1 AppGate Security Server	1
2 Introduction	2
3 Prerequisites	3
3.1 Login Page customisation prerequisites	3
4 Baseline	4
5 Architecture	5
6 Swivel Configuration 6.1 Configuring the RADIUS server 6.2 Setting up Swivel Dual Channel Transports	6 6
7 AppGate Security Server Configuration 7.1 Adding a Swivel RADIUS server 7.2 Test the RADIUS authentication	7 7 9
7.3 Optional: Login Page Customisation	9
9 Additional Configuration Options	
10 Troubleshooting	13
11 Known lesues and Limitations	1/
12 Additional Information	15
12 Augustional Information	
T3 Array Networks SPX Integration	10
14 Introduction	1/
15 Additional Contributors	
16 Prerequisites	19
17 Baseline	20
18 Architecture	21
19 Installation	22
19 Installation	
19 Installation	22 23 23 23 23 23
19 Installation	22 23 23 23 23 23 24 24 24 24 24
19 Installation 20 Swivel Configuration 20.1 Configuring the RADIUS server. 20.2 Enabling Session creation with username. 20.3 Configure Password. 21 Configure the custom login page. 21.1 Editing the Login Page. 21.2 Copy the login page files. 21.3 Create a Failed Login Page. 22 Configure the Array Networks SPX.	22 23 23 23 23 23 23 24 24 24 24 24 24 24 24 24 25
 19 Installation	22 23 23 23 23 24 24 24 24 24 24 25 25 25 28
 19 Installation	22 23 23 23 23 23 23 24 24 24 24 24 24 24 24 25 25 25 25 28 300 30
19 Installation 20 Swivel Configuration 20.1 Configuring the RADIUS server. 20.2 Enabling Session creation with username. 20.3 Configure Password. 21 Configure the custom login page. 21.1 Editing the Login Page. 21.2 Copy the login page files. 21.3 Create a Failed Login Page. 22.2 Link custom page to URL for login. 22.3 Link custom page to URL for failed login. 22.4 Link custom page to URL for generic login error. 22.5 Configure URL Policy.	22 23 23 23 24 24 24 24 25 25 28 30 30 30 30 30 30 30 30
19 Installation 20 Swivel Configuration 20.1 Configuring the RADIUS server. 20.2 Enabling Session creation with username. 20.3 Configure Password. 21 Configure the custom login page. 21.1 Editing the Login Page. 21.2 Copy the login page files. 21.3 Create a Failed Login Page. 22.1 Configure RADIUS authentication. 22.2 Link custom page to URL for login. 22.3 Link custom page to URL for failed login. 22.4 Link custom page to URL for generic login error. 22.5 Configure URL Policy. 23 Verifying the Installation.	22 23 23 23 23 23 23 24 24 24 24 24 24 24 24 25 25 25 25 25 30 30 30 30 30 30 30 30
19 Installation 20 Swivel Configuration 20.1 Configuring the RADIUS server. 20.2 Enabling Session creation with username. 20.3 Configure Password. 21 Configure the custom login page. 21.1 Editing the Login Page. 21.2 Copy the login page files. 21.3 Create a Failed Login Page. 22 Configure the Array Networks SPX. 22.1 Configure RADIUS authentication. 22.2 Link custom page to URL for login. 22.3 Link custom page to URL for generic login error. 22.4 Link custom page to URL for generic login error. 22.5 Configure URL Policy. 23 Verifying the Installation. 24 Troubleshooting.	22 23 23 23 23 23 24 24 24 24 24 24 25 25 28 30 30 30 30 30 30 30 32 34
19 Installation	22 23 23 23 23 23 24 24 24 24 24 24 24 24 24 25 25 25 25 25 25 30 30 30 30 30 30 30 30 30 30 30 30 30
 19 Installation	22 23 23 23 23 23 23 24 24 24 24 24 24 24 24 25 25 28 30 30 30 30 30 30 30 30 30 30 30 30 30
19 Installation	22 23 23 23 23 23 24 24 24 24 24 24 24 24 24 24 24 25 25 25 25 25 25 25 25 25 30 30 30 30 30 30 30 30 30 30 30 30 30
19 Installation. 20 Swivel Configuration. 20.1 Configuring the RADIUS server. 20.2 Enabling Session creation with username. 20.3 Configure Password. 21 Configure the custom login page. 21.1 Editing the Login Page. 21.2 Copy the login page files. 21.3 Create a Failed Login Page. 22.1 Configure RADIUS authentication. 22.2 L Configure RADIUS authentication. 22.2 L Configure RADIUS authentication. 22.2 L Configure RADIUS authentication. 22.4 Link custom page to URL for login. 22.4 Link custom page to URL for generic login error. 22.5 Configure URL Policy. 23 Verifying the Installation. 24 Troubleshooting. 25 Known Issues and Limitations. 26 Additional Information. 27 AuthControl Desktop. 28 Introduction.	22 23 23 23 23 23 23 24 24 24 24 24 24 24 24 24 24 24 25 28 30 30 30 30 30 30 30 30 30 30 30 30 30
19 Installation. 20 Swivel Configuration. 20.1 Configuring the RADIUS server. 20.2 Enabling Session creation with username. 20.3 Configure Password. 21 Configure the custom login page. 21.1 Editing the Login Page. 21.2 Copy the login page files. 21.3 Create a Failed Login Page. 22. Configure RADIUS authentication. 22.1 Configure RADIUS authentication. 22.2 Link custom page to URL for login. 22.3 Link custom page to URL for login error. 22.4 Link custom page to URL for generic login error. 22.5 Configure UAL Policy. 23 Verifying the Installation. 24 Troubleshooting. 25 Known Issues and Limitations. 26 Additional Information. 27 AuthControl Desktop. 28 Introduction. 29 Aventail Integration.	22 23 23 23 23 23 24 24 24 24 24 24 24 24 25 25 25 25 25 25 25 25 25 25 25 25 25
19 Installation. 20 Swivel Configuration. 20.1 Configuring the RADIUS server. 20.2 Enabling Session creation with username. 20.3 Configure Password. 21 Configure the custom login page. 21.1 Editing the Login Page. 21.2 Copy the login page files. 21.3 Create a Failed Login Page. 22.4 Configure the Array Networks SPX. 22.1 Configure RADIUS authentication. 22.2.2 Link custom page to URL for login. 22.3 Link custom page to URL for foigin error. 22.4 Link custom page to URL for foigin error. 22.5 Configure URL Policy. 23 Verifying the Installation. 24 Troubleshooting. 25 Known Issues and Limitations. 26 Additional Information. 27 AuthControl Desktop. 28 Introduction. 29 Aventail Integration. 30 Introduction.	22 23 23 23 23 23 23 24 24 24 24 24 24 24 24 25 25 28 30 30 30 30 30 30 30 30 30 30 30 30 30
19 Installation	22 23 23 23 23 23 24 24 24 24 24 24 25 25 25 25 25 25 25 25 25 25 30 30 30 30 30 30 30 30 30 30 30 30 30
19 Installation 20 Swivel Configuration 20.1 Configuring the RADIUS server. 20.3 Configure Password. 21 Configure the custom login page. 21.1 Ediling the Login Page 21.2 Copy the login page files. 21.3 Create a Failed Login Page. 22.1 Configure the Array Networks SPX 22.1 Configure the Array Networks SPX 22.1 Configure the Array Network SPX 22.2 Link custom page to URL for login. 22.3 Link custom page to URL for login. 22.4 Link custom page to URL for generic login error. 22.5 Configure URL Policy. 23 Verifying the Installation. 24 Troubleshooting. 25 Known Issues and Limitations. 26 Additional Information. 27 AuthControl Desktop. 28 Introduction. 29 Aventail Integration. 21 Torealistes. 22 Aution. 23 Verifying The Installation. 24 Troubleshooting. 25 Known Issues and Limitations. 26 Additional Information. 27 AuthControl Desktop. 28 Introduction. 30 Introduction. 31 Prerequisites. 32 Baseline. </td <td>22 23 23 23 23 23 23 24 24 24 24 24 24 24 24 25 28 30 30 30 30 30 30 30 30 30 30 30 30 30</td>	22 23 23 23 23 23 23 24 24 24 24 24 24 24 24 25 28 30 30 30 30 30 30 30 30 30 30 30 30 30

