.

```
Example: "192.168.52.25 secret 10"
```

Edit the file **/etc/pam.d/openvpn** and add after lines at the beginning with

```
account required pam_radius_auth.so
auth required pam_radius_auth.so no_warn try_first_pass
```

On the **OpenVPN server** a service restart will be needed:

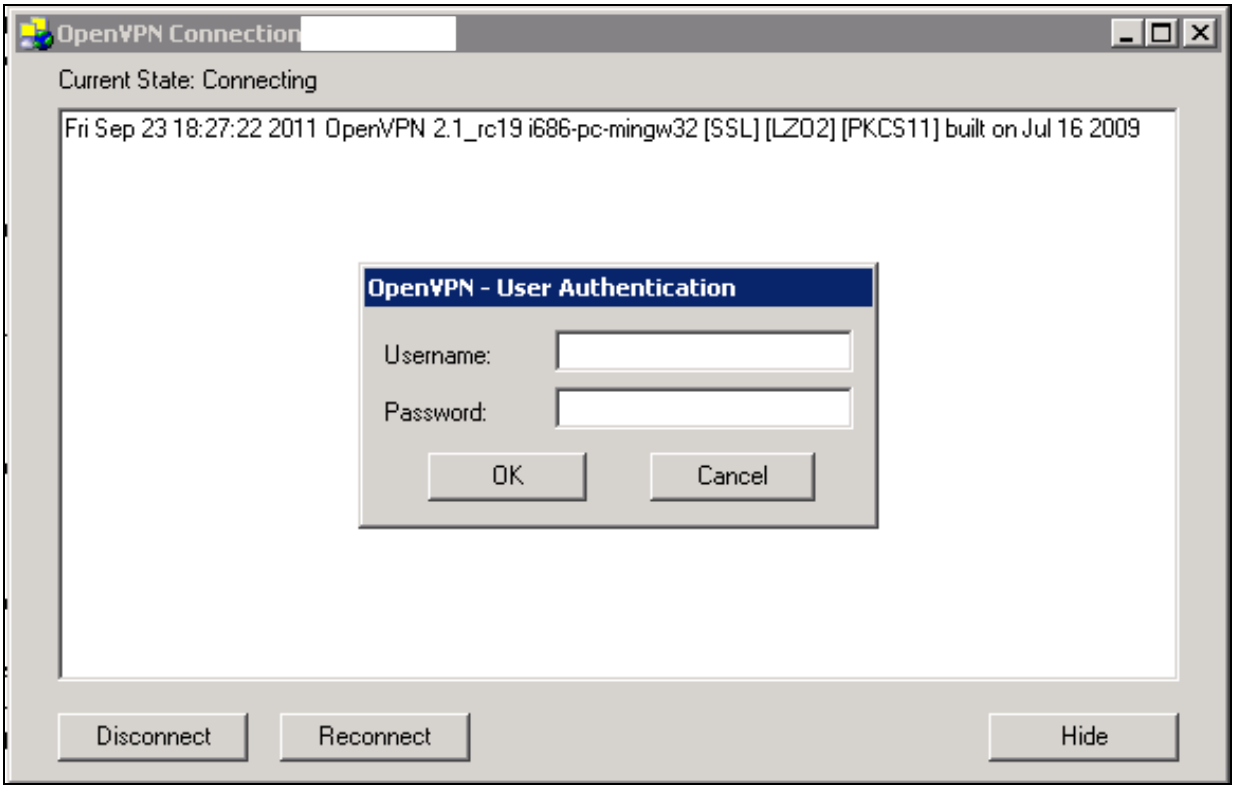
```
"/etc/init.d/openvpn restart" or "service openvpn restart"
```

128.4.3 OpenVPN Client Integration

On the client **OpenVPN configuration file**, add the following line:

```
"auth-user-pass"
```

When the client application starts it will prompt with a window before starting the connection for authentication information:



OpenVPN-GUI for Windows



Tunnelbick for Mac OSX

129 Category:Oracle

130 Palo Alto Networks Integration

130.1 Introduction

This document describes steps to configure a Palo Alto Networks Firewall with Swivel as the authentication server using RADIUS with SMS, Mobile Phone Client, and Taskbar Authentication. The solution is tested with a Palo Alto Networks GlobalProtect client.

130.2 Prerequisites

Palo Alto Networks Firewall

Palo Alto Networks documentation

Swivel 3.x, 3.5 or later for RADIUS groups

130.3 Baseline

Palo Alto Networks PA-2050

Palo Alto Networks Software 4.1.6

Palo Alto Networks GlobalProtect Client 1.14 and 1.15

Swivel 3.8

130.4 Architecture

The Palo Alto Networks makes authentication requests against the PINsafe server by RADIUS.

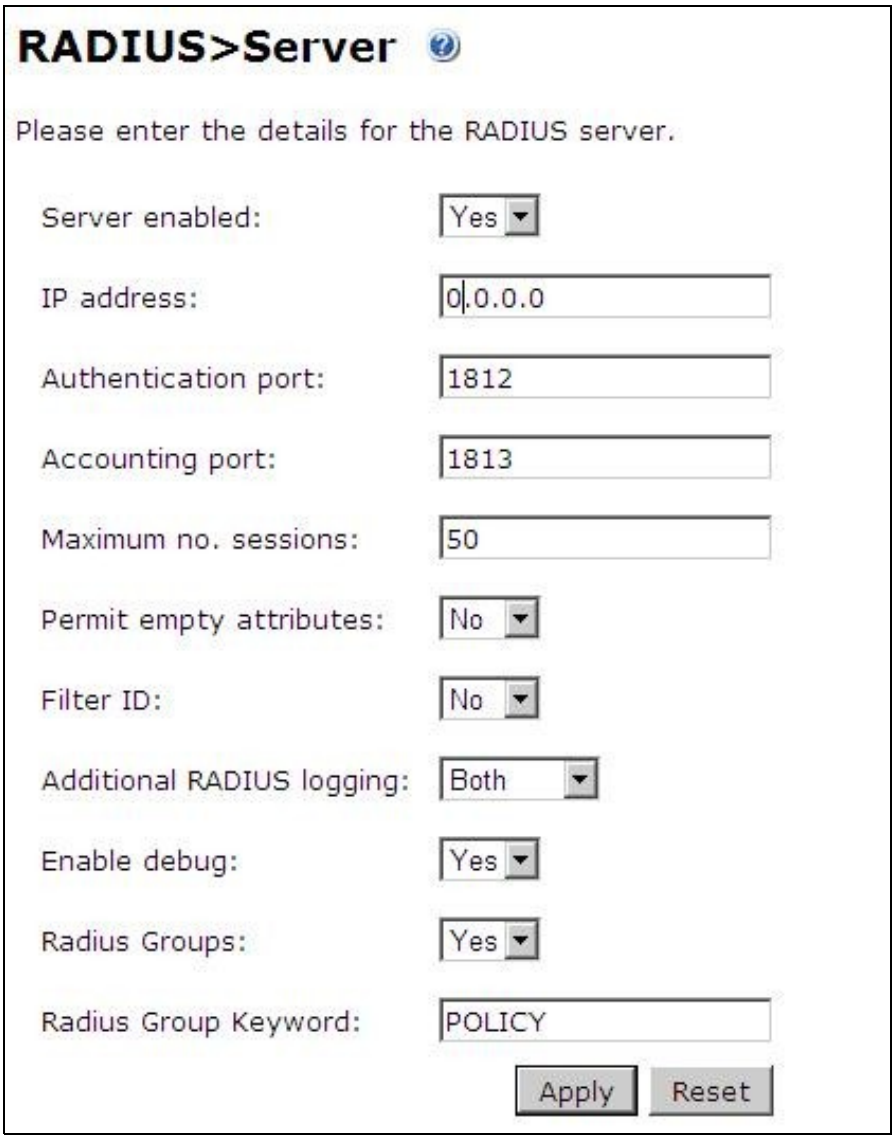
130.5 Swivel Configuration

130.5.1 Configuring the RADIUS server

Configure the RADIUS settings using the RADIUS configuration page in the Swivel Administration console by selecting RADIUS Server. To turn on RADIUS authentication set **Server Enabled** to YES. The Host or IP address is the interface which will accept RADIUS requests, leave this blank to allow RADIUS requests on any interface. (In this example the HOST IP is set to 0.0.0.0 which is the same as leaving it blank).

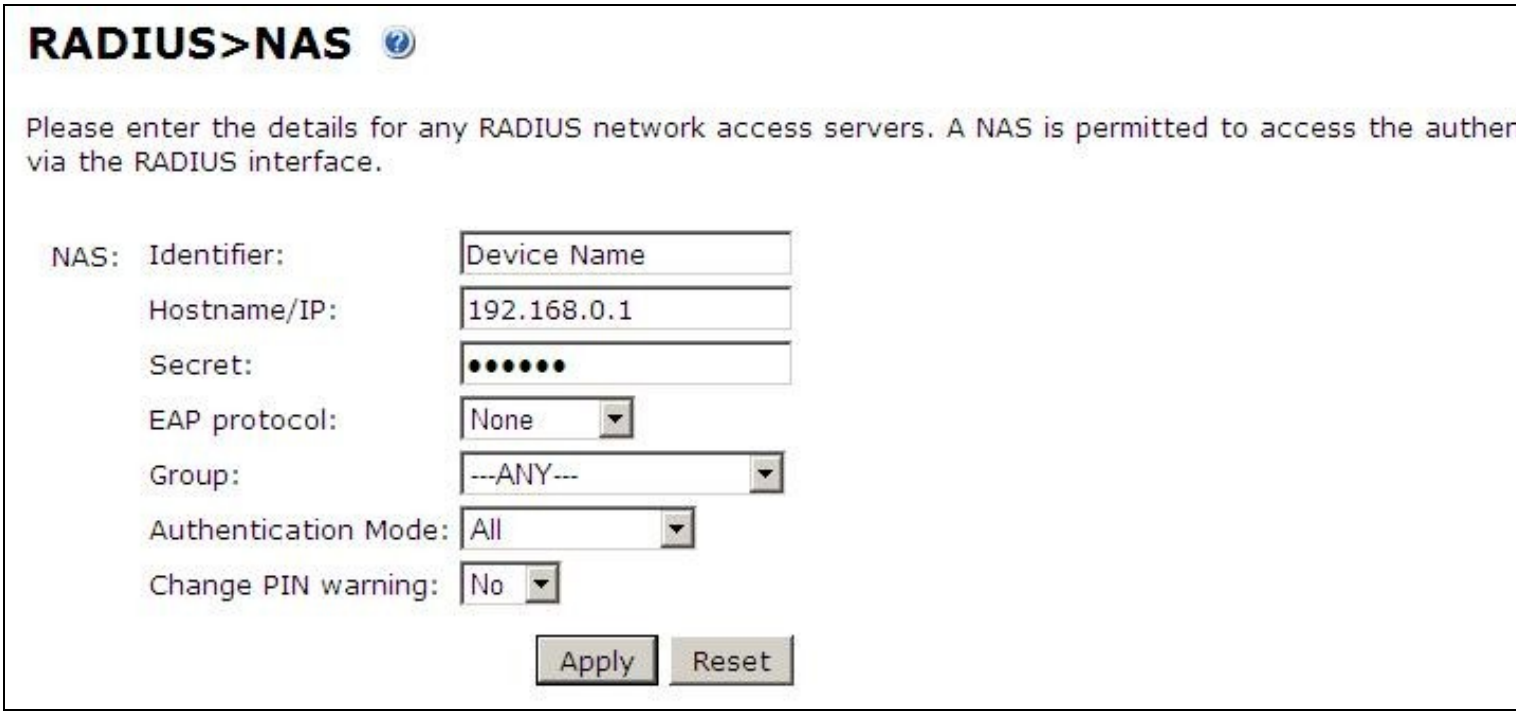
For troubleshooting RADIUS debug can be enabled together with the debug log option, see Debug how to guide

Note: for appliances, the Swivel VIP should not be used as the server IP address, see VIP on PINsafe Appliances



130.5.2 Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the PINsafe Administration console. Enter a name for the VPN server. The IP address has been set to the IP of the VPN appliance, and the secret ?secret? assigned that will be used on both the PINsafe server and VPN RADIUS configuration.



You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP are supported. All users will be able to authenticate via this NAS unless authentication is restricted to a specific repository group.