24 Swivel Configuration	44
34 Source Configuration.	
24.2 Employing Species with upprame	
34.2 Endbling Session Cleanon Transports	
54.5 Setting up Swiver Duar Channer Transports	
	45
35 Sonicwall Aventall Integration.	
35.1 Configuring The Sonicwall Aventali for RADIUS Authentication	
35.2 Test the RADIUS authentication	
35.3 Modifying the Aventail Sign-In Page for Turing	47
35.4 Creating A Custom Authentication Request Page	
36 Verifying the Installation	51
37 Known Issues and Limitations	52
38 Configuration Options	53
38.1 Turing Image Size	
38.2 Security String Index	
38.3 TUBing and SMS	
38.4 Manual Turing Display	54
38 5 Automated Turing Display	54
39 Troubleshooting	
40 Additional Information	56
41 Barracuda SSL VPN Integration	57
42 Introduction	50
42 Proroquisitos	50
45 Fielequisites	
44 Pasalina	60
	00
AF Averbitecture	61
45 Architecture	01
	~~~~
46 Swiver Configuration.	
46.1 Configuring the RADIUS server.	
46.2 Enabling Session creation with username	62
47 Barracuda SSL VPN Configuration	63
47.1 Create an authentication scheme	63
47.2 Barracuda RADIUS Configuration	65
47.3 Test the RADIUS authentication	68
47.4 Additional Configuration options	
48 Testing	70
49 Troubleshooting	72
50 Known Issues and Limitations	
51 Additional Information	
52 Romgar	75
52 Introduction	76
So introduction	
54 Proroquisitos	77
34 FIEICYUISIICS	
	70
JO DASEIIIIE	
	70
56 Architecture	
57 Swivel Configuration.	80
57.1 Configuring the RADIUS server	80
57.2 Configuring Two Stage Authentication	80
57.3 Setting up Swivel Dual Channel Transports	80
58 Bomgar Configuration	81
58.1 Test the RADIUS authentication	81
58.2 Optional	81
59 Testing	82
-	
60 Additional Configuration Options	83
61 Troubleshooting	
~ · · · · · · · · · · · · · · · · · · ·	
62 Known Issues and Limitations	85
63 Additional Information	86

64	Checkpoint EndPointSecurityVPN Integration	87
65	Checkpoint Mobile Access	88
66	Checkpoint SecureClient Integration	89
67	Introduction	90 90 90 90
68	Swivel Configuration 68.1 Configuring the RADIUS server 68.2 Enabling Session creation with username	<b>91</b> 91 91 91
69	Configuring the Checkpoint VPN-1/Firewall-1 69.1 Checkpoint VPN-1/Firewall-1 configuration Overview 69.2 Test the RADIUS authentication 69.3 Modifying the Checkpoint SecureClient for Single Channel and Advanced SMS features	<b>92</b> 92 93 93
70	Removing the Swivel SecureClient	95
71	Verifying the Installation	96
72	Bulk deployment	97
73	Troubleshooting	98
74	Known Issues and Limitations	99
75	Additional Information	.100
76	Cisco AnvConnect	.101
77	Introduction	102
78		.103
70		104
15	79.2 Install the Cisco ApyConnect Client	.104
00	Swivel medified ApyConnect Client for TUPing and PINned	107
00	80.1 Download the clerent modifications	.107
	80.2 Prerequisites for the modified client	.107 .107 .107
81	Cisco ASA Integration	.108
82	Introduction	.109
00		.109
83	83.1 Login Page customisation prerequisites	.110
84	Baseline	.111
85	Architecture	.112
86	Swivel Configuration	.113
	86.1 Configuring the RADIUS server	.113 .113
87	Cisco ASA Configuration	114
	87.1 Create a Radius Authentication Server Group.	.114
	87.3 Create a Connection Profile (Tunnel Group)	.116
		.120
88	resting	.125
89	Additional Configuration Options	<b>.129</b> .129
90	Troubleshooting	.130
91	Known Issues and Limitations	.131
92	Additional Information	.132

93 Cisco IPSEC Client Integration	133
93.1 Introduction	133
93.2 Prereauisites	133
93.3 Baseline	133
93 4 Architecture	133
04 Swivel Configuration	124
04.1 Configuring the DADIUS conver	104
	134
94.2 Enabling Session creation with username	134
94.3 PINsate Client Configration	134
94.4 Cisco VPN Server Configuration	134
94.5 Cisco IPSEC Client Configuration	134
94.6 Additional Configuration Options	134
94.7 Troubleshooting	134
94.8 Known Issues and Limitations	135
04.0 Additional Information	125
94.9 Additional miormation	135
05 01-22 04 500	400
95 CISCO SA 520	136
95.1 Introduction	136
95.2 Prerequisites	136
95.3 Baseline	136
95.4 Architecture	136
96 Swivel Configuration	137
96.1 Configuring the BADILIS server	137
96.2 Setting un PINsafe Dual Channel Transports	127
06.2 Octang dp i invade Duai Orlainet Transporta	107
90.9 USCO GA 320 CONNYUNATION	13/
So.4 Lesting	138
96.5 Additional Configuration Options	139
96.6 Troubleshooting	139
96.7 Known Issues and Limitations	139
96.8 Additional Information	139
97 Citrix Access Gateway 5 VPX	140
97.1 Introduction	140
98 Citrix Access Cateway Access Controller 5.0	1/1
00 Cityiy Access Cataway Advanced 4 y	140
Se China Access Galeway Advanced 4.2.	142
100 Internation	140
IVV Introduction	143
101 Prerequisites	144
101 Prerequisites	144
101 Prerequisites	144 145
101 Prerequisites	144 145
101 Prerequisites	144 145 146
101 Prerequisites	<b>144</b> <b>145</b> <b>146</b> 146
101 Prerequisites	144 145 146 146 146
101 Prerequisites	144 145 146 146 146 146
101 Prerequisites	144 145 146 146 146 146 146 146
101 Prerequisites	144 145 146 146 146 146 146 146 146
101 Prerequisites	144 145 146 146 146 146 146 146 146 146
101 Prerequisites	144 145 146 146 146 146 146 146 146 146
101 Prerequisites	<b>144</b> <b>145</b> 146 146 146 146 146 146 146
101 Prerequisites 102 Installation 103 Additional Installation Options 103.1 Remove automatic TURing image automatically displaying 103.2 Prevent browser caching TURing image. 103.3 Prevent the cursor from automatically entering the OTC field. 103.4 Change the TURing button text 103.5 Verifying the Installation 103.6 Uninstalling the PINsafe Integration 103.7 Troubleshooting. 103.8 Known Issues and Limitations 103.9 Additional Information	<b>144</b> <b>145</b> 146 146 146 146 146 146 146 146
101 Prerequisites	144 145 146 146 146 146 146 146 146 146
101 Prerequisites	144 145 146 146 146 146 146 146 146 146 146 146 146
101 Prerequisites	144 145 146 146 146 146 146 146 146 146 146 146 146
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.	144 145 146 146 146 146 146 146 146 146 146 146
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.	144 145 146 146 146 146 146 146 146 146 146 146 146 146 146
101 Prerequisites	144 145 146 146 146 146 146 146 146 146 146 146 147 147
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.	144 145 146 146 146 146 146 146 146 146 146 146 147 148 147 148
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.	144 145 146 146 146 146 146 146 146 146 146 146 148 149
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.	144 145 146 146 146 146 146 146 146 146 146 146 147 147 147 147 147
101 Prerequisites.         102 Installation         103 Additional Installation Options         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.	144 145 146 146 146 146 146 146 146 146 146 146 146 147 149 150
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.         108 Architecture.	144 146 146 146 146 146 146 146 146 146 146 147 148 147 148 149 150 151
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.	144 145 146 146 146 146 146 146 146 146 146 146 147 148 147 147 148 149 149 149 149 149 149 149 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 146 
101 Prerequisites	144 145 146 146 146 146 146 146 146 146 146 147 147 147 147 149 151 151
101 Prerequisites	144 145 146 146 146 146 146 146 146 146 147 147 148 149 151 151
101 Prerequisites	144 146 146 146 146 146 146 146 146 146 146 146 146 147 148 149 149 151 152 152
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.9 Additional Information.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.         108 Architecture.         109 Swivel Configuration.         109.1 Configuring the RADIUS server.         109.2 Enabling Session creation with username.         109.3 Setting up Swivel Dual Channel Transports.	144 146 146 146 146 146 146 146 146 146 146 147 148 149 149 151 152 152
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103 Additional Installation Options.         103 1 Remove automatic TURing image automatically displaying.         103.1 Pervent browser caching TURing image.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Uninstalling the PlNsafe Integration.         103.6 Uninstalling the PlNsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.         108 Architecture.         109.1 Configuration.         109.2 Configuration.         109.3 Setting up Swivel Dual Channel Transports.	144 146 146 146 146 146 146 146 146 146 146 146 147 149 149 151 151 152 152 152
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.         108 Architecture.         109 Swivel Configuration.         109.1 Configuring the RADIUS server.         109.2 Enabling Session creation with username.         109.3 Setting Use Server.	144 146 146 146 146 146 146 146 146 146 146 146 146 147 148 149 150 151 152 152 152 152 152 152
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.         108 Architecture.         109 Swivel Configuration.         103.1 Configuring the RADIUS server.         103.2 Enabling Session creation with username.         103.3 Setting up Swivel Dual Channel Transports.         110 Citrix Access Gateway Enterprise Edition Configuration.         110.1 Citrix Access Gateway Enterprise Edition Configuration.	144 146 146 146 146 146 146 146 146 146 146 146 146 147 148 149 150 152 152 152 152 152
101 Prerequisites         102 Installation         103 Additional Installation Options         103.1 Remove automatic TURing image automatically displaying         103.2 Prevent browser caching TURing image         103.3 Prevent the cursor from automatically entering the OTC field         103.4 Change the TURing button text.         103.5 Verifying the Installation         103.4 Change the TURing button text.         103.5 Verifying the Installations.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites         107 Baseline.         108 Architecture.         109 Swivel Configuration.         109.1 Configuring the RADIUS server.         109.2 Enabling Session creation with username.         109.3 Setting up Swivel Dual Channel Transports.         110 Citrix Access Gateway Enterprise Edition Configuration.         103.2 Stating Session creation with username.         103.2 Enabling Session creation with username.         103.2 Stifting the BADIUS and transports.	144 146 146 146 146 146 146 146 146 146 146 146 146 146 147 148 149 151 152 152 152 152 152 152 152
101 Prerequisites         102 Installation         103 Additional Installation Options         103.1 Remove automatic TURing image automatically displaying         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.         108 Architecture.         109 Swivel Configuration.         109.1 Configuring the RADIUS server.         109.2 Enabling Session creation with username.         109.3 Setting up Swivel Dual Channel Transports.         110 Citrix Access Gateway Enterprise Edition Configuration.         110.1 Citrix Access Gateway Enterprise Edition RADIUS configuration.         110.2 Test the RADIUS authentication	144 146 146 146 146 146 146 146 146 146 146 147 147 148 149 151 151 152 152 152 153 159
101 Prerequisites         102 Installation         103 Additional Installation Options         103.1 Remove automatic TURing image automatically displaying         103.2 Prevent browser caching TURing image         103.3 Prevent the cursor from automatically entering the OTC field         103.4 Change the TURing button text.         103.5 Verifying the Installation         103.6 Uninstalling the PINsate Integration         103.7 Troubleshooting         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction         106 Prerequisites         107 Baseline.         108 Architecture.         109 Swivel Configuration.         109.1 Configuring the RADIUS server.         109.2 Enabling Session creation with username.         109.3 Setting up Swivel Dual Channel Transports.         110 Citrix Access Gateway Enterprise Edition Configuration.         110.1 Citrix Access Gateway Enterprise Edition Configuration.         110.2 Test the RADIUS authentication.	144 146 146 146 146 146 146 146 146 146 146 146 146 147 148 149 149 150 152 152 153 159
101 Prerequisites         102 Installation         103 Additional Installation Options         103.1 Remove automatic TURing image automatically displaying         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsate Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.         108 Architecture.         109.1 Configuring the RADIUS server.         109.2 Enabling Session creation with username.         109.3 Setting up Swivel Dual Channel Transports.         110 Citrix Access Gateway Enterprise Edition RADIUS Configuration.         110.2 Text Advanced Access Gateway Enterprise Edition RADIUS Configuration.         110.2 Text Advanced Access Gateway Enterprise Edition RADIUS Configuration.         110.2 Text Her RADIUS authentication.	144 146 146 146 146 146 146 146 146 146 146 146 147 148 149 151 151 152 152 153 153 159 159
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.         109 Swivel Configuration.         109.1 Configuration.         109.2 Enabling Session creation with username.         109.3 Setting up Swivel Dual Channel Transports.         110 Citrix Access Gateway Enterprise Edition Configuration.         110.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration.         111.1 Login Page Customisation.         111.1 Login Page Customisation.	144 146 146 146 146 146 146 146 146 146 146 146 146 146 147 149 151 151 152 152 152 153 159 160 160
101 Prerequisites.         102 Installation.         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooling.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.         108 Architecture.         109 Swivel Configuration.         109.1 Configuring the RADIUS server.         109.2 Enabling up Swivel Dual Channel Transports.         110 Citrix Access Gateway Enterprise Edition Configuration.         110.1 Citrix Access Gateway Enterprise Edition RADIUS Configuration.         110.1 Citrix Access Gateway Enterprise Edit	144 146 146 146 146 146 146 146 146 146 146 146 146 147 148 149 150 151 152 152 153 153 159 160 161
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Change the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.         109 Swivel Configuration.         109.1 Configuration.         109.2 Enabling Session creation with username.         109.3 Setting up Swivel Dual Channel Transports.         110 Citrix Access Gateway Enterprise Edition Configuration.         110.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration.         111 Additional Configuration.         111.1 Login Page Customisation         111.1 Additional Login Customisation	144 146 146 146 146 146 146 146 146 146 146 146 147 148 149 150 151 152 152 152 152 153 159 161 161 162
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent browser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Charge the TURing button text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsafe Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.         108 Achitecture.         109 Swivel Configuration.         109.1 Configuring the RADIUS server.         109.2 Enabling Session creation with username.         109.3 Setting up Swivel Dual Channel Transports.         110 Citrix Access Gateway Enterprise Edition Configuration.         110.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration.         110.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration.         111.1 Login Page Customisation options.         111.1 Additional Configuration Options.         111.1 Login Page Customisation options.         111.1 Login Page Customisation opt	144 146 146 146 146 146 146 146 146 146 146 146 146 146 147 147 148 149 151 152 152 153 153 153 159 160 162 162
101 Prerequisites.         102 Installation         103 Additional Installation Options.         103.1 Remove automatic TURing image automatically displaying.         103.2 Prevent horowser caching TURing image.         103.3 Prevent the cursor from automatically entering the OTC field.         103.4 Charge the TURing buton text.         103.5 Verifying the Installation.         103.6 Uninstalling the PINsate Integration.         103.7 Troubleshooting.         103.8 Known Issues and Limitations.         103.9 Additional Information.         104 Citrix Access Gateway Enterprise Edition 10.         105 Introduction.         106 Prerequisites.         107 Baseline.         108 Architecture.         109 Swivel Configuration.         103.1 Configuring the RADIUS server.         103.2 Enabling Session creation with username.         103.3 Enting up Saved Puter Prise Edition Configuration.         105.1 Citrix Access Gateway Enterprise Edition Configuration.         110.1 Citrix Access Gateway Enterprise Edition Configuration.         110.1 Citrix Access Gateway Enterprise Edition RADIUS Configuration.         110.1 Citrix Access Gateway Enterprise Edition RADIUS Configuration.         110.2 Test the RADIUS authentication.         111.1 Login Page Customisation options.         111.1 Login Page Cust	144 146 146 146 146 146 146 146 146 146 146 146 146 147 149 151 151 152 152 152 153 159 160 162 162

113 Uninstall/Removing the integration	165
114 Troubleshooting	166
115 Known Issues and Limitations	167
116 Additional Information	168
117 Citrix Access Gateway Enterprise Edition 8	<b>169</b> 169 169 169 169
118 Swivel Configuration	170
<ul> <li>118.1 Configuring the RADIUS server</li></ul>	
119 Citrix Access Gateway Enterprise Edition 9	<b>174</b> 174 174 174 174 174
120 Swivel Configuration	
120.1 Configuring the RADIUS server	
121 Citrix Access Gateway Standard 4.x	186
122 Introduction	187
123 Prerequisites	188
124 Baseline	
125 Architecture	
126 Installation	
127 Swivel Configuration 127.1 Configuring the RADIUS server 127.2 Setting up PINsafe Dual Channel Transports 127.3 Citrix Access Gateway Standard Edition Integration	<b>192</b> 192 192 192
128 Additional Information	193
129 Citrix Access Gateway Standard 5.x	194
130 Introduction	195
131 Prerequisites	196
132 Baseline	197
133 Architecture	198
134 Installation	199
135 Swivel Configuration	
136 Citrix Access Gateway Standard Edition Integration	
136.1 CAG RADIÚS Properties	
137 Additional Installation Options	
138 Verifying the Installation	

	205
140 Troubleshooting	206
141 Known Issues and Limitations	207
142 Additional Information	
143 Citrix Access Gateway Web Interface Proxy	
144 Introduction	210
145 Prerequisites	
146 Baseline	212
147 Architecture	
148 Installation	
148.1 PINsafe and Web Interface Integration Configuration	214
148.2 CAG Standard and CAG VPX configuration and installation.	
148.3 Clinx web interface configuration and installation. 148.4 Additional Installation Options.	
149 Verifying the Installation	219
150 Uninstalling the PINsafe Integration	
151 Troubleshooting	
152 Known Issues and Limitations	
153 Additional Information	
154 Citrix Netscaler Gateway 10 x	
155 Introduction	225
	226
156.1 Note on upgrading the Netscaler.	
157 Baseline	
158 Architecture	
159 Swivel Configuration	229
159.1 Configuring the RADIUS server	
159.2 Enabling Session creation with username 159.3 Setting up Swivel Dual Channel Transports	
160 Citrix Netscaler Gateway Configuration	230
160.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration	
160.2 Citrix Receiver with Netscaler configuration	236
161 Additional Configuration Options	
161 2 Netscaler SSI Bridge	237 237
161.3 Login Page Customisation	
161.4 Upgrading Netscalers with Custom Pages	
161.6 Additional Login Customisation options	
161.7 Challenge and Response.	
161.8 Image Request button displayed when needed	243
162 Testing	245
163 Uninstall/Removing the integration	247
164 Troubleshooting	<b>248</b> 248
164 Troubleshooting	
164 Troubleshooting 164.1 Error Messages 165 Known Issues and Limitations 166 Additional Information	
164 Troubleshooting	
164 Troubleshooting	
164 Troubleshooting	248 248 249 250 251 251
164 Troubleshooting	248 248 249 250 251 252 252 253 253

171 Architecture	255
172 Swivel Configuration	256
1/2.1 Configuring the RADIUS server	256 256
172.3 Setting up Swivel Dual Channel Transports	256
173 Citrix Netscaler Gateway Configuration	257
173.1 Citrix NetScaler RADIUS Configuration	257 261
174 Additional Configuration Ontions	262
174.1 Netscaler RADIUS Monitor and RADIUS Load Balancer.	
174.2 Netscaler SSL Bridge	262 268
174.4 Additional Login Customisation options	
174.6 Image Request button displayed when needed	271
175 Testing	273
176 Uninstall/Removing the integration	274
177 Troubleshooting	275
177.1 Error Messages	275
178 Known Issues and Limitations	276
179 Additional Information	277
180 Citrix Netscaler Gateway 12	278
181 Introduction	279
181.1 Integration Architecture	279
182 Turing Image Integration	
182.1 Rewrite Rules 182.2 Green Bubble Theme	280 280
182.3 RfWebUI theme 182.4 X1	281 281
183 Pinpad Integration	282
184 Delete previous rules	283
	004
185.1 Edit Password to OTC.	
186 Troubleshooting	285
187 Netscaler Upgrade from 11 to 12	
188 nFactor ? Customizing UI to Display Images	287
189 Backup Configuration	
190 Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer	289
191 Introduction	290
192 Prerequisites	291
193 Baseline	292
194 Swivel Configuration	293
195 Netscaler Configuration	294
195.1 Greate a Swivel Hadius Monitor	294 297
195.3 Create a Swivel Load Balance Service Group	
195.5 Netscaler RADIUS configuration.	
196 Testing	
197 Known Issues	307
198 Troubleshooting	308
199 Citrix Products Integration Matrix.	<b>309</b> 309
200 Citrix Web Interface 4 with Procentation Server 4	
200 1 Introduction	
200.2 Prerequisites	310

200 Citrix Web Interface 4 with Presentation Server 4	010
200.3 Baseline	
200.5 PINsafe Configuration	
200.6 Citrix Web Interface Configuration	
200.8 Testing	
200.9 Troubleshooting	
200.10 Uninstalling	
200.11 Known Issues and Limitations	313 313
201 Citrix Web Interface 4.5 Integration	
201.1 Introduction	
201.2 Frequences	
201.4 Architecture	
201.5 PINsate Contiguration	
201.0 Giffing Configuration Options.	
201.8 Testing	
201.9 I roubleshooting	
201.11 Known Issues and Limitations.	
201.12 Additional Information	
202 Citrix Web Interface 4.6 Integration	210
202 Clinx web metace 4.0 megration	
202.2 Prerequisites	
202.3 Baseline	
2024 Ardimetation	
202.6 Citrix Web Interface Configuration	
202.7 Additional Configuration Options	
202.8 Testing	320 320
202.10 Troubleshooting	
202.11 Known Issues and Limitations.	
202.12 Additional Information	321
203 Citrix Web Interface 5.0 Integration	322
203.1 Introduction	
203.2 Friedquisites	322
203.4 Architecture	
204 Suivel Configuration	202
204 Swite Configurator	
204.2 Enabling Session creation with username	
204.3 Citrix Web Interface Configuration	
204.5 Testing	
204.6 Uninstalling	324
204.7 Troubleshooting.	
204.9 Additional Information	
205 Citrix Web Interface 5.1 Dual Channel button.	
205.2 Log-in page Customisation	
205.3 Tešting	326
206 Citrix Web Interface 5.1 Integration	307
207 Introduction	328
208 Prerequisites	329
	330
210 Architecture	331
211 Swivel Configuration	
211.1 Configuring the KADIUS server	
211.3 Setting up PINsafe Dual Channel Transports.	
212 Citrix Web Interface Configuration.	
212.1 Copy across the web interface riles.	
212.3 Edit the Web.config file	
212.4 Citrix Web Interface RADIUS Configuration	

213 Additional Configuration Options	<b>335</b>
214 Testing	
215 Uninstalling	
216 Troubleshooting	
217 Known Issues and Limitations	330
217 Known issues and Limitations	240
221 Prerequisites	
222 Baseline	344
223 Architecture	345
224 Swivel Configuration	<b>346</b>
224.2 Enabling Session creation with username	
225 Citrix Web Interface Configuration	247
225 Cliffx web interface Configuration	
225.2 Edit the Hadius_secret.txt	
225.4 Citrix Web Interface RADIUS Configuration	
226 Additional Configuration Options	
227 Testing	350
228 Uninstalling	351
229 Troubleshooting	
229.1 Error Messages	
230 Known Issues and Limitations	353
231 Additional Information	354
232 Citrix Web Interface 5.3 Integration	355
233 Introduction	356
234 Prerequisites	357
235 Baseline	358
236 Architecture	359
237 Swivel Configuration	
237.1 Configuring the RADIUS server	
237.3 Setting up PINsafe Dual Channel Transports.	
238 Citrix Web Interface Configuration	
238.1 Copy across the Web Interface Files	
238.2 Edit the Web.config file	
238.4 Citrix Web Interface RADIUS Configuration	
239 Additional Configuration Options	
240 Testing	
241 Uninstalling	
242 Troubleshooting	<b>366</b>
243 Known Issues and Limitations	367
244 Additional Information	260
245 Citrix Web Interface 5.4 Integration	200

246 Introduction	370
247 Prerequisites	
248 Baseline	
249 Architecture	
250 Swivel Configuration	374
250.1 Configuring the RADIUS server	
251 Citrix Web Interface Configuration	
251.1 Edit the radius_secret.txt	
251.3 Citrix Web Interface RADIUS Configuration	
252 Additional Configuration Options	
252.1 Changing the OTC label	
252.3 Configuring Single Channel: Edit the Web.config file	
253 Testing	
254 Uninstalling	
255 Troubleshooting	
256 Known Issues and Limitations	
257 Additional Information	
258 Citrix Web Interface 5.X additional login page options	
258.1 Citrix Web Interface 5.x additional login page options	
258.3 Replacing the Single Channel Button with a Dual Channel Button	
258.4 Single Channel Button with an automated Single Channel Image	
256.5 Turing, Duar channel and Display index bullons	
259 Cyberoam UTM SSL VPN	
260 Introduction	
260 2 Baceline	
260.3 Architecture	
261 Swivel Configuration	
261.1 Configuring the RADIUS server	
262 Cyberoam CR25i Configuration	301
262.1 Define a RADIUS server on the Cyberoam	
262.2 Cyberoam SSL VPN Authentication Methods	
262.4 Additional Cyberoam Configuration Options	
262.5 Testing	
262.6 Troubleshooting	
262.8 Additional Information	
263 Deploy ACD using MS group policies	
264 Introduction	
265 Steps	398
	200
200 Notes	
268 Ericom PowerTerm WebConnect	401
2/U Prerequisites	
2/2 Architecture	405
273 Installation	
273.2 Ericom PowerTerm WebConnect Integration.	

273 Installation 273.3 Additional Installation Options	
274 Verifying the Installation	
275 Uninstalling the Swivel Integration	
276 Troubleshooting	
277 Known Issues and Limitations	
278 Additional Information	
279 F5 APM Integration	
280 F5 Big-IP Access Policy Manager (APM) Integration Notes	
281 RADIUS Integration	
281.1 Test the RADIUS authentication	
282 Logon page Customisation	
283 Testing	
284 F5 Firepass Integration	
284.1 Introduction	
284.3 Architecture	
284.4 Installation	
284.5 F5 Networks FirePass VPN Configuration	
284.7 Modifying the FirePass login page for PINsafe TURing image	
284.8 Verifying Installation.	
284.9 Houseshould a second sec	
285 F5 SAM Integration	
286 F5 Secure Access Manager (SAM) Integration Notes	
287 BADIUS Integration	431
287.1 Test the RADIUS authentication	
288 Log-in page Customisation	
289 Testing	
290 Fortinet Fortigate Integration	
291 Introduction	
292 Prerequisites	
293 Baseline	
294 Architecture	
295 Swivel Configuration	
295.1 Configuring the RADIUS server.	
295.2 Enabling Session creation with username	
296 Fortinet Fortigate Configuration	
296.1 Fortinet FortigateVersion 3.x Integration guide	
296.2 Fortinet Fortigate Version 4.X Integration guide.	
296.4 Test the RADIUS authentication	
	454
297 Additional Configuration Options	
297.2 Login Page Customisation.	
298 Testing	
299 Troubleshooting	
300 Known Issues and Limitations	
301 Additional Information	
302 HOB Remote Desktop VPN	456
303 Introduction	457

304 Prerequisites	458
305 Baseline	459
306 Architecture	460
<b>307 Swivel Configuration</b>	<b>461</b> 
308 HOB RD VPN WebSecureProxy Integration	<b></b>
309 Verifying the Installation	
310 Uninstalling the PINsafe Integration	
311 Troubleshooting	470
312 Known Issues and Limitations	471
313 Additional Information	
314 Juniper ChangePIN	
315 Introduction	
316 Prerequisites	
317 Baseline	476
318 Architecture	
<b>319 Installation</b>	<b>478</b> 
320 Verifying the Installation	
321 Uninstalling the Swivel Integration	
322 Troubleshooting	
323 Known Issues and Limitations	
324 Additional Information	
325 Juniper OneTouch	
326 Overview	
327 Prerequisites	
328 Baseline	491
329 Architecture	
330 Installation         330.1 One Touch Demo Application Installation         330.2 Swivel Integration Configuration         330.3 Juniper One Touch Integration         330.4 Modifying the Custom login Pages.         330.5 Uploading the Custom Sign in pages.         330.6 RADIUS Authentication Server Configuration.         330.7 Additional Installation Options.	493 493 493 493 493 493 493 493 493 496 500