130.5.3 Enabling Session creation with username

The Swivel server can be configured to return an image stream containing a TURing image in the Taskbar

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

To test your configuration you can use the following URL using a valid Swivel username:

Appliance

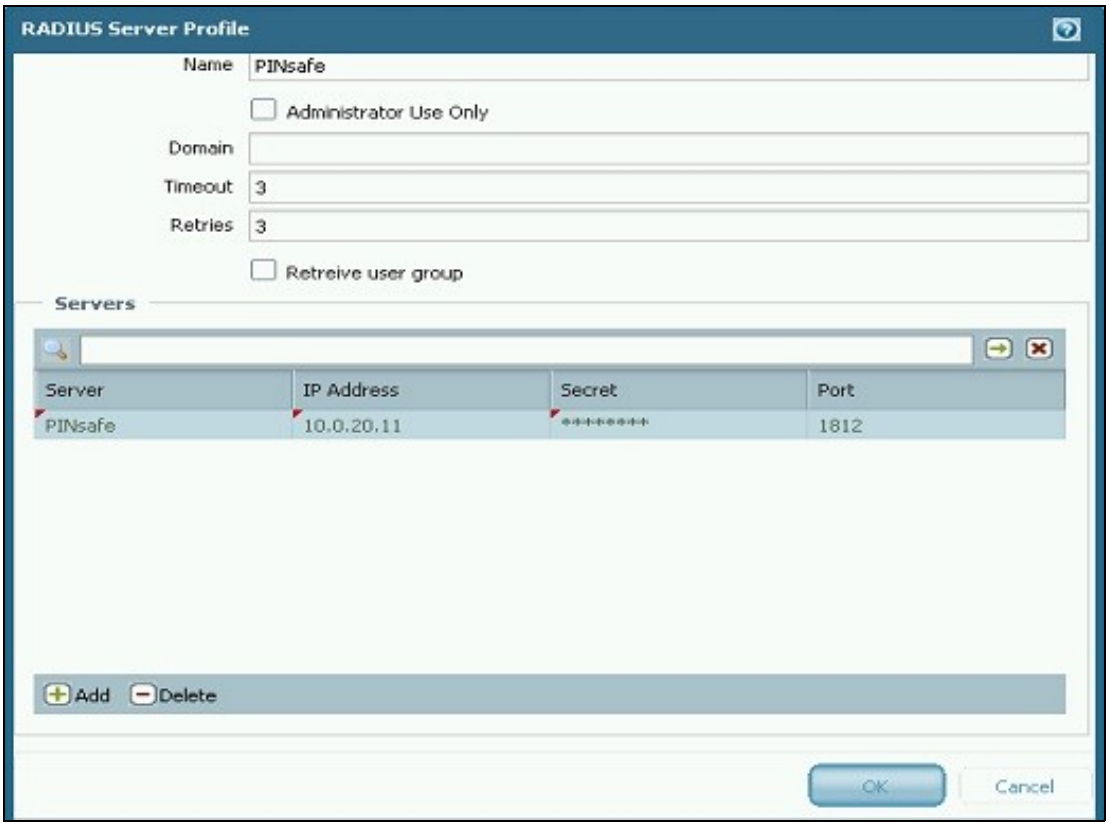
https://Swivel_server_IP:8443/proxy/SCImage?username=testuser

For a software only install see Software Only Installationr

130.6 Palo Alto Networks Configuration

130.6.1 Create a RADIUS Server Profile

On the Palo Alto Networks Administration console select the Device tab then Server Profiles and then RADIUS, and click on Add.



Enter the following information:

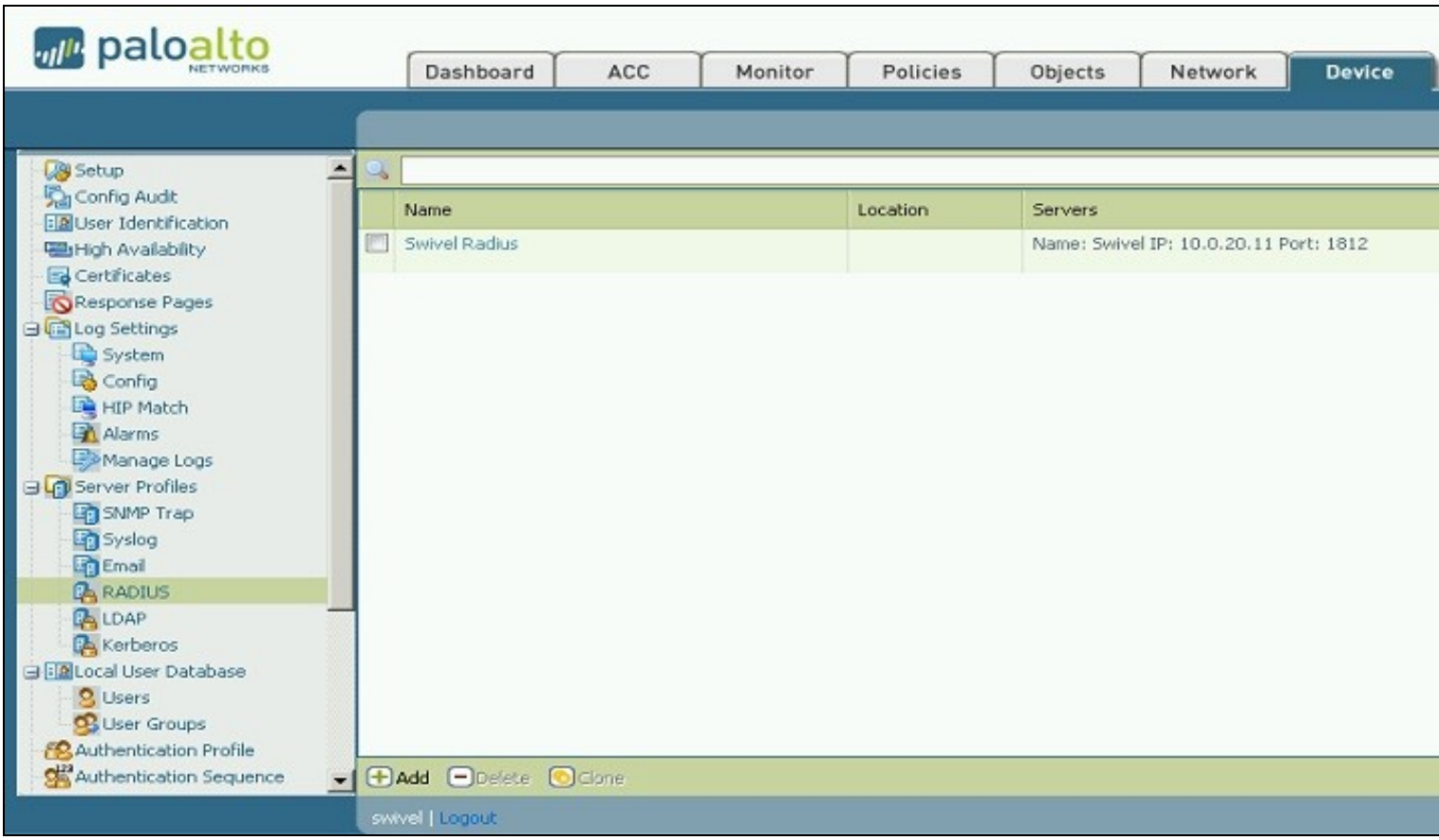
Name Descriptive name for the authentication server

Domain A domain to be appended to the authentication request

IP address or hostname of the Swivel server

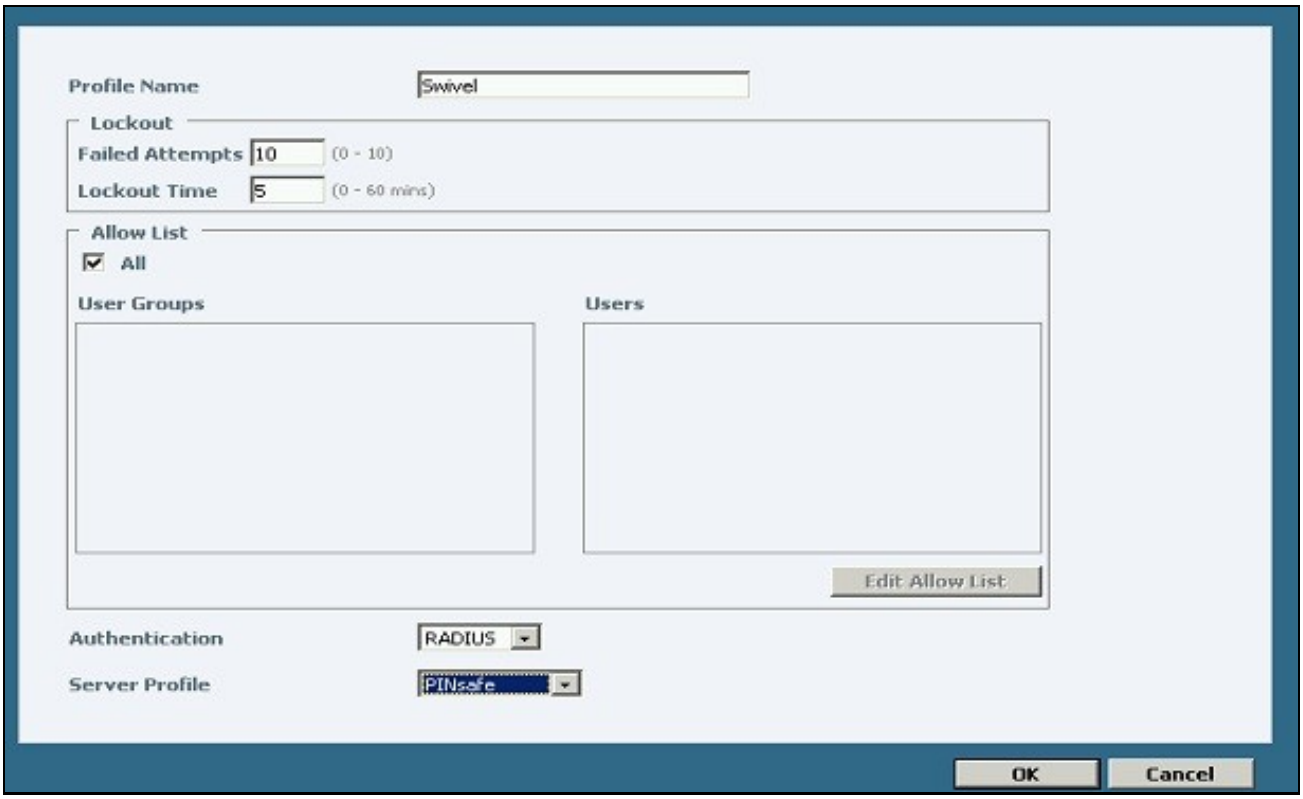
Shared secret as entered on the PINsafe server

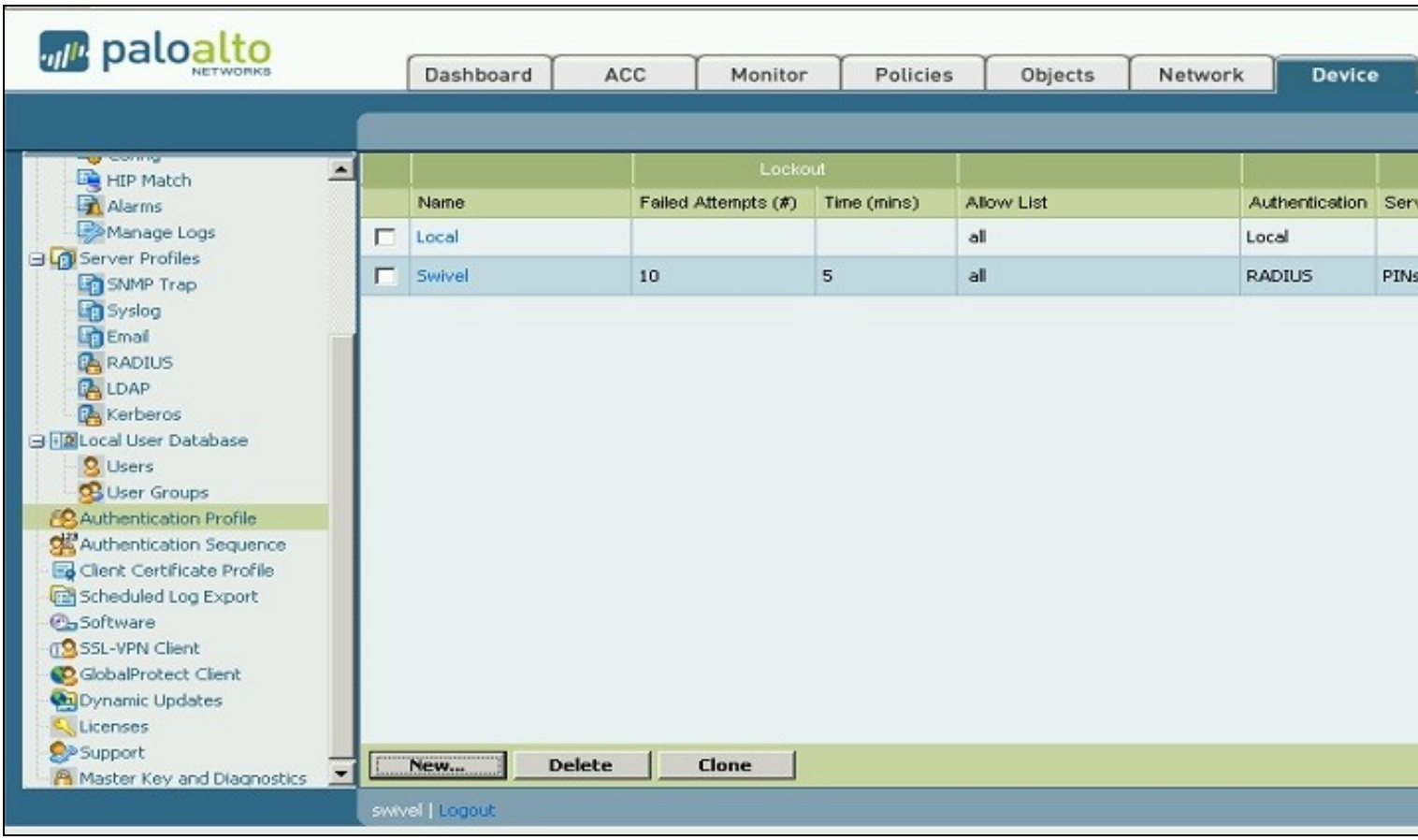
Port usually 1812 by default



130.6.2 Create an Authentication Profile

On the Palo Alto Networks Administration console select the Device tab then Authentication profiles, and click on New. Enter a name and select RADIUS as the authentication type, and the Swivel server for the profile.