331 Verifying the Installation	501
332 Uninstalling the Swivel Integration	
333 Troubleshooting	
334 Known Issues and Limitations	
335 Additional Information	
336 Juniper SA 5.x Integration 336.1 Overview	<b>506</b> 

337 Juniper SA 6.x Integration	
337.1 Overview 337.2 Troubleshooting	
338 Juniper SA 7 v Integration	508
339 Overview	
340 Prerequisites	510
341 Baseline	
342 Architecture	512
3/3 Installation	513
343.1 Swivel Configuration	
343.2 Setting up Swivel Dual Channel Transports	
343.3 Juniper Integration	513
344 Additional Installation Options	
344.1 Creating a Virtual DNS Entry	
344.2 Login Page Modifications for Single Channel Authentication and SMS On Demand	
345 Verifying the Installation	537
346 Uninstalling the Swivel Integration	538
347 Troubleshooting	539
348 Known Issues and Limitations	540
348.1 iPhone, iPad iOS automatic TURing image generation issue	
348.2 Junos Pulse usability issue	
346.5 Authentication rais after upgrading Swiver	
349 Additional Information	541
350 Juniper SA 8.x Integration	542
351 Overview	543
352 Prerequisites	544
353 File Downloads	545
354 Baseline	546
355 Architecture	547
356 Installation	
356.1 Swivel Configuration	
356.2 Setting up Swivel Dual Channel Transports	548 548
257 Additional Installation Ontiona	559
357.4 Creating a Virtual DNS Entry.	
357.2 Login Page Modifications for Single Channel Authentication and SMS On Demand	
358 Verifying the Installation	
359 Uninstalling the Swivel Integration	
360 Troubleshooting	
361 Known lesues and Limitations	575
361.1 iPhone, iPad iOS automatic TURing image generation issue	
262 Additional Information	
363 Juniper Two Stage Challenge and Response.	
363.2 Introduction	
363.3 Prerequisites	
363.4 Baseline	
363.6 Installation	
363.7 Adding Two Stage Authentication	
363.8 Adding Challenge and response Authentication.	
363.10 Verifying the Installation	
363.11 Troubleshooting	
363.12 Known Issues and Limitations	
JUD. TU AUUIIUTIAI ITTUTTIAIUTI	

364 Microsoft Direct Access Integration	
365 Introduction	
366 Prerequisites	
367 Baseline	
368 Architecture	
369 Installation	
369.1 PINsafe Configuration	
369.2 Microsoft Direct Access Integration	
270 Varifying the Installation	۲۵۵. دمع
371 Uninstalling the DINsafe Integration	
372 Troubleshooting	604
373 Known Issues and Limitations	605
374 Additional Information	ana
375 Microsott IAG Integration	
375.1 Introduction	
375.3 Baseline	
375.4 Architecture	
375.5 Installation	
3/5.6 Verifying the Installation.	
375.7 Officiality the Firstale Integration.	
375.9 Known Issues and Limitations	
375.10 Additional Information	
270 Niewson & JAO Multimla Authorition	<b>CO0</b>
376 1 PINsafa and IAG/IIAG Integration using multiple repositories	<b>000</b> 808
376.2 Abproach	
376.3 Implementation	
376.4 User Experience	610
277 Microsoft IAC SMS login video	612
377 Microsoft IAG SMS login Video	
378 Microsoft IAG Turing login video	614
378.1 Microsoft IAG TURing login Videa	614
379 Microsoft ISA 2006 Cluster Integration	615
379.1 ISA 2006 Cluster Integration	
379.2 Overview	615
379.3 Prerequisites	615
379.4 ISA 2006 Cluster Installation Steps.	
380 Microsoft ISA 2006 Integration	616
381 Microsoft Internet Security and Acceleration Server (ISA) Integration Notes	617
382 Introduction	618
383 Drerequisites	610
383 1 ISA 2006 Filter	619 619
383.2 TMG Filter.	619
384 Baceline	620
SOS AICHRECRIPE	
386 Swivel Configuration	
386.1 Contigure a Swivel Agent For XML Authentication	
300.∠ CONTIGURE SINGLE CHARINEL ACCESS	
JUU.J UUTINGUIE A MADIUS NAS EILLY IUI SHAIEPUITI AUUTETIIUAUUT	
387 ISA Installation	
387.1 Publish OWA or Sharepoint	
387.2 Register the ISA Filter	
387.3 Confirm that the filter has been registered correctly	
Sor.4 MOULY LIE LISTERIEL	
388 SSL Certificate Considerations	
388.1 Installing a Self Signed Certificate into the ISA trusted root store	

389 Special Considerations for Sharepoint	629
390 Verifying Installation	630
390.1 Outlook Web Access	
390.2 Sharepoint	
391 Additional Options	632
391.1 RADIUS Authentication	632
391.2 Editing the Security String Request Buttons	
	<u></u>
392 Uninstalling 392 1 Modify the Listener	<b>63</b> 4 634
393 Known Issues	635
394 Troubleshooting	636
20E Additional Information	627
395.1 Note on Activesync and RADIUS authentication.	637
395.2 ISA and OWA	637
396 Microsoft ISA 2006 web page customisation How to Guide	638
396.1 Microsoft ISA 2006 web page customisation How to Guide	638
396.2 Overview	
397 Microsoft OWA 2003 IIS Integration	<b>642</b>
397.2 Prereguisites	642
397.3 Baseline	642
397.4 Architecture	642
397.6 Verifying the Installation	650
397.7 Uninstalling the PINsate Integration	650 651
397.9 Known Issues and Limitations.	
397.10 Useful Links	
397.11 Additional Information	002
398 Microsoft OWA 2007 IIS Integration	653
399 Introduction	654
400 Prerequisites	655
401 Baseline	
402 Architecture	657
403 Installation	658
403.2 Configuration of the IIS Filter.	658
403.3 Configure The PINsafe Server	661
404 Additional Installation Options	
404.1 Modifying the login Page to stop the Single Channel Image automatically appearing	
404.2 Modifying the login Page to allow Dual Channel On Demand Delivery	
405 Verifying the Installation	664
406 Uninstalling the PINsafe Integration	665
407 Troubleshooting	
407.1 Name resolution issue	
408 Known Issues and Limitations.	667
409 Additional Information	
410 Microsoft QWA 2010 IIS Integration	000
411 Introduction	670
	671
413 Prerequisites	<b>672</b> 672
	072
414 File Downloads	
TIT. I OWA I ILEI OIRINGE HISUIY	0/3
415 Architecture	674

410 IIIStallation	
416.1 Preparation for Installing Version 2.9.	675
416.2 Upgrading to Version 2.9.	
416.3 Software installation. 416.4 Configuration of the IIS Filter	
416.5 Configure The Swivel Server	679
416.6 Using additional attributes for authentication	680
417 Additional Installation Options	
417.1 Modifying the login Page to stop the Single Channel Image automatically appearing	681
417.2 Modifying the login Page to allow Dual Channel On Demand Delivery	681
418 Verifying the Installation	
419 Uninstalling the Swivel Integration.	<b>683</b> 683
420 Change PIN	684
420.1 Change Pin with PinPao	
421 Troubleshooting	689
421.1 Enabling debug logging.	
421.3 Juring image appears but user cannot authenticate.	
421.4 User Authenticates Successfully to Swivel but OWA Login Page is Redisplayed	
421.5 Name resolution issue	
422 Known Issues and Limitations.	690
422.1 Known Issues with Version 2.9	690
423 Multiple Swivel Servers	
424 Additional Information	693
425 Microsoft OWA 2013 IIS Integration	
426 Introduction	
427 Compatibility	696
	607
429 File Downloads	698
429 File Downloads	698
429 File Downloads	698
429 File Downloads 430 Architecture	698 699 
429 File Downloads 430 Architecture 431 Installation	698 699 
429 File Downloads	
<ul> <li>429 File Downloads</li></ul>	
<ul> <li>429 File Downloads</li></ul>	
<ul> <li>429 File Downloads</li></ul>	
429 File Downloads	
429 File Downloads	
<ul> <li>429 File Downloads</li></ul>	
429 File Downloads	
<ul> <li>429 File Downloads</li></ul>	
<ul> <li>429 File Downloads</li></ul>	
429 File Downloads	

441 Microsoft TMG 2010 Integration	717
441.7 Swivel Comgutation	
441.8 Swivel TMG Filter Installation.	
441.9 SSL Certificate Considerations	
441.10 Special Considerations for Sharepoint	
441.12 Additional Options.	
441.13 Uninstalling	
441.14 Known Issues	
441.15 Troubleshooling.	
442 Microsoft UAG Integration	
442.2 Prerequisites	
442.3 Baseline	
442.4 Architecture	
442.6 Verifying the Installation	
442.7 Troubleshooting	
442.8 Additional Configuration Options.	
442.10 Additional Information	
443 Microsoft Windows Crodential Provider Integration (Legacy OS)	747
The increase the second and the seco	
444 Introduction	
444.1 Swiver Credential Provider PAQ	
445 Prerequisites	
446 Baseline	
447 Architactura	751
447.1 Offline Authentication	
448 Swivel Integration Configuration	
446.1 Configure a Swite Agent. 448.2 Configure Single Channel Access	
448.3 Create a Third Party Authentication	
449 Microsoft Windows Swivel Credential Provider Installation	755
449.1 Windows Swivel Credential Provider configuration.	
449.2 Additional Installation Options	
449.3 Lest Mode	
450 Verifying the Installation	
451 ChangePIN	
452 Uninstalling the Swivel Integration.	
452 Troublesheating	767
453 1 Disabling the Swivel Login	
453.2 Error Messages	
454 Release Notes	771
454.1 Belease of Version 4.6.	
454.2 Release of Version 4.5.	
454.3 Release of Version 4.4	
455 Known Issues and Limitations	772
456 Microsoft Windows Small Business Server 2011	
457 Introduction	77/
458 Prerequisites	
459 Baseline	776
460 Architecture	
461 Installation	770
461.1 Configure The Swivel Server.	
461.2 Configure the SBS 2011	
462 Verifying the Installation	
405 Troubleshooting	

464 Additional Configuration Options	783
465 Known Issues and Limitations	784
466 Additional Information	785
467 Netgear	
468 Introduction	
469 Baseline	788
470 Division	780
470.1 Configuring the RADIUS server.	
471 Netgear Configuration	
471.1 Contiguring the Domain	
471.3 Additional Configuration Options.	
471.4 Known issues	793
472 Netilla Integration	794
473 Nortel VPN Integration	795
474 Introduction	796
475 RADIUS Integration	797
476 TURING Integration	799
477 Notes	801
478 OpenVDN integration	202
478 OpenVPN Integration	
478.2 Prerequisites	802
478.3 Baseline	
478.4 Integration	
479 Palo Alto Networks Integration	806
4/9.1 Introduction	806
479.3 Baseline	
479.4 Architecture	
479.5 Swivel Configuration	806
479.7 Additional Configuration Options.	
479.8 Testing	
479.9 Troubleshooting.	
479.10 Known issues and Limitations	
490 Salasfaras sam	915
461 Introduction.	
482 Prerequisites	817
483 Baseline	818
484 Architecture	819
485 Installation	820
485_1 Salesforce_com Configuration	
485.2 Configure The Swivel Server	
465.4 Kev and Certificate Generation.	
485.5 Additional Installation Options	828
486 Verifying the Installation	829
487 Uninstalling the Swivel Integration	830
488 Troubleshooting	831
489 Known Issues and Limitations	832
490 Additional Information	
491 SonicWall NSA Integration	834
491.1 SonicWall NSA PINsafe integration with SMS.	
491.2 Overview	
491.0 INStallation	834

492 SonicWall SMA Appliances	838
493 SonicWall SRA EX appliances	839
494 SonicWall SSL VPN Integration	<b>840</b> 
494.2 Prerequisites	840 840
494.4 Architecture	
494.5 Swivel Configuration	
494.6 Soficwall SSL VPN Conliguration. 494.7 Additional Configuration Options	
494.8 Testing	846
494.9 Troubleshooting	
494.11 Additional Information	
495 Stonesoft Integration	849
496 Introduction	850
497 Prerequisites	851
498 Baseline	852
499 Architecture	853
500 Swivel Configuration	
500.1 Configuring the RADIUS server	
500.2 Setting up the RADIUS NAS	
500.3 Enabling Session creation with username	
501 Stonesoft Configuration	856
501.1 Create a Radius Authentication Method.	
501.2 Optional: Greate a Secondary Authentication Server	862 862
502 Testing	863
503 Additional Configuration Options	
	000
504 Troubleshooting	
506 Additional Information	868
507 Swivel Windows Credential Provider	869
508 Introduction	870
508.1 Downloads	870 
509 Prerequisites	871
510 Baseline	872
511 Installation	873
511.1 Basic Installation	
	073
512 Architecture	
512.1 Offline Authentication	8/4
513 Swivel Integration Configuration	875
513.1 Čonfigure a Swivel Agent	
513.2 Configure Single Channel Access	875 876
514 Microsoft Windows Swivel Credential Provider Installation	878
514.1 Windows Swiver Credential Provider configuration	
514.3 Importing Configurations	
515 Verifying the Installation	
516 ChangePIN	
517 Uninetalling the Swivel Integration	000
517 Officiality the Swiver Integration. 517.1 Disabling the Credential Provider.	
518 Known Jesuse and Limitations	000
טוט תווטאוו וששנה בוווונמנוטווש.	

519 VMware View (Horizon)	891
519.1 Introduction	
519.2 Oreguistes	
519.4 Baseline	
519.5 Architecture	
519.7 VMware View Configuration	
519.8 Additional Configuration Options	
519.10 Troubleshooting	
519.11 Known Issues and Limitations	
520 WatchGuard Firebox	900
521 Overview	
522 Windows Credential Provider	902
522 Introduction	002
523.1 Downloads	
523.2 Swivel Credential Provider FAQ	903
524 Prerequisites	904
50E Pagalina	005
525 Dasenne	905
526 Installation	906
526.1 Basic Installation	
527 Release Notes	<b>907</b> 907
528 Architecture	<b>908</b> 908
529 Swivel Integration Configuration	<b>909</b>
529.2 Create a Third Party Authentication	
530 Microsoft Windows AuthControl Credential Provider Installation	011
530.1 AuthControl Credential Provider configuration.	
530.2 Test Mode	
550.5 Importing Configurations	
531 Verifying the Installation	919
532 ChangePIN	921
533 Uninstalling the Swivel Integration	923
533.1 Disabling the Credential Provider	923
533.2 Temporarily Disabling the Credential Provider Remotely	923
534 Known Issues and Limitations	925
535 Windows Credential Provider with RBA	926
536 Introduction	927
537 Prerequisites	928
538 Limitations	929
539 RBA Configuration	930
540 WCP Configuration	932
541 Authenticating	933
542 RBA with fingerprint	934

1 AppGate Security Server

## **2 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.

## **3 Prerequisites**

AppGate Security Server Appliance

AppGate documentation Swivel 3.x, 3.5 or higher for RADIUS groups NAT for Single channel access

#### 3.1 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.

# 4 Baseline

AppGate Security Server Appliance

Swivel 3.8

## **5 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

### **6 Swivel Configuration**

#### 6.1 Configuring the RADIUS server

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

#### 6.1.1 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.

#### 6.2 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

# 7 AppGate Security Server Configuration

#### 7.1 Adding a Swivel RADIUS server

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

Console Help			
	PinSafe (Radius)		
appgate     Administration	Identifier radius/9 Server configuration		
<ul> <li>Authentication Methods</li> <li>Password</li> </ul>	Hostname(s)	swivel	
One Time Password (OTP) OTP+Password	Port(s)	1812	(Common port
Radius	Retries	3	