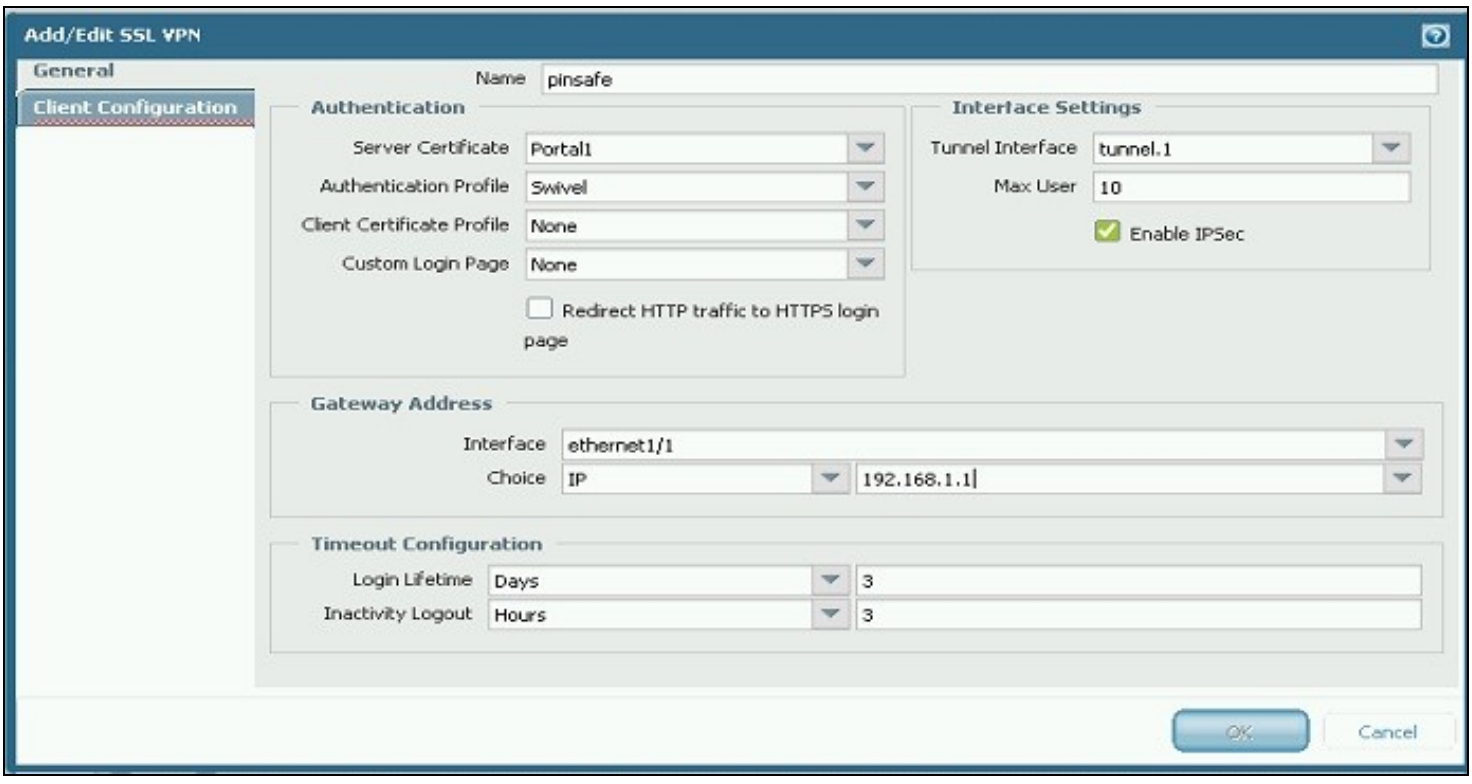




130.6.3 Configure the GlobalProtect Portal to use Swivel RADIUS Authentication

On the Palo Alto Networks Administration console select the Network tab then SSL-VPN, either edit an existing GlobalProtect Portal or configure a new one by clicking on New.

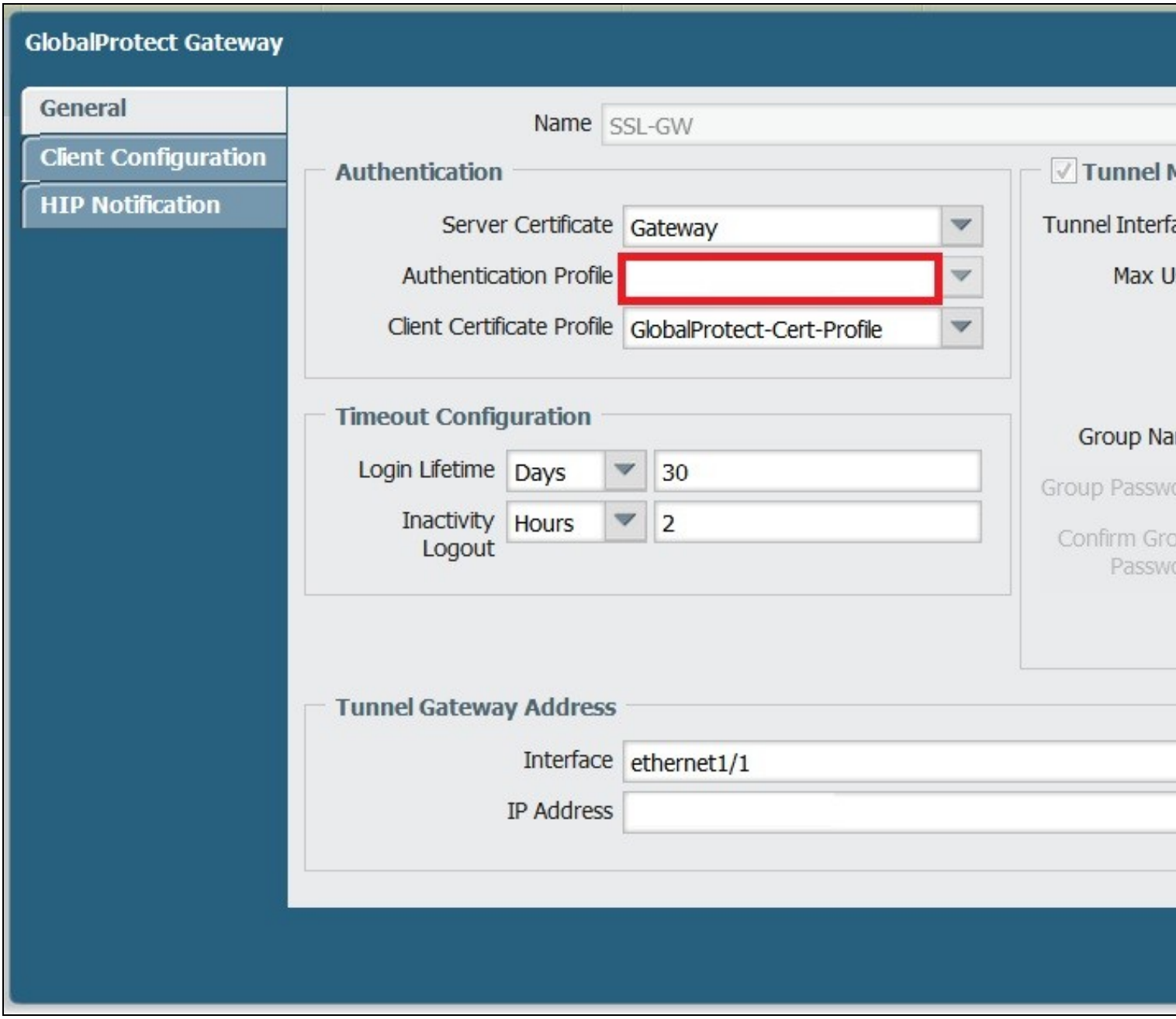
Configure the **Authentication Profile** to use the authentication profile created above.



130.6.4 Configure the GlobalProtect Gateway to use Swivel RADIUS Authentication

On the Palo Alto Networks Administration console select the Network tab then SSL-VPN, either edit an existing GlobalProtect Gateway or configure a new one by clicking on New.

Configure the **Authentication Profile** to use the authentication profile created above.