PinSafe PinSafe+Password	Timeout(s)	7	(seconds)
Counts	Shared secret	*****	
<ul> <li>Clients</li> <li>Clients</li> <li>Clients</li> </ul>	Repeat shared secret	****	
	Use password for SSO	8	
	Pick password from log Pick password from rep Add	pin dialog oly to any of these prompts: Delete	Z
🖏 Run Commands 🕨 🐴 System Settings	Prompts		
	Initial prompt		
	Compatibility		
	✓ Reject means rese	t (complies with RFC 5080 se	ction 2.6.1)
	Help		

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

Console Help		
	PinSafe+Password (Chained)	
Console Help	PinSafe+Password (Chained) Identifier chained/10 Included methods Password PinSafe	Add
System Settings	Help	

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

Console Help		
	SSL ACCESS	
	Certificate	
Authentication Methods	5-1-1-1 0044 00 4	
Oser Accounts	Expires 2014-06-1	9
Access Rules	Host names appgate	
Roles		
<ul> <li>Satellites</li> </ul>	Generate Uploa	ad Remove
Monitor and Status	Settings	
Clients	Gottingo	
Client Configuration Files	Listen on interfaces	✓ appgate
Device Firewall rules		
S Run Commands	Listen port	443
🔻 🕰 System Settings		
AppGate Firewall rules	Title	SSL
Backup & Restore	and the second second second	
🛧 Built-in web server	DNS lookup timeout	10 Seconds
🔁 Connection Settings	1200000	
🚜 Daemons	Refresh time	5 Minutes
😴 File System Manager		
File Transfer	Inactivity timeout	1 Hours
🔜 L2TP/IPsec Access	Ocalita firma aut	
🔒 License Management	Cookie timeout	Jays V
🚔 Local Print	SSL Protocols	SSL 2.0 🗸 SSL 3.0 🗸 TLS 1.0
💫 Log settings		
Network/Cluster Management	SSL Protocol options	Allow MD5 hash
Server Files	Authentication methods	🗹 Password 🗌 One Time Password (OTP
🥑 Software Update		
SSL Access	Help	
🔮 Time Synchronization		

#### 7.2 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.

#### 7.3 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.



# 8 Testing

# 9 Additional Configuration Options

# 10 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

# **11 Known Issues and Limitations**

None

# **12 Additional Information**

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

# 13 Array Networks SPX Integration
## **14 Introduction**

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

## **15 Additional Contributors**

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

## **16 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

## 17 Baseline

Array Networks SPX 8.2.2.0 and also 8.4.4.2 Build 9

Swivel 3.5 and Swivel 3.7

## **18 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.

## **19 Installation**

### **20 Swivel Configuration**

### 20.1 Configuring the RADIUS server

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

### 20.2 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.

### 20.3 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

### 21 Configure the custom login page

### 21.1 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

#### 21.2 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: cpath 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

#### 21.3 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.

## 22 Configure the Array Networks SPX

### 22.1 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 A	Array Pilot! - Micro	soft Internet Exp	lorer		
<u>File Edit View Favorites Tools</u>	Help				
🔇 Back 🔻 🕤 👻 😰 🐔 🔎 Se	earch 🛛 👷 Favorites	🙆 🔕 · 🕹 🛙	2		
Address () https://192.168.200.240:888	38/				
	Username: arr SPX Host Name	ay e: UK01-IPH-SP	x		
Mode: C Enable 🕞 Config					
Portal2	General	<mark>1ethod</mark>	ntication Au	thorization Ac	counting
Virtual Site Home	Active Dire	ctory LDAP	Multi-Domain	LDAP RADIUS	Client Cert
SITE CONFIGURATION	RADIUS SE	RVER CONFIGUE	RATION		
SSL Certificates	Server I	iP Server	Port Secret Pas	sword	
Portal	1 192.168	3.200.30 1812	XXXXXc2V)	icmV0	
Security Settings					
Networking					
LOCAL USERS & GROUPS					
Local Groups					
Login Authorization					
ACCESS METHODS					
Web Access					
File Access					
L3VPN					
ACCESS POLICIES					
ACLs					
URL Filtering					
ADMIN TOOLS					
Session Management					
Config Management Monitoring					
Troubleshooting					
Change Password					
	-				
ê l					

### 22.2 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 A	rray Pilot! - Microsoft Internet Explorer
Eile Edit View Favorites Tools H	<u>t</u> elp
🔇 Back 🝷 🕤 👻 😰 😚 🔎 Sea	arch 🥳 Favorites  😥 - 🐉 🗔
Address 🔊 https://192.168.200.240:8888	3/
Array	Username: array SPX Host Name: UK01-IPH-SPX
Mode: C Enable 📀 Config	
Portal	General Settings Themes External Pages
Virtual Site Home	Portal Pages Error Pages
SITE CONFIGURATION	LOGIN PAGE
SSL Certificates	URL: http://192.168.200.30/login/default.html
Portal	Username: uname
Security Settings	Password: pwd
Networking	
LOCAL USERS & GROUPS	loken: token
Local Users	Password: pwd2
Local Groups	WELCOME PAGE
Login Authorization	
ACCESS METHODS	ORE: ]
Web Access File Access	CHANGE PASSWORD PAGE
TCP Applications	UBL: http://192.168.200.30:8080/changepin/changepin.isp
L3VPN	how at
ACCESS POLICIES	LOGOUT PAGE
ACLs	URL:
URL Filtering	
ADMIN TOOLS	
Session Management	
Config Management Monitoring	
Troubleshooting	
Change Password	
e	

#### 22.3 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:

General Setting	s Themes	External Pages	
Portal Pages	Error Pages		
ADD ERROR PA	GE	C	ancel   Save & Add Another   Save
Error Type: fail	ledlogin 💽		
URL: http	o://192.168.1.1,	/errorpage.html	

The custom login page should be listed under Error Pages

General Setti	ngs Themes External Pages			
Portal Pages Error Pages				
ERROR PAGE	s	Delete   Add		
Error Type	URL			
failedlogin	http://192.168.1.1/errorpage.html			

#### 22.4 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.

### 22.5 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



### 23 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.

Please enter you	r login details below:		
Username:	graham		
Password:	••••		
	Get Security Image		
OTC:	••••		
	Sign In		
	1 2 3 4	5 6 7 1 93 91	8 9 0

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.

Please enter you	ır login details below:
Username: Password:	graham ••••
OTC:	Get Security Image

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

Your attempt to a are correct, and	sign in failed. Please make sure that your username and password try again.
Username: Password:	graham
OTC:	Get Security Image

# 24 Troubleshooting

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

# 25 Known Issues and Limitations

## **26 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

# 27 AuthControl Desktop

## **28 Introduction**

AuthControl Desktop is the brand name for Swivel Secure's custom Windows Credential Provider.

The detailed article can be found under Windows Credential Provider.

# 29 Aventail Integration

SonicWall Aventail clientless SSL VPN Gateway

Integration Guide

## **30 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.

# **31 Prerequisites**

SonicWall Aventail 10.5.2 or SonicWall Aventail 10.5.3 Client Hot Fix 003 Swivel 3.x Aventail login page script

## 32 Baseline

SonicWall Aventail 10.5.2 and 10.6.2-196

Swivel 3.7

## **33 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.



### 34 Swivel Configuration

#### 34.1 Configuring the RADIUS server

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

#### 34.2 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.

#### 34.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

### **35 SonicWall Aventail Integration**

#### 35.1 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

SONICWALL	<b>Iventail </b> Management Console	
Security Administration Access Control	Configure Authentication Server	Authentication Servers > Configure Authent
Resources Users & Groups	Configure authentication settings for a RAD	DIUS server.
User Access Realms Aventail WorkPlace Agent Configuration End Point Control	Credential type: Username/Password Name:* Swivel PinSafe	
System Configuration	General	
General Settings Network Settings SSL Settings	Primary RADIUS server:* 192.168.1.100:1812	
Authentication Servers	Secondary RADIUS server:	
Services Maintenance	Shared secret: *	
Monitoring User Sessions System Status	Match RADIUS groups by: None	
Logging Troubleshooting	Retry interval: 5 seconds	
	Advanced	
	Save Cancel	

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

Ad	vanced				٢
Se	ervice type:	1		An integer, usually 1 Authenticate Only.	for Login or <b>8</b> for
E	Suppress RA	DIUS success mes	sage	Determines whether displays the login con (as configured on the the end user.	the appliance firmation message : RADIUS server) to
RAD	IUS identifier				
Spec not t	cify how the app cypically necessa	liance identifies to ary). If both fields	the RADIUS se are left blank, t	rver (specifying both at ne appliance sends its l	tributes is allowed but nost name.
NAS	-Identifier		NAS-IP-Addre	22	
Ave	ntail		192, 168, 1, 100		
Cus	tom prompts				
V	Customize auth Title:	nentication server	prompts		
	Please log in:				
	Message				
	One Time Code a	nd dick "OK"			
	Identity: Usern	ame:	Proof:	Enter your OTC:	
Loca	ale encoding –				
Cha	nae this settina l	to control the enco	dina scheme us	ed by your RADIUS se	rver.
	Calactad			Cthan	
	Unicode (UTF-	8) -		Other:	
NTL	M authenticatio	on forwarding —			
Forw	vard NTLM crede	ntials to back-end	Web servers.		
	Forward a cu	stom domain name	e		
	Domain name	domain		For resources con authentication for used for the doma credentials.	figured with NTLM warding, this will be in name portion of the
C	) Forward the a	authentication serv	ver name as dor	nain name	
	Save	ncel			

#### 35.2 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.

### 35.3 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.

Security Administration Access Control	Edit Resource - URL	<u>Resources</u> > Eo
Resources Users & Groups	Create or modify a resource.	
User Access Realms	Name:* Description: swivel Test URL for Swivel	Auth
Aventall WorkPlace Agent Configuration End Point Control	URL:* https://100.100.30:8443/proxy	If an HTTPS resource, incl {variable}
<b>System Configuration</b> General Settings Network Settings	WorkPlace shortcuts	
Authentication Servers Services Virtual Assist Maintenance	Link text Description	Used
Monitoring User Sessions System Status Logging Troubleshooting	Web proxy options         Web application profiles         Web application profiles         Web application profile:         Default         View selex         Custom access         You can choose to translate this resource or provid         Translate this resource         Alias name:         swivel         Synonyms:	apabilities and content translation opt cted profile e access to it on a custom port or FQ

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.

Security Administration Access Control	Edit Access Rul	e	
Resources	General   Adv	vanced	
Users & Groups User Access Realms Aventail WorkPlace Agent Configuration End Point Control	Create or mod Number: * Description:	lify an access control rule.	ID: AV1394036930 The Description app useful in debugging
System Configuration General Settings	Action:	Permit C Deny C	) Disabled
Network Settings SSL Settings Authentication Servers	Basic setting Click an Edit b	<b>s</b> utton to specify the users and	resources to which this rule applies
Virtual Assist Maintenance		O User C Resource	Select User for a forward connection resource). If you deploy a network tu Resource for a reverse connection (re cross connection (user to user).
Monitoring User Sessions System Status Logging Troubleshooting	From:	Any user	
	To:	swivel	
	End Point Cor	ntrol zones	

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 refld="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.

### 35.4 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 <div> tags that define more general divisions on the workplace portal pages (for example, <div id="container">, <div id="container">, <div id="foot">, 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

Security Administration			
Access Control Resources Users & Groups	Configure WorkPlace Sit	te	<u>WorkPlace Sites</u> > Configure Wor
User Access Realms Aventail WorkPlace Agent Configuration End Point Control	General   <u>Advanced</u> Name this Aventail Work access WorkPlace).	Place site and assign a domain	name (which determines the URL u
Furthern Configuration	Name:*	Description:	
System Configuration General Settings Network Settings SSL Settings Authentication Servers Services Maintenance Monitoring User Sessions System Status Logging Troubleshooting	Demo         Fully qualified domain         Specify the FQDN used to         Image: Custom host name         Demo         Custom host and content	Demo workplace site name to access this WorkPlace site. to only* domain name*	This site configuration will share the appliance domain name. This name prefixed with https://workplace.glos.nhs.uk/go/, used to access WorkPlace.
	Login page appearance Select a style that has th can also modify an exist portal pages is specified Style: Demo Style Save Cancel	e he logo, color scheme, and text ing style, or create a new one. during community configuratio	you want for the WorkPlace login p The style and layout for other Work n. ID: AV1243420624569NM

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 sUr="https://FQDN_of_workplace/swivel/SCImage?username="; //Find the image using Mozilla compatible pproach... varIng = document.getElementById("imgTuring"); //Set the image SRC and make it visible varIng.src = sUrl + sUser + "srandom=" + Math.round(Math.random()*1000000); varIng.style.visibility = "visible"; //Alternative approach - show image in Popup //Window.showModalDialog(SUI + 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.

<ipre><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.

# 36 Verifying the Installation

Login using the Turing or SMS.

Example of a modified SonicWALL Aventail sign-in page

Username:	tes	t							
Enter your OTO	: [								
	L	.og in			Tu	iring			
	_								
1.1	1 2	2 3	4	5	6	7	8	9	Q

# **37 Known Issues and Limitations**

None
### **38 Configuration Options**

### 38.1 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.

### **38.2 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.

```
<</td>
```

#### 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()
 élse
  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();
 élse
 //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){</pre>
  index.value = text;
 } else {
  index.value = "";
 }
```

#### 38.3 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.

#### **38.4 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();};
}
```

#### 38.5 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>
```

### **39 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.

## **40 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

# 41 Barracuda SSL VPN Integration

## **42 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.

## **43 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.

## 44 Baseline

Barracuda SSL VPN 2.2.2.203 and 2.2.2.115

Swivel 3.9

## **45 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

## 46 Swivel Configuration

### 46.1 Configuring the RADIUS server

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

### 46.2 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.

## 47 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.

### 47.1 Create an authentication scheme

From the Access Control tab select Authentication schemes.

50L 87 A 10	BASIC	RESOUR	CES ACCI	ESS CONTROL	ADVANCED	
Accounts	Groups	5	Polici	es	User Databases	Aco
NAC Exceptions	Authentication	Schemes	Security S	ettings	Configuration	S
reate Authenticati	on Scheme					
• User Database:		Global Vi	ew 🔻			
• Name:						
	Available modu	ules				Se
Authentication Key Client Certificate IP Authentication One-Time Password Password	rd (Secondary)		E	Add >> << Remov Up Down	e	
DIN	Available Polic	ies				Se
Administrators Auditors Everyone Help Desk Adminis Help Desk Users	strators			Add >> Add All > << Remov	> re All	
Add						
uthentication Sche	emes					
	Apply Filter R	leset				
me			Use	er Database		
Password			Sup	er Users		
Password			Def	ault		
WebDAV			Glo	bal View		

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.

6				
Details				
• Name:	Swivel RADIUS			
Description:				
(				
Modules				
Available mod	ules			Selecte
Authentication Key		Add >>	RADIUS	
Client Certificate		Add All >>		
One-Time Password (Secondary)		<< Remove		
Password		<< Remove All		
PIN Security Questions (Secondary)		Up		
Security Questions (Secondary)		Down		
L				
Policies				
Available Polic	cies			Selecte
Administrators		Add >>	Swivel	
Auditors		Add All >>		
Help Desk Administrators		<< Remove		
Help Desk Users		<< Remove All		
Power Users				
L				
Show Personal Pol	licies			
Save Cancel				

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.

### 47.2 Barracuda RADIUS Configuration

On the SSL VPN administration console select the  $\ensuremath{\mathsf{Access}}$  Control tab then select configuration.

RADIUS		
RADIUS Server:	localhost	
	Hostname	Hostnames
Backup RADIUS Servers:		Add >>
		<< Remove
Authentication Port:	1812	This is the port number stipulated for the RADIUS authentication
	1012	port between <b>0</b> and <b>65535</b> . Default (1812).
Accounting Port:	1813	This is the port number stipulated for the RADIUS accounting probetween <b>0</b> and <b>65535</b> . Default (1813).
Shared Secret:		The RADIUS shared secret which has been set up on the RADIUS
Authentication Method:	CHAP -	If your server does not use a specific authentication method, this that are currently supported in this configuration are ${\bf PAP}, {\bf CHAP}$
Time Out:	30	The timeout for a RADIUS message.
Authentication Retries:	2	The number of retries for a RADIUS message.
	Attribute	Attributes
RADIUS Attributes:		Add >> Add >> VAS-IP-Address = %NASIP® User-Name = %USERNAME User-Password = %PASSW
Username Case:	<ul> <li>As Entered</li> <li>Force Upper Case</li> <li>Force Lower Case</li> </ul>	Setting that defines what case the username is sent to the RADI entered, force to upper case or force to lower case.
Password Prompt Text:	RADIUS Password	Customize the RADIUS password prompt text.
Reject Challenge:	◉ Yes ◎ No	Reject a challenge-response request from the RADIUS server. D
Challenge Image URL:		A URL for generated challenge images. Leave blank to disable.
Allow Untrusted Challenge Image URL:	🛇 Yes 🖲 No	Allow Challenge Images to be server from untrusted servers.

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.

RADIUS			
RADIUS Server:	172.16.1.96		
	Hostname		Hostnames
Backup RADIUS Servers:		Add >>	172.16.1.97
		<< Remove	
Authentication Port:	1812	This is the port number stipul between <b>0</b> and <b>65535</b> . Defa	ated for the RADIUS authentication ault (1812).
Accounting Port:	1813	This is the port number stipul between <b>0</b> and <b>65535</b> . Defa	ated for the RADIUS accounting pro- ault (1813).
Shared Secret:	•••••	The RADIUS shared secret w	hich has been set up on the RADIUS
Authentication Method:	PAP -	If your server does not use a are currently supported in th	a specific authentication method, this is configuration are <b>PAP</b> , <b>CHAP</b> , <b>M</b>
Time Out:	30	The timeout for a RADIUS me	essage.
Authentication Retries:	2	The number of retries for a R	ADIUS message.
	Attribute		Attributes
RADIUS Attributes:	\${}	Add >> </td <td>NAS-IP-Address = \${radius:r User-Name = \${session:user User-Password = \${session:</td>	NAS-IP-Address = \${radius:r User-Name = \${session:user User-Password = \${session:
	<u></u>		
Username Case:	<ul> <li>As Entered</li> <li>Force Upper Case</li> </ul>	Setting that defines what car	se the username is sent to the RADIU
	C Force Lower Case	entered, force to upper case	or force to lower case.
Password Prompt Text:	отс	Customize the RADIUS passv	word prompt text.
Reject Challenge:	C Yes @ No	Reject a challenge-response	request from the RADIUS server. De
Challenge Image URL:	me=\${radius:userName}	A URL for generated challeng	ge images. Leave blank to disable.
Allow Untrusted Challenge Image URL:	● Yes C No	Allow Challenge Images to be	e server from untrusted servers.

Save the RADIUS settings.

### 47.3 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.

### 47.4 Additional Configuration options

#### 47.4.1 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.

#### 47.4.2 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.



Welcome to Barracuda SSL VPN, a secure gateway to your network.
00
Refresh
отс
Login Cancel
There are other methods of authentication available. Click here to choose a different Auth
🌮 Virtual Keyboard

#### 47.4.3 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.

# 48 Testing

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

SSL VPH 380VX	
	Login
	Welcome to the Barracuda SSL VPN, a secure gateway to your netwo
	Username: username
	Login
	🌍 Virtual Keyboard

Enter the One Time Code and click login.



Refresh OTC •••• Login Cancel
There are other methods of authentication available. Click <b>here</b> to choose a different Authenti

# 49 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

## **50 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.

## **51 Additional Information**

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

## 52 Bomgar

## **53 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.

## **54 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.

## 55 Baseline

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

Swivel 3.10.1

## **56 Architecture**

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

### **57 Swivel Configuration**

### 57.1 Configuring the RADIUS server

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

### 57.2 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

### 57.2.1 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.

### 57.3 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

## **58 Bomgar Configuration**

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

### 58.1 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

B Bomgar - Rep	resentative Login			
BOMGAR				
	maersk-otp.bomgar.com			
Username:	graham			
Password:	•••••			
	Remember my login information			
Authenticate Using: Username & Password 🔻				
	English (US)			
	Login Quit About			

Bomgar client login uisng Two Stage Authentication

Bomgar - Aut ?	
graham:One-Time Code	
OX Cancel	

#### 58.2 Optional

59 Testing

# 60 Additional Configuration Options

# 61 Troubleshooting

## 62 Known Issues and Limitations

None

## **63 Additional Information**

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

# 64 Checkpoint EndPointSecurityVPN Integration

Place Holder

## **65 Checkpoint Mobile Access**

Please refer to the Checkpoint Connectra Integration page.
# 66 Checkpoint SecureClient Integration

**Checkpoint SecureClient** 

Integration Guide

Version 1.1 March 2010, Updated March 2014

## **67 Introduction**

This document outlines the steps required to integrate the Checkpoint SecureClient VPN software with Swivel.

Swivel users can use Swivel?s Token, SMS, Mobile Phone Client, as well as the single channel TURing and Pinpad methods to retrieve a One Time Code or a Security string.

With Single Channel methods, the user must be presented with a TURing or Pinpad at sign-in time, so they can extract their OTC such as the TURing using the Taskbar.

The settings and software can be configured for larger deployments within an msi file to ease installation.

#### **67.1 Prerequisites**

Checkpoint SecureClient E75. This solution is not compatible with E80.

Swivel 3.x. Where the Single Channel image is to be used, this should be presented to the user through a Network Address Translation to the Swivel server.

Swivel SecureClient software

• The file extensions have been changed to prevent them being blocked by filters etc .dll files to .dlx, and .reg to .rex. These need to be renamed back again.

#### 67.2 Baseline

Checkpoint SecureClient R60 and R77,

Checkpoint SecureClient E75.10 (tested for Token, SMS, Mobile App, Taskbar)

Checkpoint VPN server R75.45 (tested for Token, SMS, Mobile App, Taskbar)

Swivel 3.6, 3.9.7, 3.10

## **67.3 Architecture**

The user connects to the Checkpoint VPN by using the SecureClient software. The Checkpoint is configured to use a Swivel server for radius authentication. Users are stored and maintained in Swivel.

## **68 Swivel Configuration**

## 68.1 Configuring the RADIUS server

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

#### 68.2 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.

## 68.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

## 69 Configuring the Checkpoint VPN-1/Firewall-1

#### 69.1 Checkpoint VPN-1/Firewall-1 configuration Overview

The steps for enabling SecureClient users on the Checkpoint VPN-1/Firewall-1 is outlined below. For further details refer to the VPN-1/Firewall-1 Administration Guides.

- 1. Install the SecureClient license.
- 2. Create SecureClient users.
- 3. Define a SecureClient authentication method using PINsafe as a RADIUS server
- 4. Create a SecureClient group.
- 5. Add SecureClient users to the SecureClient group.
- 6. Define a Remote Access Community and participants.
- 7. Create SecureClient rule for the Remote Access Community.
- 8. Create the Desktop Security Policy rules.
- 9. Install Security Policy.

#### 69.1.1 Configure Checkpoint VPN-1/Firewall-1 to use the Swivel RADIUS server

Create a RADIUS server entry on the Checkpoint Policy Editor

Select Manage/Network Objects' then Click on New then Workstation. In the Workstation Properties window, enter the, Swivel server IP Address, choose 'Host' for Type. For the Comment enter enter "PINsafe authentication". When complete, click OK. Note: When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see VIP on PINsafe Appliances.

Select Manage/Servers then click on New and from the menu select Radius. In the RADIUS Server Properties window enter the following:

Name RADIUS server name

Comment information e.g. PINsafe RADIUS server

Colour A colour for the object (we like orange!)

Host hostname of the Swivel server created above

Service select New Radius (Uses port 1812)

Shared secret enter the shared secret that is also entered on the Swivel server

Version select the RADIUS version required

Protocol select the required RADIUS version

Priority The priority for authentication to multiple RADIUS devices

RADIUS Server	Properties - PINsafeRADIUS
General Acco	ounting
<u>N</u> ame:	PINsafeRADIUS
<u>C</u> omment:	PINsafe RADIUS server
Color:	
<u>H</u> ost:	PINsafe  New
<u>S</u> ervice:	
Shared Secret:	•••••
⊻ersion:	RADIUS Ver. 2.0 Compatible
P <u>r</u> otocol:	PAP
Priority:	1 🕂 (1 is highest)
	OK Cancel Help

#### 69.1.2 To configure External Checkpoint VPN-1/Firewall-1 users to authenticate by RADIUS

External User Profiles There are two different types of External User Profiles available in the Check Point VPN-1/Firewall-1 product, either match all users or match by domain, whereby users are differentiated by their domain name.

The steps below will configure an External Profile of Match All Users.

- 1. On the Checkpoint VPN-1/Firewall-1 configuration select Manage/Users and Administrators/New/Match All Users/Default.
- 2. The user generic* is created and greyed out.
- 3. Select the Authentication tab.
- 4. From the drop down box choose RADIUS as the user?s Authentication Method.

For further details on the available user authentication methods, configuration and setup, refer to the VPN-1/Firewall-1 Administration Guides.

The SecureClient is now ready for two factor authentication using standard SMS delivery or the Mobile Phone Client.

#### 69.2 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. Open the Secureclient, 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 SecureClient 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. Note: When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see VIP on PINsafe Appliances.

#### 69.3 Modifying the Checkpoint SecureClient for Single Channel and Advanced SMS features

Note that all .dll files have been renamed to .dlx, and .reg files to .rex, to avoid problems with email filters. You will need to change the names back before deploying the files.

Stop the SecureClient or ensure it is not running.