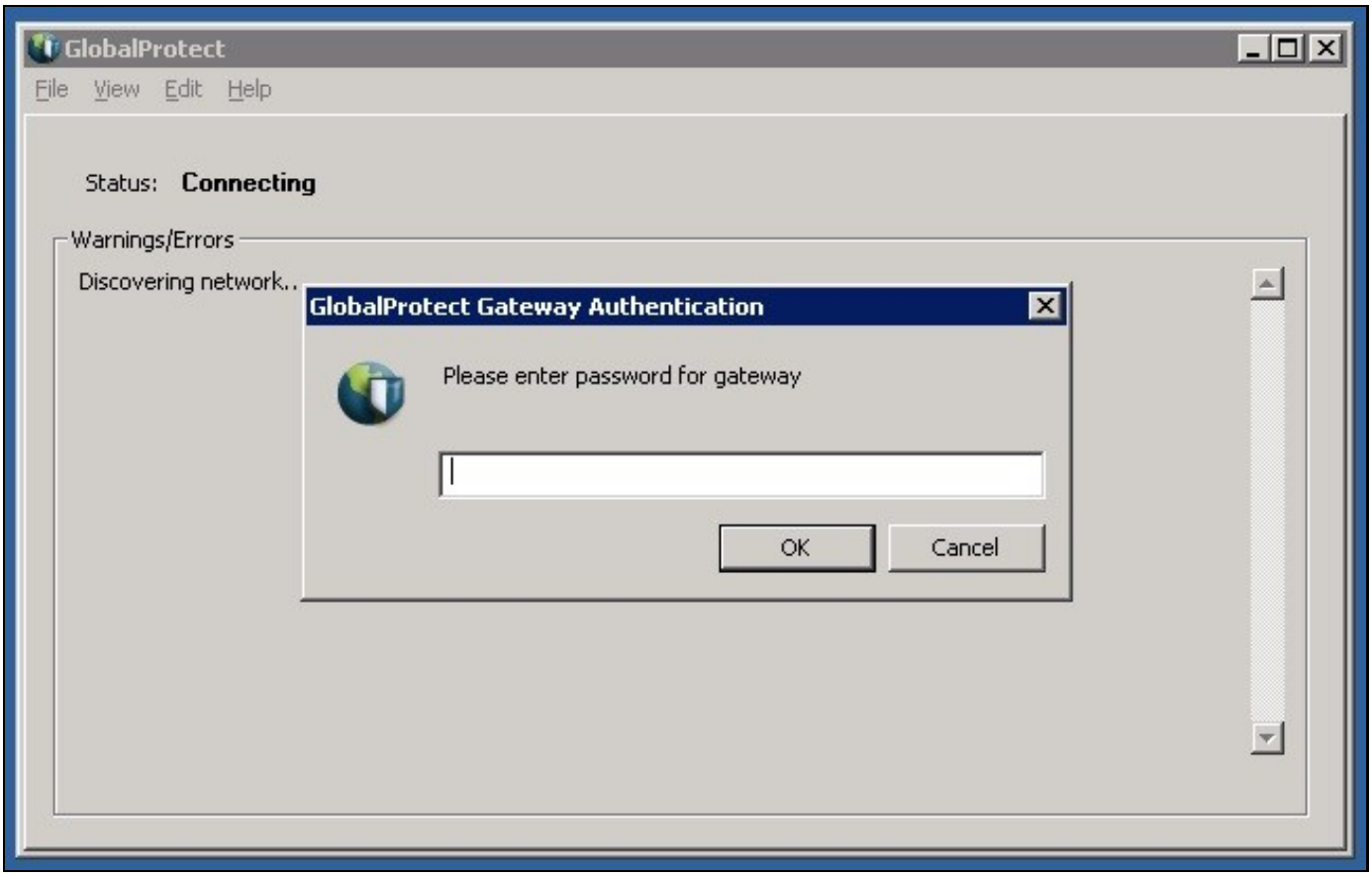


130.7 Additional Configuration Options

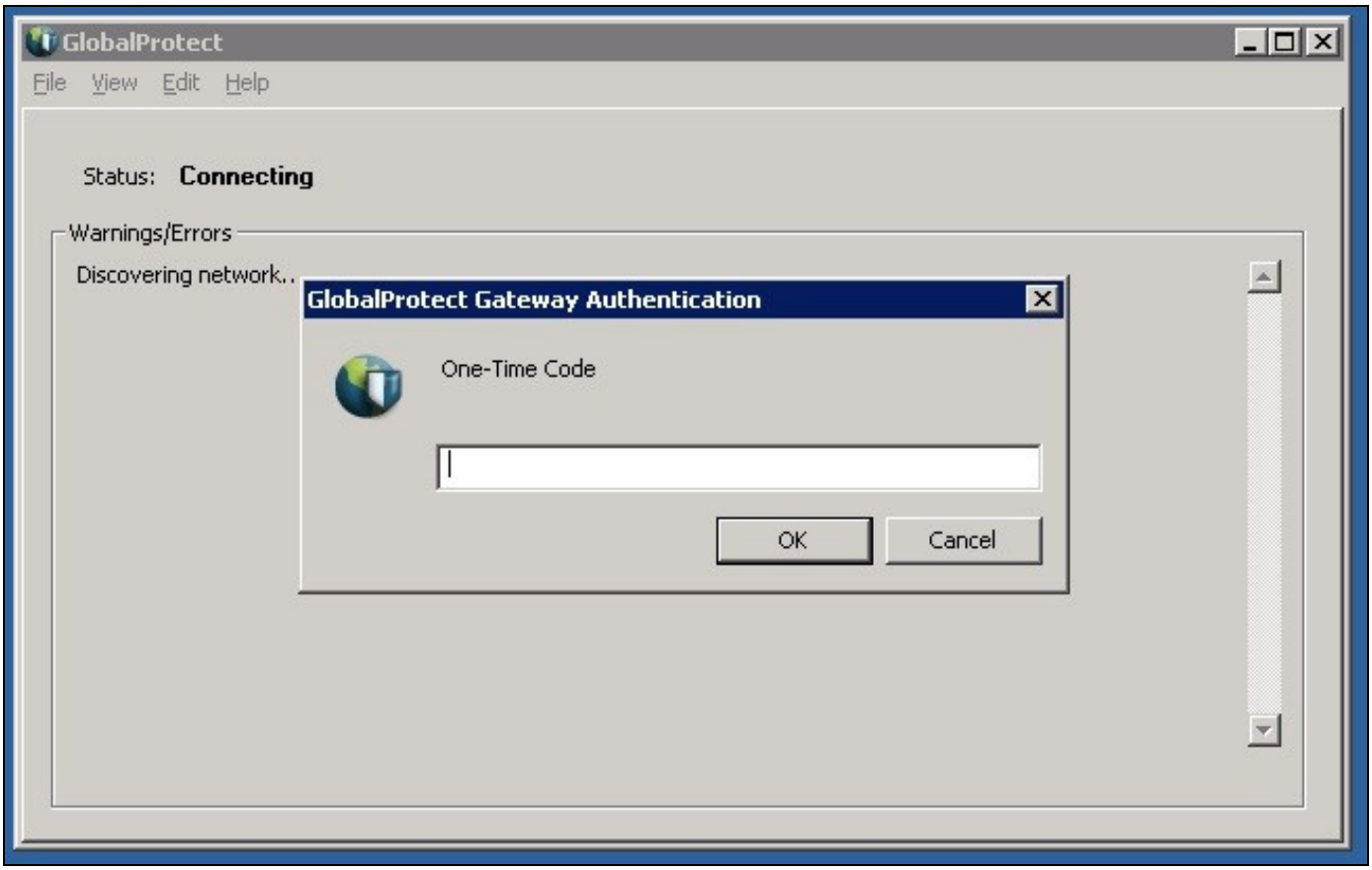
130.7.1 Challenge and Response with Two Stage Authentication

Challenge and Response is supported by using Two Stage authentication and Check Password with Repository using RADIUS PAP authentication. See Challenge and Response How to Guide.

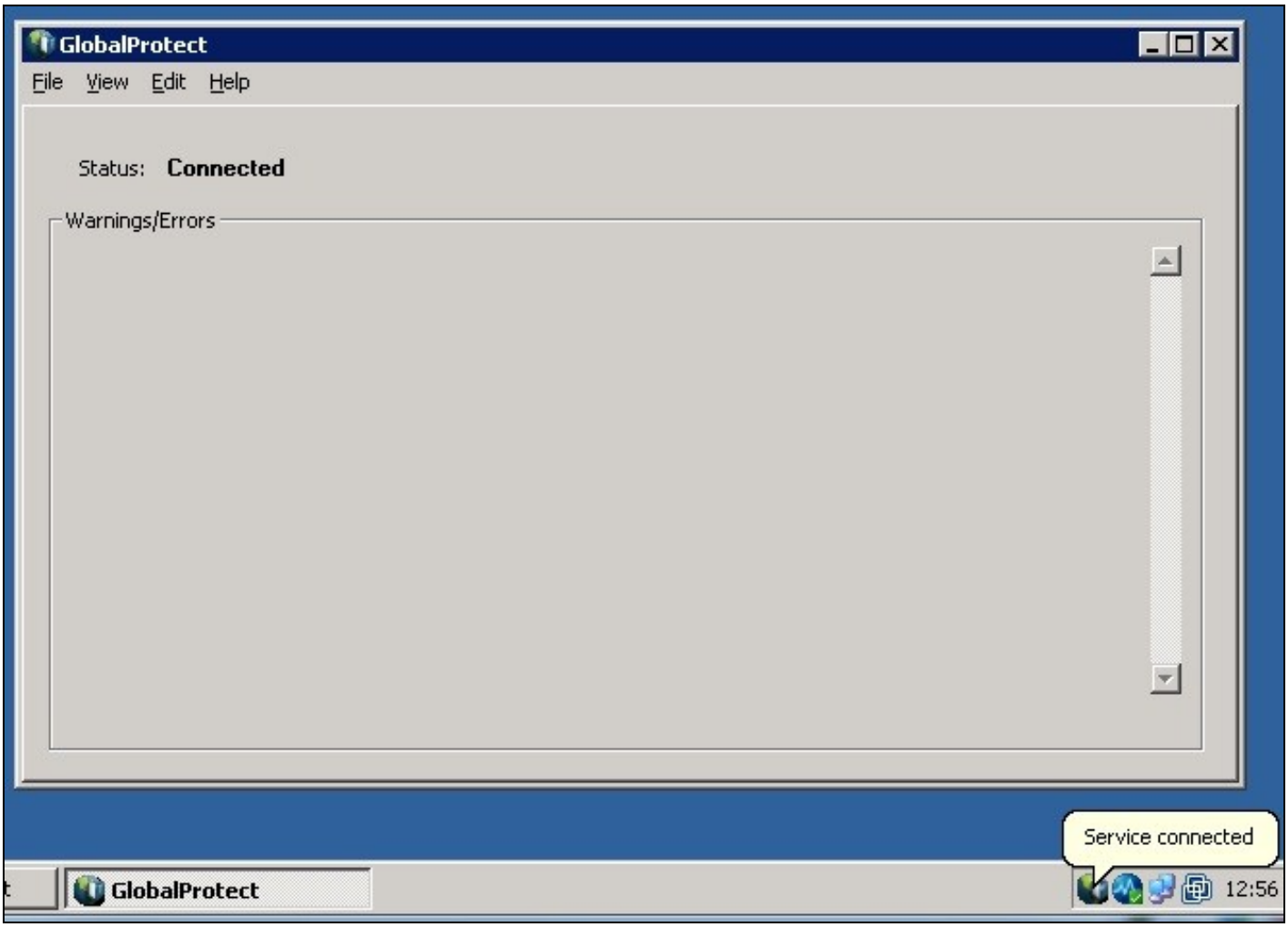
Enter Password



Enter OTC



IF OTC is correct then connection will be established



130.8 Testing

Connect to the GlobalProtect Client and authenticate using RADIUS authentication.

130.9 Troubleshooting

Check the PINsafe logs for RADIUS requests.

130.10 Known Issues and Limitations

None

130.11 Additional Information

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

131 Category:SAML

132 Sawmill Integration

132.1 Sawmill Integration with Swivel

Sawmill is a log analysis tool and can produce reports from Swivel logs. Log output from a syslog server can be also read by Sawmill.

132.2 Prerequisites

This article assumes you are running Swivel 3.2 or later and Sawmill Version 8

The Swivel Custom plugin for Sawmill (http://store.sawmill.co.uk/store/index.asp?pid=41) is also required

For Sawmill Enterprise Enterprise Edition a single copy license of the plug-in is provided for free, contact sales@sawmill.co.uk for further information.

132.3 Baseline

Swivel 3.5

Sawmill 8.08

132.4 Architecture

Swivel produces XML log files, there are several deployment scenarios which can be used:

1. These can be copied to a log server for analysis
2. Pulled from the Sawmill server from the PINsafe server.
3. Analysis of log files from Syslog log files.

132.5 Swivel Configuration

Ensure that the PINsafe logs are readable by the Sawmill server.

132.6 Sawmill Configuration

Copy Across PINsafe log filter files

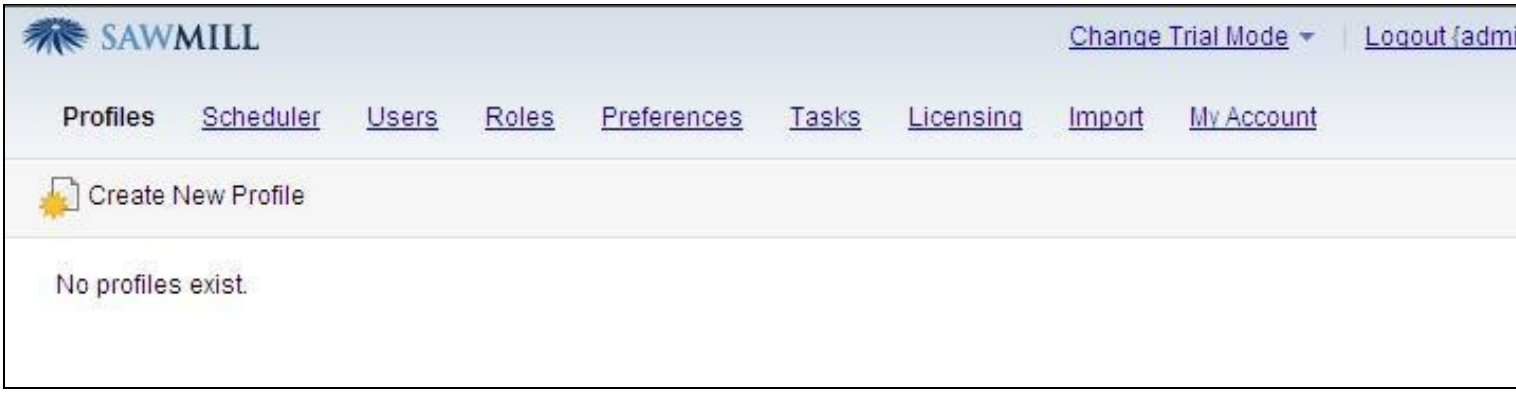
The Log format files (swivel_pinsafe_xml.cfg and swivel_pinsafe_syslog.cfg) need to be copied to the Sawmill Server into Sawmill 8\LogAnalysisInfo\log_formats

Example:

C:\Program Files\Sawmill 8\LogAnalysisInfo\log_formats

Start the New Profile Wizard

From Profiles select Create New Profile



Enter the Log Source

Enter the log Source and any required information such as pathname for the PINsafe logs.

This setting will depend on which logs you are using, for example if Sawmill is deployed on the same server as PINsafe the path would be

\usr\local\apache-tomcat-x.xx\webapps\pinsafe\WEB-INF\logs*log



Sawmill will automatically attempt to identify the correct log format options.

Select Log Format

Select the required log format, then click on Next



Complete Profile

The following steps complete the profile, these are standard Sawmill steps and deafuault settings are probably acceptable.

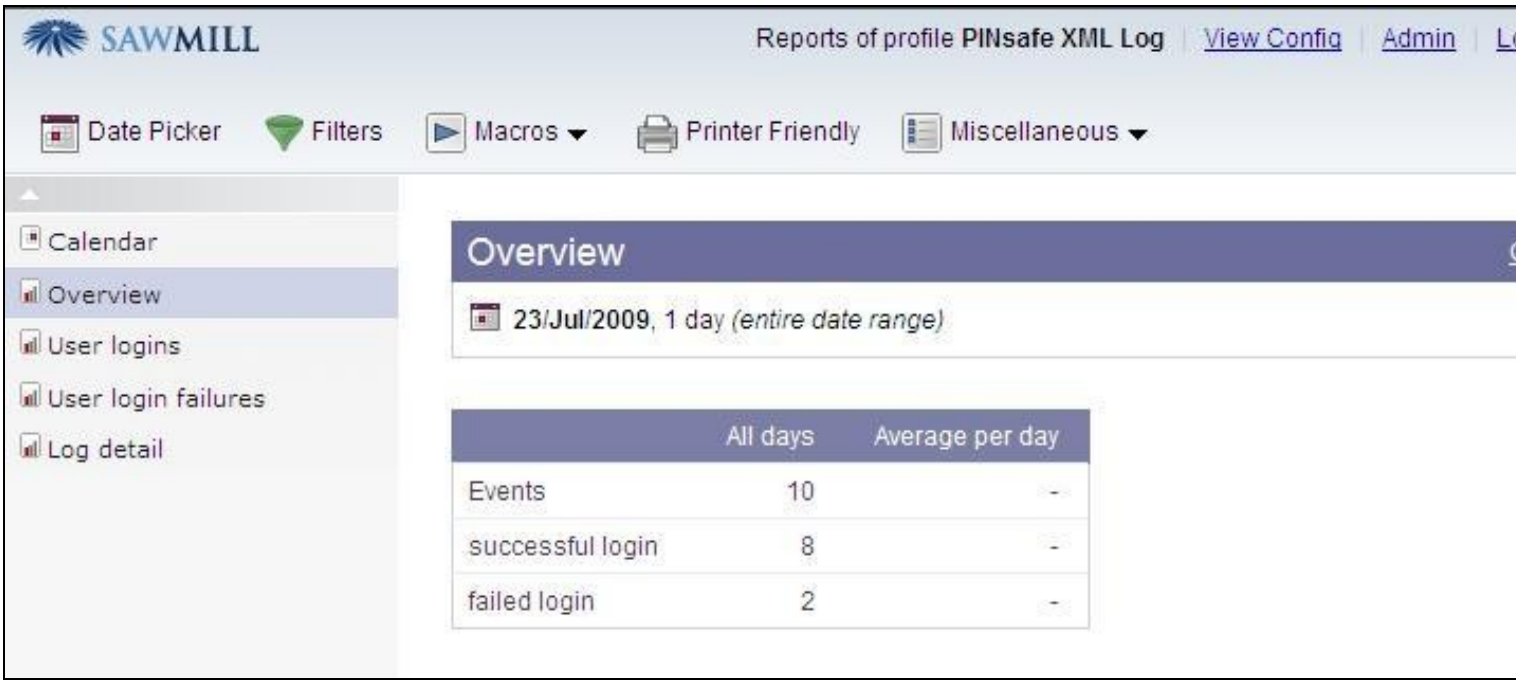
Enter the required Sawmill Database, then click on Next, then the Performance options.

Select the required Numerical Field options then click on Next.

Give a name for the profile, then click on Next.

132.7 Process Data and View Reports

Click on Process Data and View Reports to create the database and generate reports.



For scheduled processing of the PINsafe logs into the database, create a task in the Sawmill scheduler.

132.8 Verifying the Installation

Reports should show information, as in the above screen shot.

132.9 Troubleshooting

Check that the Swivel logs have some data in them, such as successful and failed login attempts..

View the Task log on the Sawmill server from Tasks/View Task Log, and check for any errors.

132.10 Known Issues and Limitations

If attempting to read PINsafe syslog output, the data needs to be sent to a syslog server first.

132.11 Additional Information

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

For Sawmill assistance please contact support@sawmill.co.uk.

133 Category:SMS Provider

134 Category:Sonicwall

135 Splunk

135.1 Introduction

This document outlines how to integrate Splunk with Swivel by using Syslog and/or PINsafe log files. The integration requires the PINsafe server to write log files to a location that can be read by the Splunk server.

135.2 Requirements

Swivel, running version 3.2 or later. (This article is based on Version 3.6 running on Windows XP)

Splunk server, (This article was based on Splunk running on Windows XP)

135.3 Installation

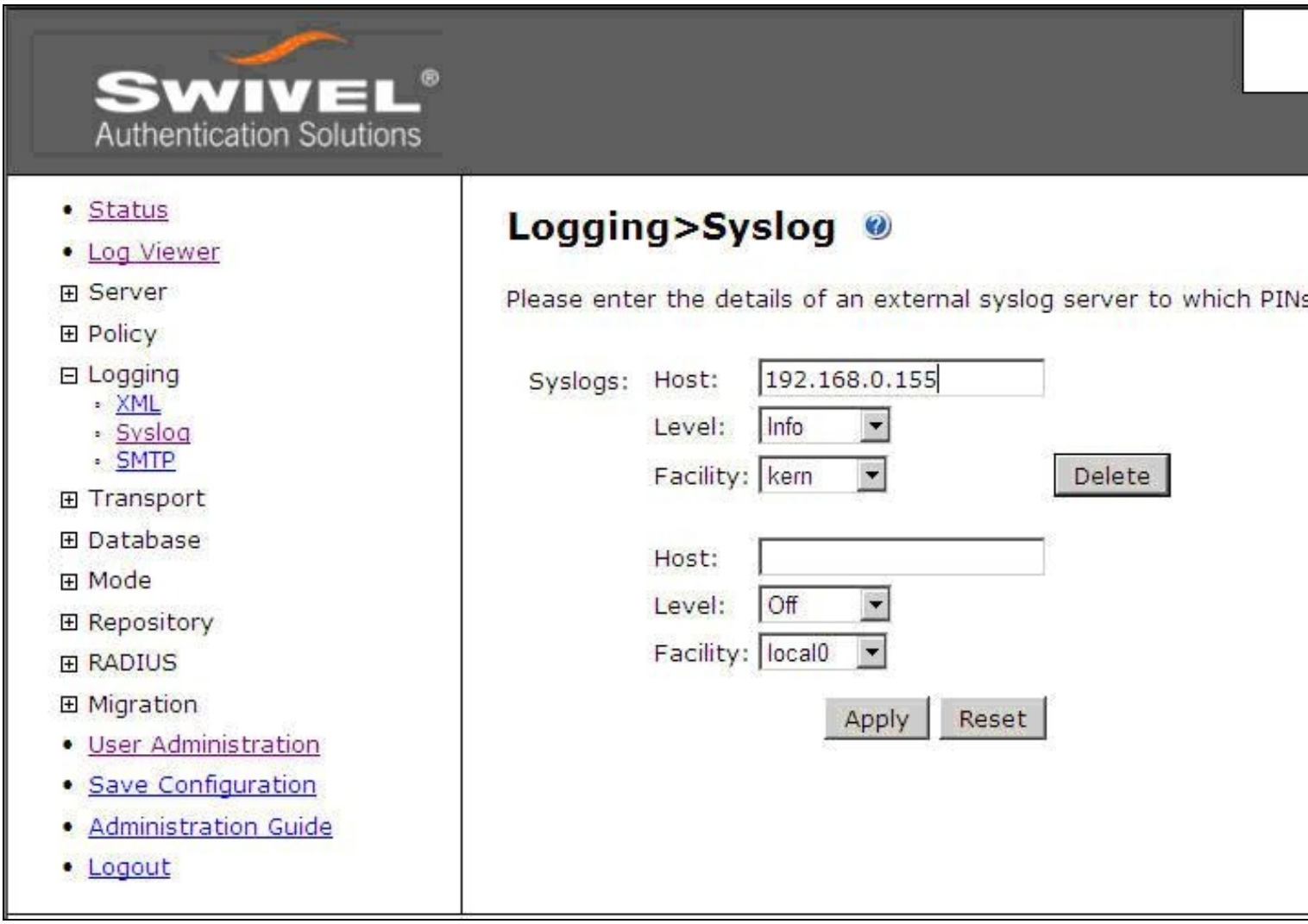
On the Swivel Administration Console, configure PINsafe to send syslog information to the Splunk server by selecting Logging/Syslog.

Enter the following information

Host: Hostname or IP address of the Splunk server

Level: The level of log information to be sent

Facility: The syslog facility in which event logs will be sent



If there is no syslog service, the PINsafe .xml log files produced by PINsafe can be imported into Splunk.

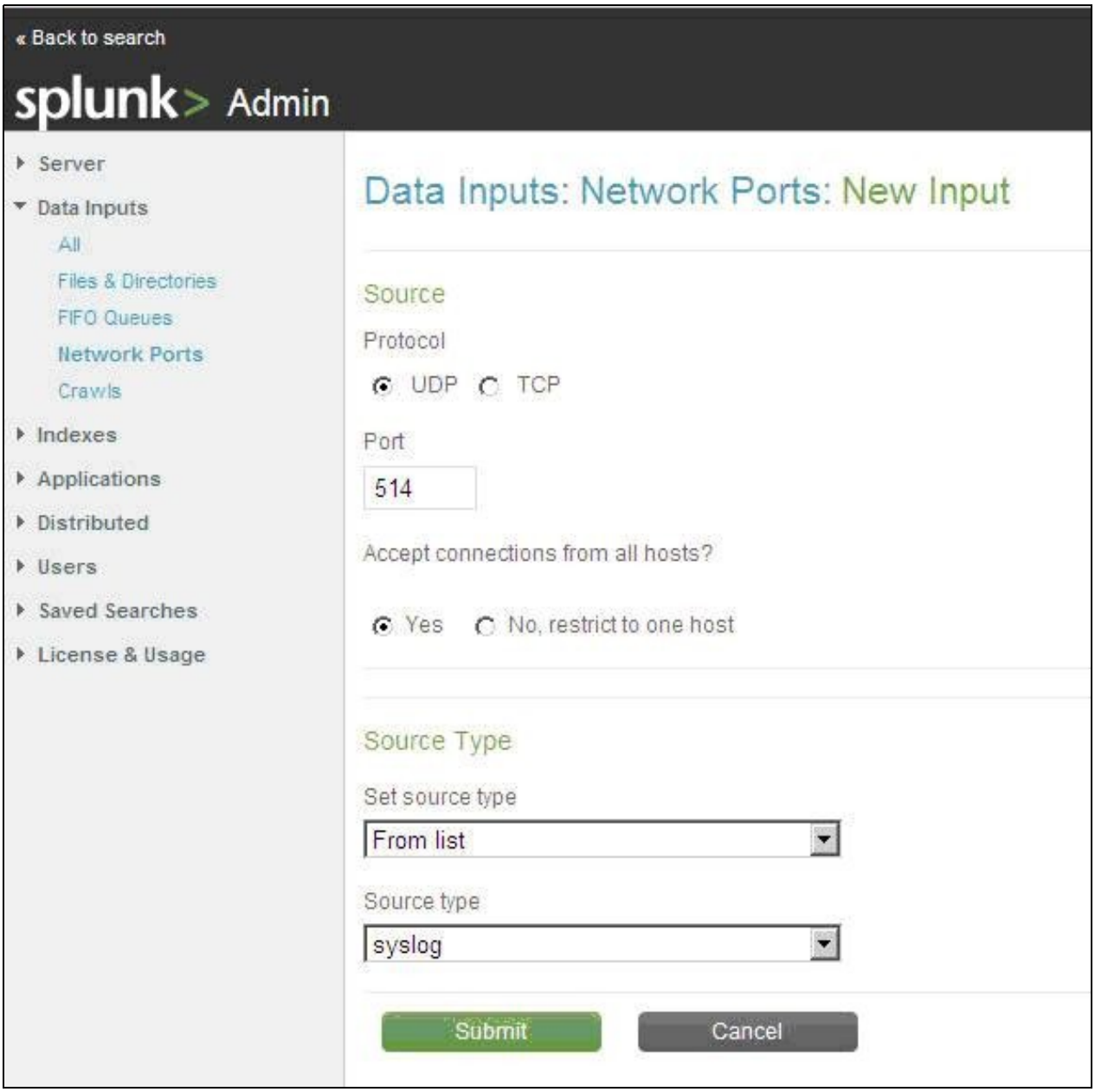
For a PINsafe appliance, they can be manually copied off to the Splunk server, see the appliance Administration guide for further details.