Copy PINsafeAuthGUI.dll, and copy it to the SecuRemote\bin folder

Edit SecuRemote\database\userc.C. and add the below to the :options section

:guilibs ( : ("C:\Program Files\CheckPoint\SecuRemote\bin\PINsafeAuthGUI.dll") )

Edit RegSettings.reg. to set the correct Swivel server and possibly the port and context. Double-click RegSettings.reg to install the registry settings the DLL needs.

The options are:

PINsafeServer: The IP address of the Swivel server. This should be a NAT address of the Swivel server and accessible from the client.

PINsafeProtocol: 1 for https, or 0 for http

PINsafePort: The port used to retrieve single channel images from the Swivel server, usually 8443 for a Swivel virtual or hardware appliance. For a software only install see Software Only Installation

PINsafeContext: The installation instance of the pinsafe server, usually pinsafe or proxy for a Swivel virtual or hardware appliance

PINsafeAllowSelfCert: 1 to allow self signed certificates on the Swivel server, 0 to not allow them to be used

#### **PINsafeSecret:**

PINsafeUser: The user for authentication can be pre-configured. Do not set this value if this is a template to be used for deployment to multiple users.

**PINsafeChannelType:** single or dual channel communications. Setting dual, requests an SMS security string by the on demand method. The On Demand authentication must be enabled on the Swivel server.

Default Values are:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\PINsafe SecureClient]
"PINsafePortv="localhost"
"PINsafePortv="8080"
"PINsafeContext"="pinsafe"
"PINsafeAllowSelfCert"="1"
"PINsafeSecret"="secret"
"PINsafeSeret"="single"
```

#### Swivel virtual or hardware Appliance Values:

#### Default Values are:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\PINsafe SecureClient]
"PINsafePortocol"="1"
"PINsafePort"="8443"
"PINsafeContext"="proxy"
"PINsafeAllowSelfCert"="1"
"PINsafeSecret"="secret"
"PINsafeSeret"="secret"
"PINsafeContext"="secret""
"PINsafeSeret"="secret""
```

Verify that winhttp.dll is present in C:\Windows\System32

Start SecureClient. Click connect. Under Options, Change Authentication to Secure Authentication API.

When you click Connect, you should now either see a dialog with a TURing on it, or "CONFIRMED" for dual channel, in which case a security string will be sent by the appropriate transport. The password field has been left in case you want a password as well as a OTC, but this can be removed if required. Enter the OTC, and hopefully it will authenticate.

# 70 Removing the Swivel SecureClient

To remove the Swivel authentication remove the earlier added content in Edit SecuRemote\database\userc.C.

then restart the client

# 71 Verifying the Installation

Login using the Turing or SMS.

Site:	192.168.1.1	
User: OTC:		TURing
1 2 0 5	3 4 5 6 7 4 <b>3 8 6 1</b>	8 9 9 2 7 9
	OK Cancel	
	and the second second	
N-1 Secu	rreClient: PINsafe	
N-1 Secu Site: User:	reClient: PINsafe 192.168.1.1 graham	
N-1 Secu Site: User: OTC:	rreClient: PINsafe 192.168.1.1 graham	TURing
N-1 Secu Site: User: OTC:	rreClient: PINsafe	TURing

# 72 Bulk deployment

With a tested deployment, it is possible to take these settings and create a msi file that will install the Swivel SecureClient software.

For further information see [[1]]

# 73 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Check the Checkpoint Firewall Logs

#### radius not supported

This can be seen when using local policies, switch to a Global Policy for RADIUS authentication and test, or for individual users use RADIUS authentication.

## 74 Known Issues and Limitations

Checkpoint will not accept RADIUS passwords greater than 16 characters in length. If check password with repository is used, then the PIN length will also need to be taken into account, i.e. for a 4 digit PIN, this restricts the length to 12 characters. Two stage RADIUS authentication will bring this back to 16 characters.

## **75 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

# 76 Cisco AnyConnect

## 77 Introduction

The Cisco AnyConnect client allows authentication using the following methods from Swivel:

- SMS Text
  Mobile Phone Client
  Token
- Taskbar Utility

This document describes a custom AnyConnect Windows client with built-in support for single channel Swivel authentication, both TURing and Pinpad. For the IPSEC client see Cisco IPSEC Client Integration.

Our custom Cisco AnyConnect clients are available for versions 2.4, 3.1, 4.4 and 4.7 of AnyConnect. Note that the 4.4 client has been successfully tested with version 4.5 as well.

# 78 Cisco AnyConnect Integration

Product Integration

Product	SMS Text	SMS On Demand	Mobile Phone Client	Token	Taskbar Utility	TURing Image	Pinpad	Index number display
Standard Cisco AnyConnect 2.4	Yes	No	Yes	Yes	Yes	No	No	No
Swivel modified AnyConnect 2.4	Yes	No	Yes	Yes	Yes	Yes	No	No
Standard Cisco AnyConnect 3.1	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Standard Cisco AnyConnect 4.4/5	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Standard Cisco AnyConnect 4.7	Yes	No	Yes	Yes	Yes	Yes	Yes	No

The Cisco AnyConnect client should be downloaded from the Cisco website. The Swivel AnyConnect modifications, where available, can be downloaded below.

## 79 Cisco AnyConnect Client Integration

## 79.1 Configure the Cisco ASA

In order to use Swivel authentication, you need to follow the instructions in Cisco ASA Integration, creating a RADIUS server for Swivel authentication within the Cisco AnyConnect configuration. However, ignore the section on Login Page Customisation, as it is not relevant for the AnyConnect client.

The basic steps for AD Primary and Swivel RADIUS secondary are:

- Configure the ASA for Primary authentication server access, such as AD, and test that it works.
  From Remote Access VPN > AAA/Local Users > AAA Server Groups, create a Swivel group, and add the Swivel RADIUS servers.
  From Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles open the required Connection Profile, and under Advanced Secondary Authentication, set the Secondary Authentication Server Group to the Swivel group.

Edit AnyConnect Con	nection Profile: De	efaultWEBVPNGroup		
Basic General Client Addressing Authentication Secondary Authenti Authorization Accounting Group Alias/Group I	Secondary Authent Server Group: Attributes Server Session Usernan Interface-Specific S	ication Server Group — PINsafeDem Use LOC/ Use prim C Use prim C O Primary Ne Server: O Primary Secondary Authentication	o AL if Server Group fails ary username (Hide secondary u Secondary Secondary Secondary	ısername on login
	Interface	Server Group	Fallback to LOCAL	Use primar
	Username Mapping Pre-fill usern Hide use Fallback Password: (	From Certificate ame from certificate rname from end user when a certificate is una Prompt O Use prin	available nary 🔿 Use	
	Specify the c	ertificate fields to be use	ed as the username	
	Secondary Field	ield: OU (Organization	Unit)	
	O Use the entir	e DN as the username		
۰ III ۲	Use script to	select username	🖶 Add 🗹 Edit 📋 Delete	
Find:		Next	Previous	
	[	ОК	Cancel Help	

When using a Primary authentication service such as Active Directory and a secondary authentication service such as Swivel, the AnyConnect client will display an extra password field, allowing entry of username, password and One Time Code.

## 79.2 Install the Cisco AnyConnect Client

Download and install the normal Cisco AnyConnect client from your Cisco VPN.

The client should connect and allow authentication using SMS, Mobile Phone Client, Token, and the Taskbar Utility. For PINpad and TURing the below modification is available for testing.

S Cisco AnyConnect	88.97.135.44
Please enter	your username and password.
Username:	
Password:	
Second Password:	
	OK Cancel

## 80 Swivel modified AnyConnect Client for TURing and PINpad

#### 80.1 Download the client modifications

You can download the 4.7 client from here.

You can download the 4.4 client from here.

You can download the 3.1 client from here.

You can download the 2.4 client from here.

#### 80.2 Prerequisites for the modified client

The client machine must be running a recent Microsoft Windows operating system. This client will not work on non-Windows systems. It has been tested on Windows 7 and XP, but we would expect it to work on any Windows system supported by Cisco.

The client machine must have the Microsoft.Net Framework version 3.5 or later installed. Windows 7 and later will probably have this installed by default.

Your Cisco VPN must support version 2.4, 3.1 or 4.4 of the AnyConnect client.

You must have Swivel 3.4 or later. For Pinpad support, you must either have Swivel 3.9.2 or later, or an appliance with the latest release of the Proxy application.

The client makes a direct call to request the TURing or Pinpad images, so you must have direct access to the Swivel server, or else have a proxy set up to redirect requests. The current version always adds "SCImage" to the URL for TURing images and "SCPinPad" to the Pinpad URL, so you cannot at present use our ASP, ASP.Net or PHP proxy solutions. This will be rectified before the product is released.

#### 80.3 Installation of the Cisco AnyConnect client modifications

Locate the installation directory: by default this is C:\Program Files\Cisco\Cisco AnyConnect VPN Client. If you have a 64-bit operating system, the folder will probably be C:\Program Files (x86)....

Take a copy of the file vpnui.exe and rename it or store it in a safe place. You will need to restore this to use the default AnyConnect client again.

Copy the files vpnui.exe, Interop.vpnapi.dll and SwivelSettings.xml from the downloaded zip file into the AnyConnect folder. Alternatively, if you want to keep both clients alongside each other, you can rename the new vpnui.exe to something else.

Run the AnyConnect client. If you get an error at this point, check that you have the right Microsoft.Net Framework library installed.

## 80.4 Cisco Modified AnyConnect Configuration for PINpad and TURing

The first time you run the client, you will need to configure it. Click the arrow to the right of the **Options** button and select **Preferences** from the pop-up menu.

Fill in the correct settings in the dialog box. For a Swivel Appliance, the Swivel URL should be https://*Swivel Server>:8443/proxy/*. For a software only install see Software Only Installation. If you are using a proxy, or a software-only installation, use the URL appropriate for your installation.

Note the option **PINsafe is primary authentication**. This should be checked if Swivel is the only form of authentication, or is the primary authentication. It should be unchecked if you are using PINsafe as secondary authentication. This option is only relevant for Pinpad, as it determines which password field is populated by the pad.

To add new Cisco VPNs, if yours is not shown, right-click on the box labelled **Use PINsafe for the following connections**, and select **Add Server...**. Note that you can specify that the Swivel security string is not shown for certain VPNs.

Now you have entered the preferences, you should be able to click **Connect** and see the login prompt. After you enter a username, or if you have checked the option to remember the last username, immediately, you should see either a TURing image, or a Pinpad. Use these to enter the Swivel one-time code.

Assuming you have entered the correct credentials, you will be connected to the Cisco VPN, and the client will minimize to the system tray. Click on the tray icon to restore the dialog.

# 81 Cisco ASA Integration

## 82 Introduction

This document describes steps to configure a Cisco ASA 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. AnyConnect works with Swivel if started in the portal.

Swivel integration is made using RADIUS authentication protocol with an option to configure the login page. Depending on your needs, you can modify the default customization object or create a new customization object. There are many ways to configure it to work with Swivel such as:

- Username AD Password and Swivel Authentication (The most common method with AD authentication made against the LDAP server and
- OTC checked against Swivel using RADIUS)
   Username AD Password and Swivel Authentication (AD authentication and OTC checked against Swivel using RADIUS)
- Username and OTC (OTC checked against Swivel using RADIUS authentication)

And various other options including local password.

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 virtual appliance or hardware appliance is configured with a proxy port to allow an additional layer of protection.

For the Cisco IPSEC client Swivel integration see Cisco IPSEC Client Integration

#### 82.1 Configuration steps overview

- · Configuring the Swivel server
- Create a customization object to hold the attached Javascript.
- Create an authentication server group with RADIUS protocol.
- Create a connection profile (tunnel group) to link login URL, authentication server and custom login page together.

## **83 Prerequisites**

Cisco ASA 8.03 or higher

Cisco documentation

Swivel 3.x, 3.5 or higher for RADIUS groups

NAT for Single channel access

## 83.1 Login Page customisation prerequisites

Cisco ASA 8 customisation Script Note: beware if opening this in Wordpad or similar in case the text editor wraps the text onto a new line. This script can be used for TURing, SMS, Token or Mobile Phone Client. There is an alternative customisation for Pinpad, available from here.

For Single Channel TURing images some editing of the script is required.

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

## 84 Baseline

Cisco ASA 8.03, Also tested with 8.21

Swivel 3.5, 3.6, 3.7, 3.8, 3.9

## **85 Architecture**

The Cisco ASA makes authentication requests against the Swivel server by RADIUS.

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

## **86 Swivel Configuration**

## 86.1 Configuring the RADIUS server

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

#### 86.1.1 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.

## 86.2 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

## 87 Cisco ASA Configuration

## 87.1 Create a Radius Authentication Server Group

Authentication Server Group is used to hold necessary information about the Swivel server. Go to Remote Access VPN -> AAA/Local users -> AAA Server. Click on Add to add an AAA Server Group.