Alternatively a scheduled job maybe employed to copy the files across.

135.4 Splunk Syslog Configuration

On the Splunk server select Data Inputs/Network Ports then New Input, select the following options:

Source: UDP Port: 514 Accept connections from all hosts?: optional Set Source Type: From List Source Type: Syslog

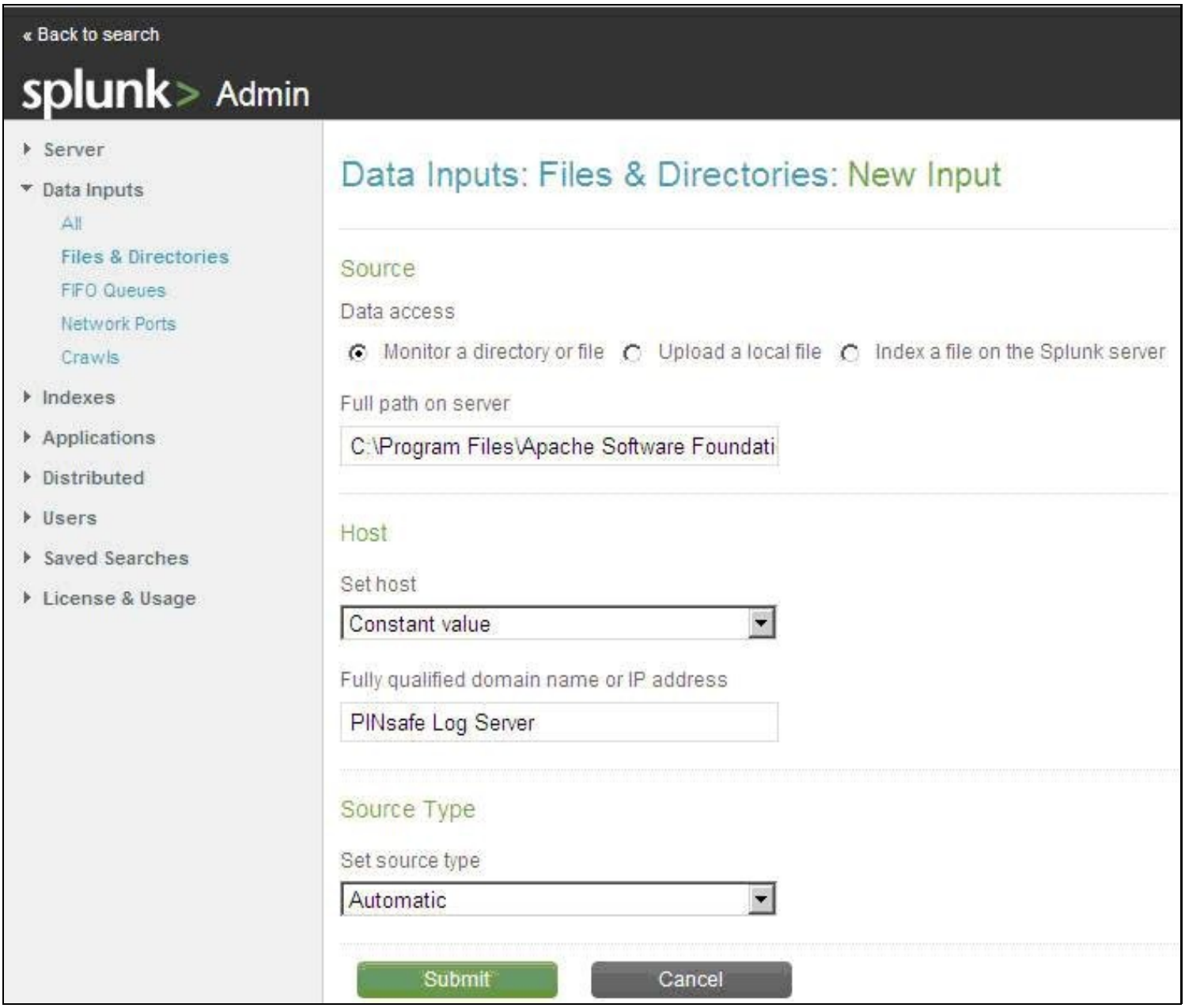


Then restart the Splunk Application by selecting Server/Control Server and Restart Now.

135.5 Splunk XML Log File Configuration

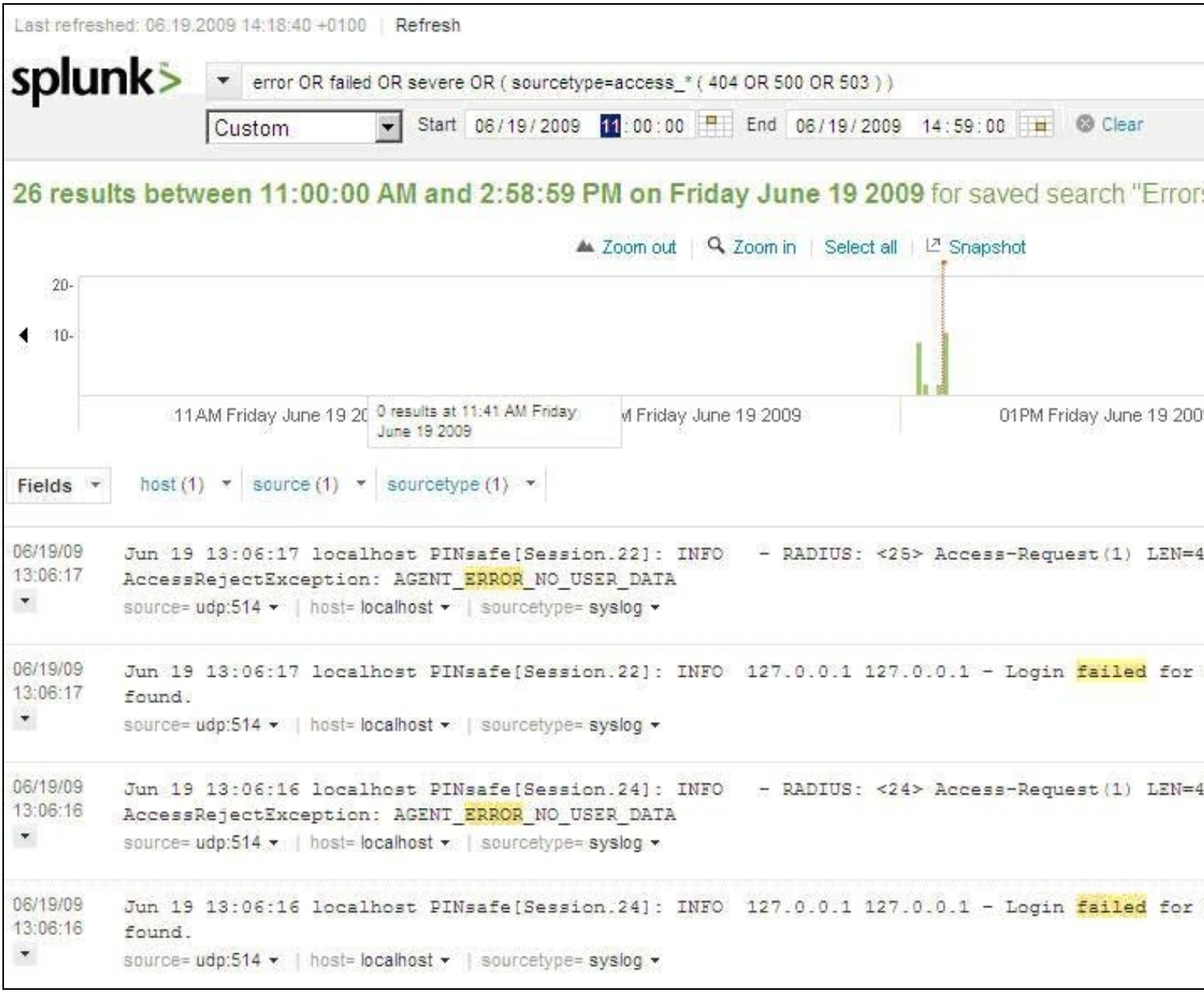
On the Splunk server select Data Inputs/Files and Directories then New Input, select the following options:

Data Access: Monitor a directory or file Full Path on server: location of log files Set Source Type: Automatic



135.6 Verifying the Installation

The Splunk screen should show input when PINsafe events occur or from historical logs.



These events can be filtered to display only specific events. Refer to Splunk documentation for more details.

135.7 Additional Information

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

136 Symantec Secure Web Gateway Integration

Media:Swivel_Secure_Symantec_SWG_Integration.pdf

137 Category:Taskbar

138 VMware View (Horizon)

138.1 Introduction

This document describes steps to configure VMware View with Swivel as the authentication server. The solution is tested with VMware View 5.1. using RADIUS authentication protocol with SMS, Token, Mobile Phone Client, and Taskbar Authentication

The VMware View Client also functions on a number of mobile phone client devices including iPhone, iPad and Android.

138.2 Credits

Swivel would like to thank the following contributors to this document:

Barry Coombs (VMware vExpert) of Computerworld Systems LTD www.computerworld.co.uk

138.3 Prerequisites

VMware View 5.1 or higher

VMware View documentation

Swivel 3.x,

138.4 Baseline

VMware View 5.1

Swivel 3.8

138.5 Architecture

The VMware View makes authentication requests against the Swivel server by RADIUS.

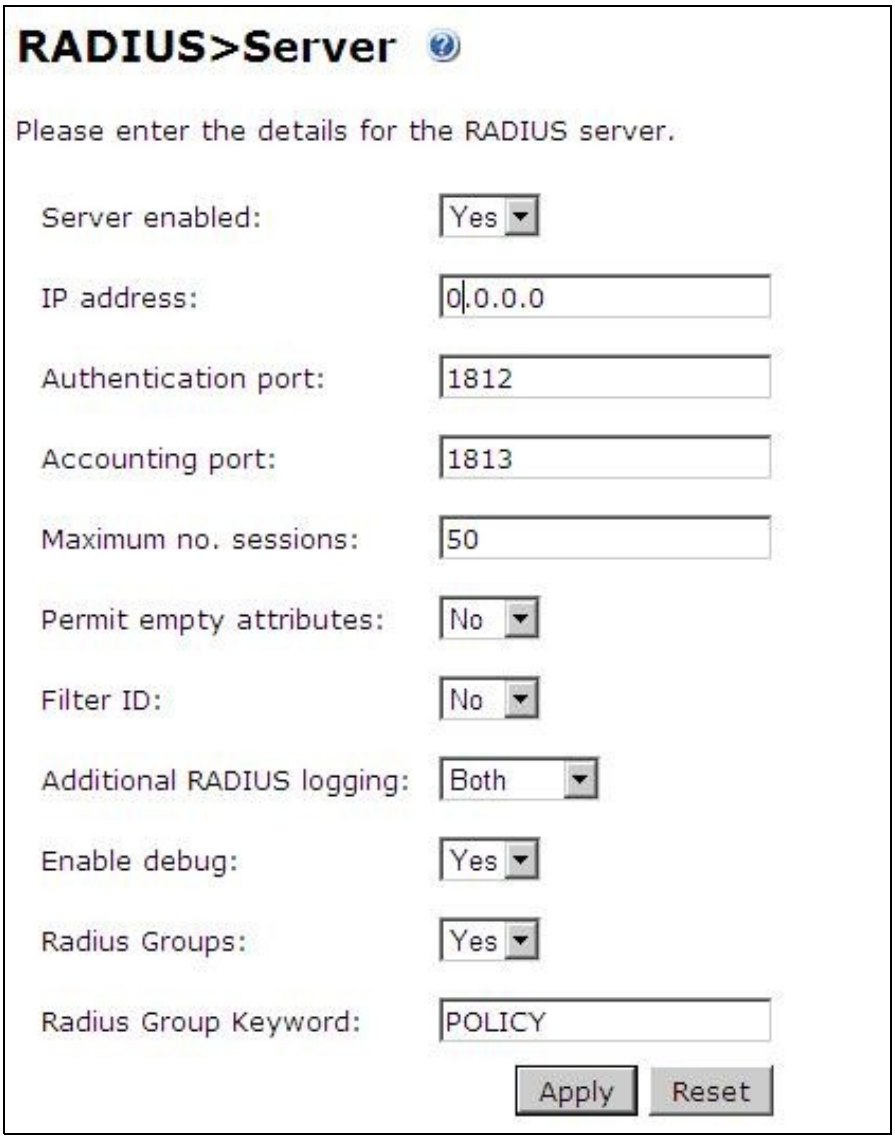
138.6 Swivel Configuration

138.6.1 Configuring the RADIUS server

Configure the RADIUS settings using the RADIUS configuration page in the Swivel Administration console by selecting RADIUS Server. To turn on RADIUS authentication set **Server Enabled** to YES. The Host or IP address is the interface which will accept RADIUS requests, leave this blank to allow RADIUS requests on any interface. (In this example the HOST IP is set to 0.0.0.0 which is the same as leaving it blank).

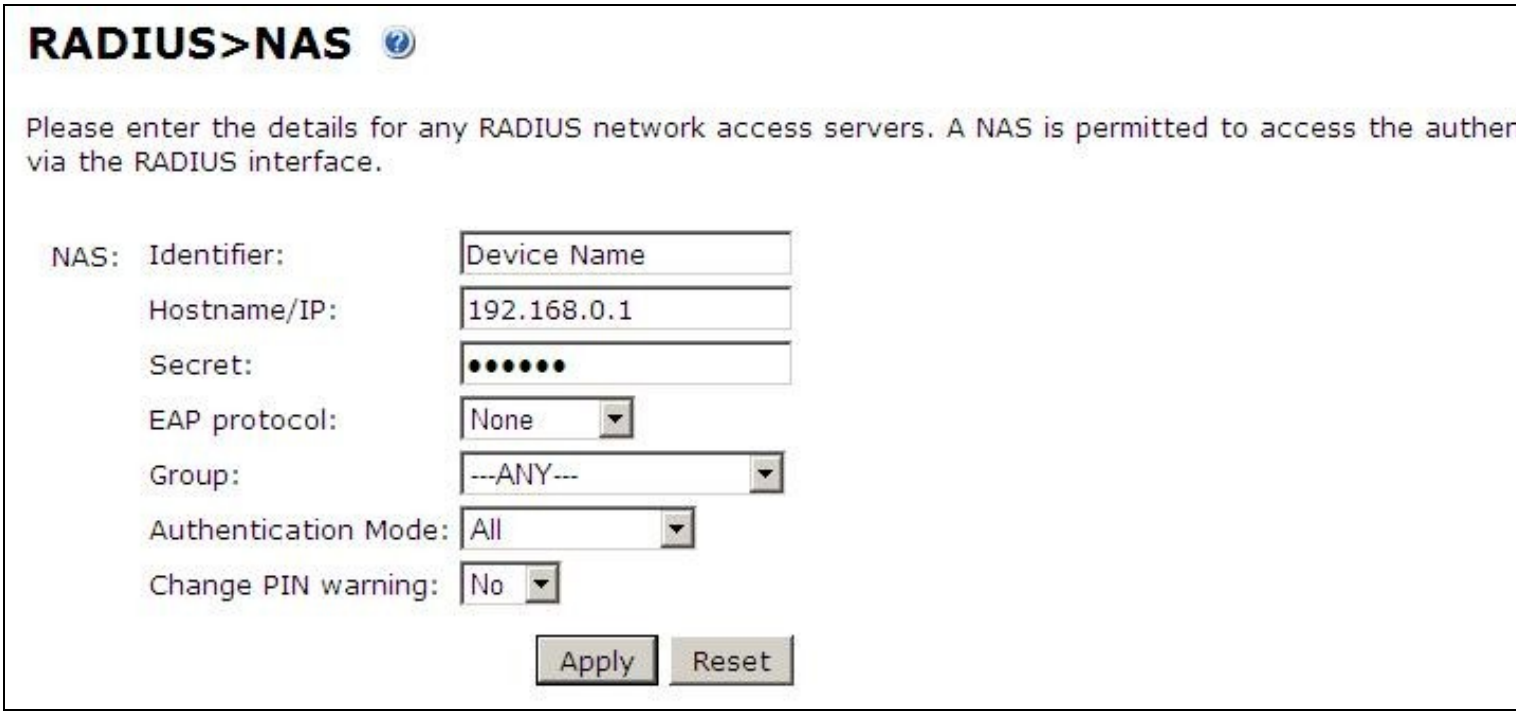
For troubleshooting RADIUS debug can be enabled together with the debug log option, see Debug how to guide

Note: for appliances, the Swivel VIP should NOT be used as the server IP address, see VIP on PINsafe Appliances



138.6.2 Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the Swivel Administration console. Enter a name for the NAS Client. The IP address has been set to the IP of the NAS Client, and the secret ?secret? assigned that will be used on both the Swivel server and the NAS Client.



You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP are supported. All users will be able to authenticate via this NAS unless authentication is restricted to a specific repository group.

138.6.3 Enabling Session creation with username

The Swivel server can be configured to return an image stream containing a TURing image in the Taskbar

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

To test your configuration you can use the following URL using a valid Swivel username:

Appliance

https://Swivel_server_IP:8443/proxy/SCImage?username=testuser

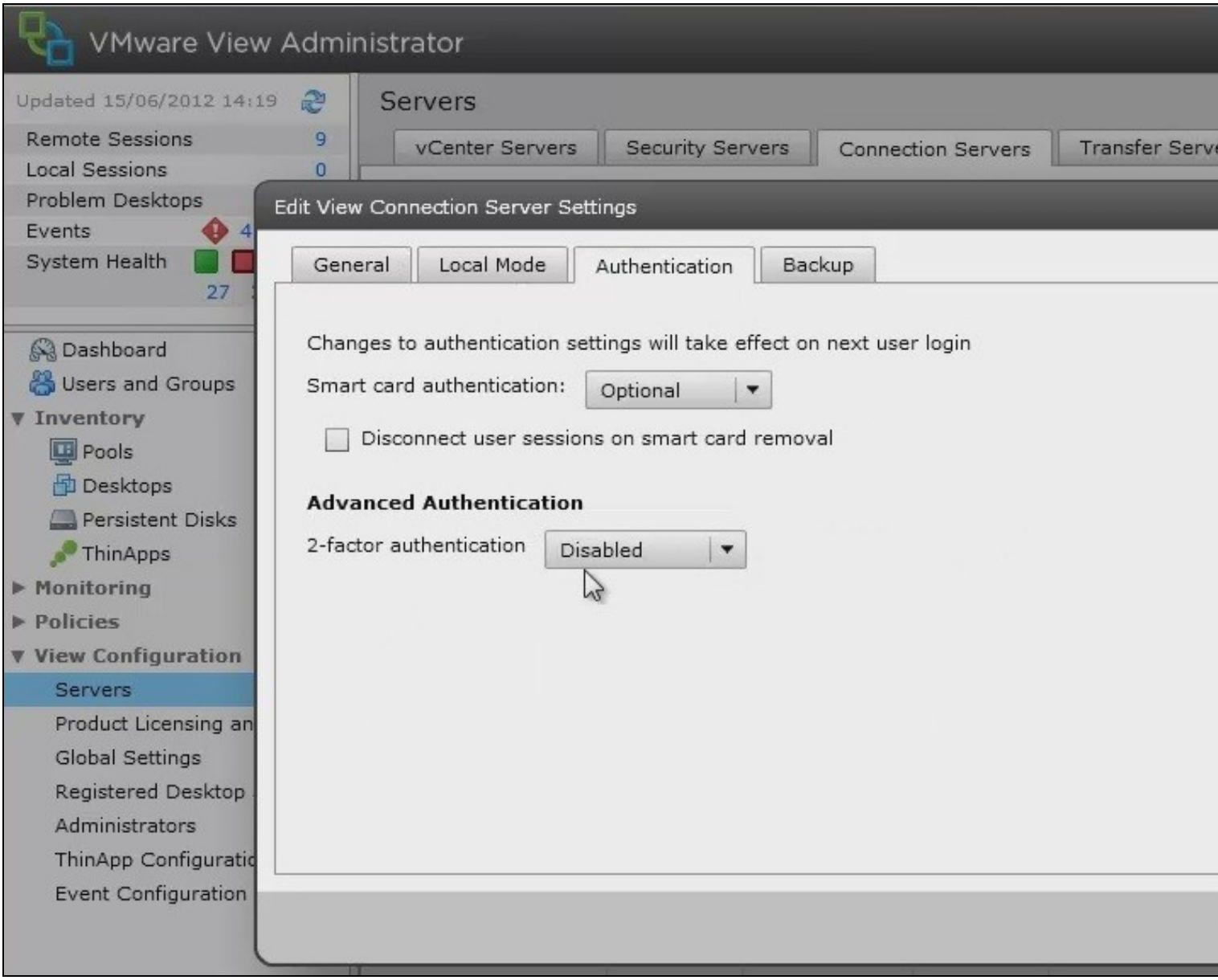
For a software only install see Software Only Installation

138.7 VMware View Configuration

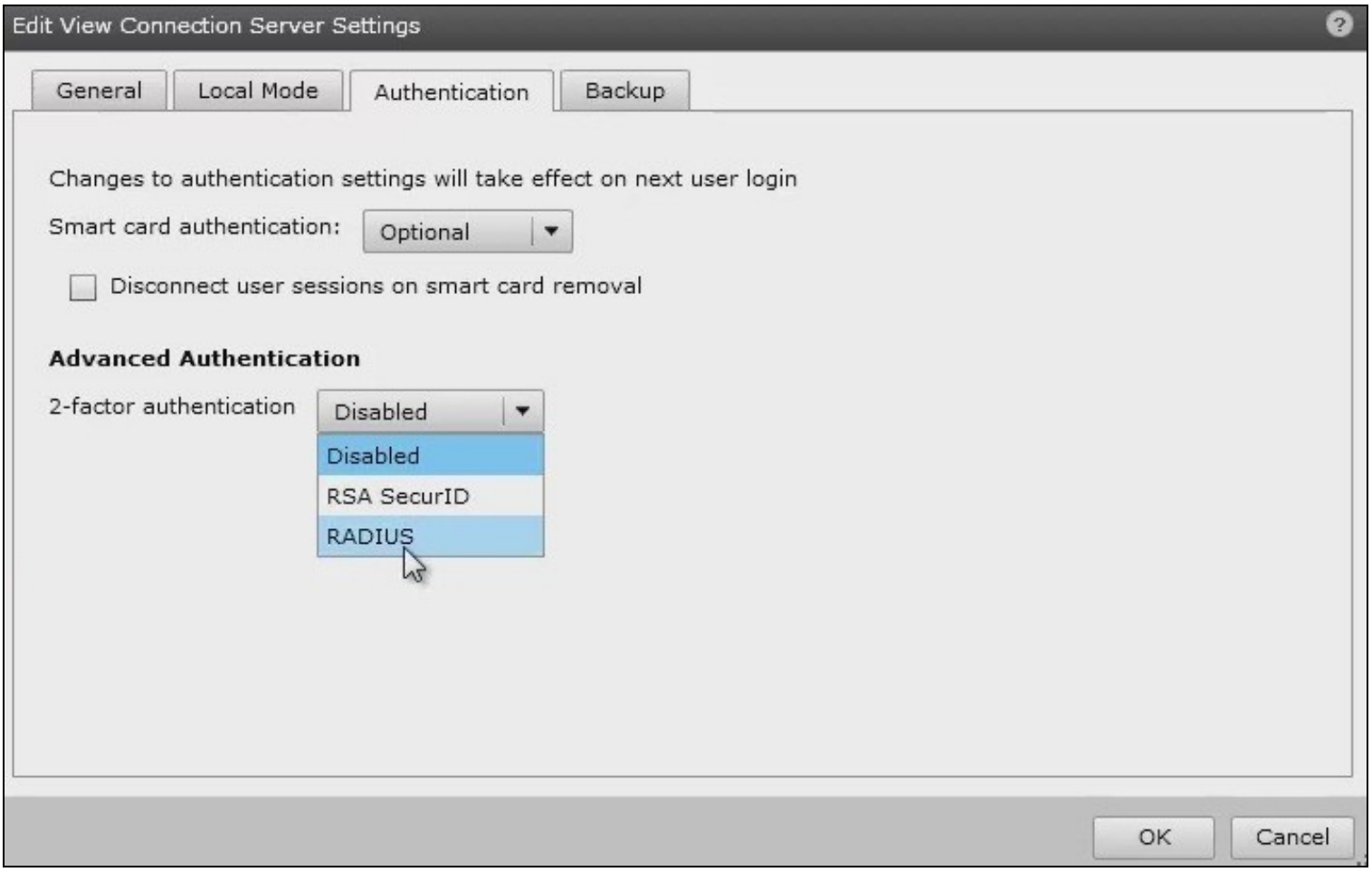
Ensure that the VMware View is fully functioning using standard authentication, then start the Swivel integration configuration.