Remote Access VPN $\Box P \times$	Configuration > Remot	e Access VPN >	AAA/Local Users > /	AAA Se	rver E
P Introduction	AAA Server Groups			-	
E Clientless SSL VPN Access	Server Group	Protocol	Accounting Mode	F	Add
AAA/Local Users	🖆 Add AAA Serve	er Group			Edit
	Server Group:	pinsafe		Di	Delete
🕀 🔏 Secure Desktop Manager	Protocol:	RADIUS	~	D	
E B Language Localization	Accounting Mode:	🔘 Simultaneou	us 💿 Single	Di	
	Reactivation Mode:	<ul> <li>Depletion</li> </ul>	◯ Timed	Di	
DNS	Dead Time: 10	min	nutes	D	
Handred		(		Di	
	Max Failed Attempts	; [3			
	Enable interim ac	counting update			
	ОК	Cancel	Help		
		10 M		600	

Enter a name for Server Group, select RADIUS for Protocol and click OK. With the newly created server group name selected, click on Add on the right bottom to add a Swivel server.

Tentiess 55, VDU Access	Server Group	Protocol	Accounting Mode	Reactive	ation Mode	Add
Connection Profiles	LOCAL	LOCAL				
Portal	pinsafe	RADIUS	Sinde	Deplation	é de	Edit
Bookmarks	📬 Edit AAA Sei	ver				Delete
	Server Group:	pinsafe				
	Interface Name:	outside		Y		
Web Contents	Server Name or B	Address: 192.16	8.8.88)			
Group Policies	Timeout:	10			seconds	
🔓 Dynamic Access Policies	RADIUS Paramete	rs				+
AAA/Local Users	(Server Authent	ication Port: 1812	1			
LDAP Attribute Map	(Server Account	ng Port: 1813			5	
sure Desktop Manager	Retry Interval:	10 se	conds	~	Ê	1
ertificate Management	Server Secret k	ey:	•••		ſ	odd
ad Balancing	Common Passw	ord:			5	Auto
HCP Server	ACL Netmask C	onvert: Stand	iard	~	L L	Edit
Revenued	SDI Messages				[	Delete
	Message Ta	ble			8	Move Up

Enter Swivel server?s IP, authentication port and server secret key as indicated. Click on OK then Apply to save the AAA server group.

## 87.2 Optional: Create a Secondary Authentication Server

The login page can be configured to display Swivel as a primary or secondary authentication server. To use multiple authentication servers, they must be configured under Remote Access VPN -> AAA/Local users -> AAA Server. This example shows an AD Server being added.

Go to Remote Access VPN -> AAA/Local users -> AAA Server. Click on Add to add an AAA Server Group.

Remote Access VPN 리 무 ×	Configurat	ion > Remol	te Access	VPN > AAA/	Local Users > A	AA Server	Groups	
Introduction	AAA Server	Groups						
Inetwork (Client) Access	Se	ver Group	Prot	ocol .	Accounting Mode	Reacti	vation Mode	T
Connection Profiles	AD		NT Doma	in		Depletion		10
🖻 📴 Portal	LOCAL		LOCAL			11.	a	
- III Bookmarks	PINsaf	🚘 Add AAA	Server Gr	oup		×		10
- 🐻 Client-Server Plug-ins								
Customization		Server Group	p:					
Help Customization		Protocol:	R	ADIUS	*			
Port Forwarding		Anne white a b	Andre C	Cinculture and	a C Sinala			
Web Contents		Accounting h	Mode: 1	Simultaneou	is (• Single			
Group Policies		Reactivation	Mode: 🤇	Depletion	C Timed			
Dynamic Access Policies								
🕀 📆 Advanced		Dead Im	ne: [10	mir	nutes			
- Gasy VPN Remote	2 2		_					
AAA/Local Users	Servers in	Max Failed A	ttempts: 3					
AAA Server Groups		Enable in	nterim accou	nting undate			erface	
LDAP Attribute Map	192.16	I chable ii	iconini occou	intening apadeo				
Local Users						-		
Secure Desktop Manager		VPN3K Co	mpatibility	y Option		۲		
Setup				<u>а</u>	1	1		
Englished Language Localization			ОК	Cancel	Help			
DHCP Server		32. 	4	91. 	1977			
Advanced								

Enter a name for Server Group, select NT Domain or Kerberos for Protocol and click OK. With the newly created server group name selected, click on Add on the right bottom to add a NT Domain Server.

付 Add AAA Server	Group	×
Server Group:	AD	
Protocol:	NT Domain	
Reactivation Mode:	• Depletion C Timed	
Dead Time: 10	minutes	
Max Failed Attempts:	3	
ОК	Cancel Help	

Enter the AD server?s IP, Server port and Domain Controller hostname. Click on OK then Apply to save the AAA server group.

Server Group:	AD	
Interface Name:	inside	
Server Name or IP Address:	192.168.0.100	
limeout:	10	seconds
NT Domain Parameters		
VT Domain Parameters		
NT Domain Parameters	168.0.100	

This secondary authentication server then needs to be linked to the Connection Profile (see below).

## 87.3 Create a Connection Profile (Tunnel Group)

Swivel can be defined as a Primary Authentication server or as a Secondary authentication server.

Connection Profile is used to link authentication server group, URL used to access the ASA, and login page customization together. Go to Remote Access VPN -> Clientless SSL VPN Access -> Connection Profiles. Click on Add to add a connection profile.

Remote Access VPN 리 무 ×	Configuration > Remote Acc	ess VPN > Clientle:	ss SSL VPN Access > Cor	nection Profiles
🔤 🥐 Introduction 📃	Access Interfaces			
🕀 🧰 Network (Client) Access	Enable interfaces for clientless	SSL VPN access.		
Clientless SSL VPN Access		1		
Connection Profiles	Interrace		Allow Access	
Portal	outside			
Bookmarks	inside			
Client-Server Plug-ins				
Help Customization				
Port Forwarding				
	Access Port: 443			
Web Contents	Click bere to Assign Certificati	e to Interface.		
Group Policies	cilerentition to hissign contented	5 00 111011 0001		
	Login Page Setting			
🕀 📆 Advanced	Allow user to select coppe	ction profile, identifie	d by its alias, on the login pa	age. Otherwise. Def
Easy VPN Remote				.gor o thormoo, o on
🖻 🚽 AAA/Local Users	🗖 Allow user to enter interna	al password on the log	gin page.	
AAA Server Groups				
- Attribute Map	Connection Profiles			
Local Users	Connection profile (tunnel grou	up) specifies how use	r is authenticated and other	parameters.
🖻 🚮 Secure Desktop Manager	a	. 1		
Setup		308		
🕀 🔂 Certificate Management	Name	Enabled	Aliacae	0.00
Language Localization	GisseUDN		Allases	
Phone Server	DefeultDefeur			AAA(LOCAL)
DNS	DeraultRAGroup		State State	AAA(LOCAL)
Advanced	DefaultWEBVPNGroup		pinsate	AAA(PINsafe)
🚽 🖓 Connection Gateway				

In Basic panel, enter a name, alias and select the AAA Server Group created. Swivel can be configured as the Primary authentication server or the secondary authentication server.

Basic	Name:	DefaultWEBVPNGroup		
Advanced	Aliases:	pinsafe		
Authentication Secondary Authenticat Authorization	Authentication	AAA C Certificate C Both		
Accounting NetBIOS Servers	AAA Server Group:	PINsafe	<b>-</b>	Manage
Clientless SSL VPN		Use LOCAL if Server Group fails		
	DNS			
	Server Group:	DefaultDNS	-	Manage
		(Following fields are attributes of the DNS serv	/er grou	up selected a
		Servers: 192.168.0.100		
		Domain Name: swivel.local		
	Default Group Policy -			
	Group Policy:	DfltGrpPolicy	<b>.</b>	Manage
		(Following field is an attribute of the group poli	icy sele	cted above.)
		☑ Enable clientless SSL VPN protocol		
ind:		Next O Previous		
5.8				

Click on Advanced then Clientless SSL VPN. Select the customization object created and add a Group URL used to access the ASA with Swivel authentication.

Basic -Advanced -General -Authentication -Authorization -Accounting NetBIOS Servers -Clientless SSL VPN	Portal Page Customization:       pinsafe       Manage         Image:       Enable the display of Radius Reject-Message on the login screen when authentication         Image:       Enable the display of SecurId messages on the login screen         Connection Aliases       Add Z Delete		
	Alias	Enabled	
	Group URLs  Add C Delete  URL  https://pinsafe.cisco.com/pinsafe	Enabled	

Click on OK then Apply to save the Connection Profile.

## 87.4 Optional: Create a Secondary Authentication for the Connection Profile (Tunnel Group)

This option has been configured using the Secondary Authentication server option available in ASA 8.21

Go to Remote Access VPN -> Clientless SSL VPN Access -> Connection Profiles, select the connection profile created above then select Edit. Expand the Advanced option list and select Secondary Authentication. Enter the Secondary server group required and if the username should be reused.

Ensure the box "Use primary username (Hide secondary username on login page)" is ticked. Click on OK to save the settings. If AD is defined as the Primary authentication server then Swivel can be defined as the secondary AD server.

	Secondary Authentication	n Server Group		9 W -	
Advanced	Server Group:	AD		<b>*</b>	Manage
General Authentication		Lise LOCAL if Serv	ver Group fails		
Secondary Authentic	at	-			
Authorization		🔽 Use primary usern	ame (Hide secondary usernam	e on login page)	
Accounting	Attributes Server:	Primary C Seco	ondary		
	Seccion Licernamo Ser	uoru @ Drimoru C Socr	odaw.		
	Session Osemanie Serv	ver; (• Primary (• Sect	n luar y		
	Interface-Specific Second	dary Authentication Server	Groups		
	🔂 Add 📝 Edit	💼 Delete			
	Interface	Server Group	Fallback to LOCAL	Use primary us	ername
	Username Mapping from	Certificate			
	Pre-fill Username from Certificate				
		from and uses			
	Hide username	rrom end user			
	Constitution and the	the fields to be used to the			
	<ul> <li>specify the certaint</li> </ul>	ate neius to be used as th	e username:		
	Primary Field:	CN (Common Name)	<b>v</b>		
	Secondary Field:	OU (Organization Unit)	*		
	C				
	${f C}$ Use the entire DN	as the username			
	C Use the entire DN	as the username t username			
	C Use the entire DN	as the username t username			
1	C Use the entire DN C Use script to select	as the username t username	🖬 Edit <u> Î</u> Delete		
	C Use the entire DN C Use script to select	as the username t username	🖬 Edit 📋 Delete		
1:	C Use the entire DN C Use script to select	as the username t username Add   Next OPrevious	🖀 Edit 💼 Delete		
-ind:	C Use the entire DN C Use script to select	as the username t username Add ( Next O Previous	Edit Delete		

#### 87.5 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.

#### 87.6 Optional: Login Page Customisation

If the Swivel Single Channel Image is to be used, then the login page needs to be customised. If single channel authentication is not required, or other page modifications such as for SMS on Demand buttons, then this section can be skipped. The login page customization is used to insert necessary

Javascript to retrieve Swivel Turing image. In ASDM, go to Remote Access VPN ->Clientless SSL VPN Access -> Portal -> Customization. Click on Add to add a new customization object.

Remote Access VPN 🗗 🕂 🗙	Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Cus
<ul> <li>Introduction</li> <li>Network (Client) Access</li> <li>Clientless SSL VPN Access</li> <li>Connection Profiles</li> <li>Portal</li> </ul>	Customization Objects Configure customization objects that the security appliance uses to customize the SSL Add 2 Edit 1 Delete 4 Import 2 Export
Bookmarks	Customization Objects
Client-Server Plug-ins Customization	Template DfltCustomization
Port Forwarding	🖆 Add Customization Object 🛛 🔯
Smart Tunnels	This will create a copy of default customization object and save it with the specified name. Customization Object Name: pinsafe
Certificate Management     Language Localization	OK Cancel Help

Enter a name for the object, click on OK then Apply.

💠 Add 🗹 Edit 📋 Delete		
Customization Objects		
Template		
DfltCustomization		
pinsafe		

With the new object selected, click on Edit to enter the Customization Editor. Click on the Information Panel menu item. Note: If the information panel has been moved to a different location then the script can be added to the Copyright panel instead.

# CISCO SSL VPN Customization Editor

Logon page	pinsafe : Logon Page > Browser Window
<ul> <li>Browser Window</li> <li><u>Title Panel</u></li> <li><u>Languages</u></li> <li><u>Language Selector</u></li> <li><u>Logon Form</u></li> <li><u>Information Panel</u></li> <li><u>Copyright Panel</u></li> <li><u>Full Customization</u></li> </ul>	Title SSL VPN Service default customization

Logon page	pinsafe : Logon Page > Information Panel
<ul> <li>Browser Window</li> <li><u>Title Panel</u></li> <li><u>Languages</u></li> <li><u>Language Selector</u></li> <li><u>Logon Form</u></li> <li><u>Information Panel</u></li> <li><u>Copyright Panel</u></li> <li><u>Full Customization</u></li> </ul>	Mode Enable  Panel Position Right  Text Image URL Image Position Above text

Change Mode to ?Enable?. Modify the pinsafeurl variable in the Cisco ASA 8 customisation Script to reflect your Swivel server?s URL. (The scripts are located at the top of the page under prerequisites). Paste the modified content into the Text box. Click on Save on