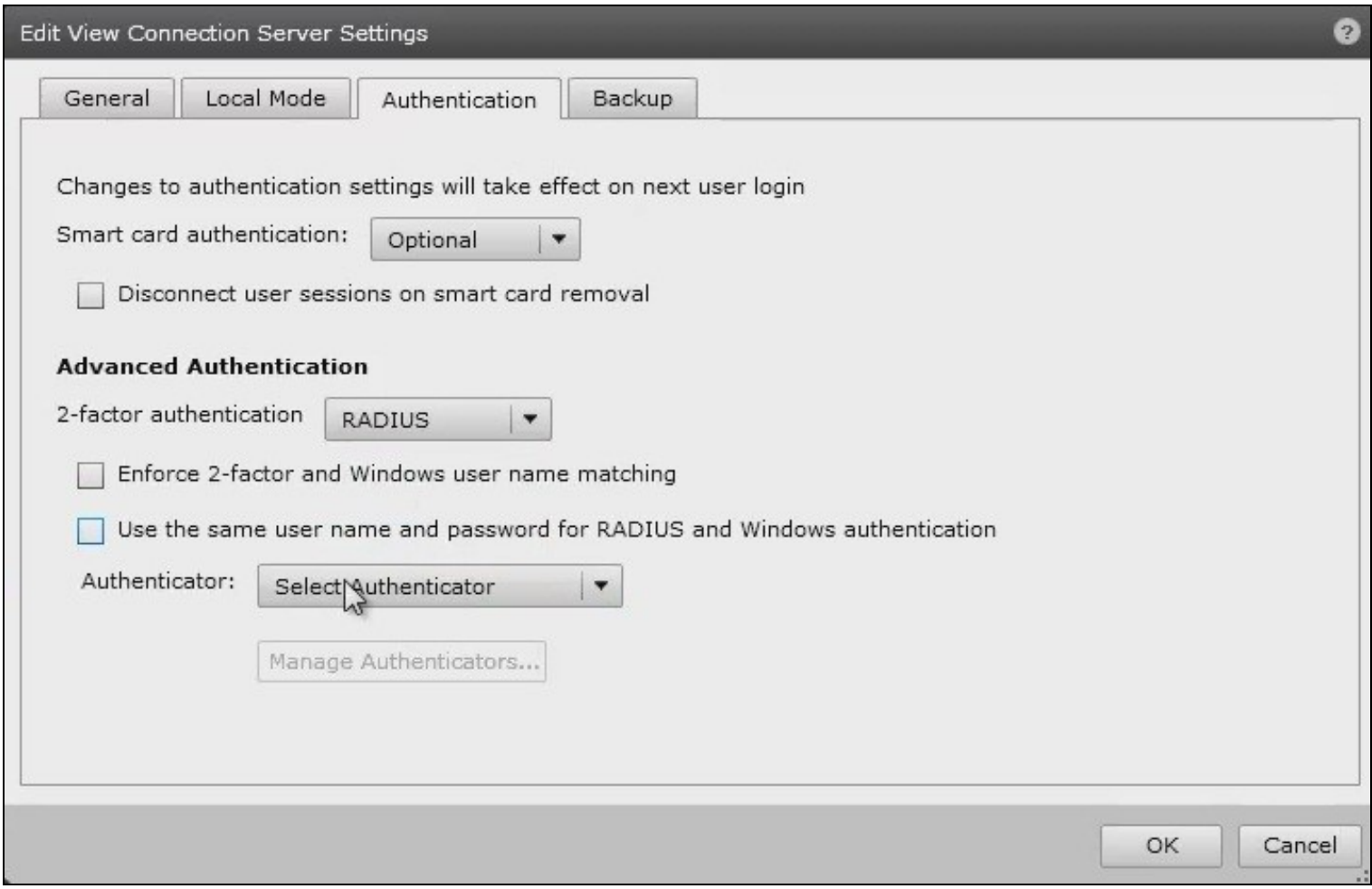
138.7.1 Create a Radius Authentication Server Group

On the VMware View Administrator select **View Configuration**, then **Servers**, select the **Connection Servers** tab and then **Edit** to bring up the Edit View Connection Server Settings and select the **Authentication** tab.



Under Advanced Authentication choose, for 2-factor authentication, the **RADIUS** tab.


Edit View Connection Server Settings
General
Local Mode
Authentication
Backup
Changes to authentication settings will take effect on next user login
Smart card authentication:
Optional
Disconnect user sessions on smart card removal
Advanced Authentication
2-factor authentication
Disabled
Disabled
RSA SecurID
RADIUS
OK
Cancel



Under Authenticator select Create new, this opens the Add RADIUS Authenticator screen, this allows a Primary and Secondary RADIUS authentication servers to be configured, enter the following:

Label: A label shown to clients

Primary Authentication Server

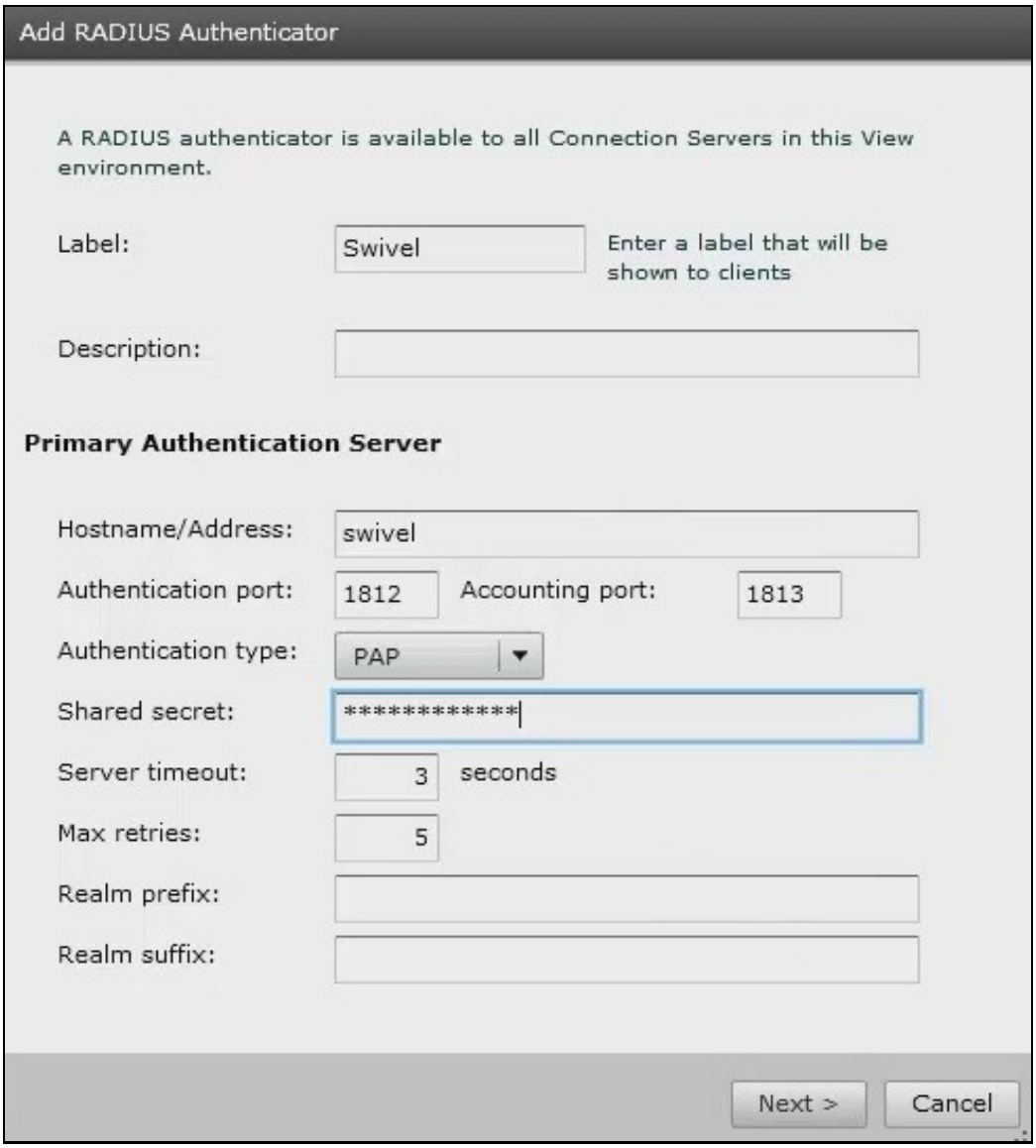
Hostname/Address: IP address of the Swivel server (This must not be a Swivel VIP for Active/Active appliances)

Authentication Type: select RADIUS authentication type, use PAP for initial setup.

Shared secret: The shared secret, the same as entered on the Swivel server

Domain Prefix: Allows a domain name to be added, and to be sent to the Swivel server in the format domain\username

Domain Suffix: Allows a domain name to be added, and to be sent to the Swivel server in the format username@domain



Clicking OK returns to to the Authentication tab.



It is possible to specify here the option **Enforce 2-factor and Windows name matching** so that the AD username is used for the Swivel authentication.

138.8 Additional Configuration Options

138.8.1 Challenge and Response with Two Stage Authentication

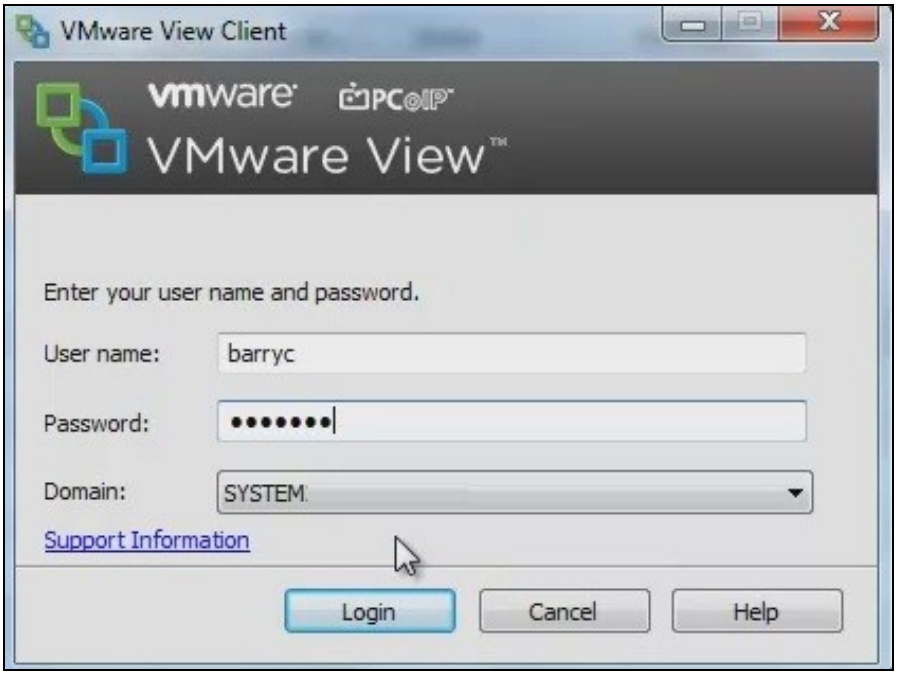
Challenge and Response is supported by using Two Stage authentication and Check Password with Repository using RADIUS PAP authentication. See Challenge and Response How to Guide. Using the option to allow the Same Username and Password for Windows and RADIUS authentication allows the AD username and password to be entered once and then challenge for a One Time Code.

138.9 Testing

The VMware View client will display fields for Username and Password. The username should be entered followed by the Swivel One Time Code in the Passcode field.



If the OTC is correct the user will be prompted for a AD Password



138.10 Troubleshooting

Check the Swivel logs for RADIUS requests. RADIUS requests should be seen even if the OTC is incorrect.

138.11 Known Issues and Limitations

None

138.12 Additional Information

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

139 WatchGuard Firebox

140 Overview

For the Watchguard Firebox integration refer to the following document WatchGuard Firebox Swivel Integration: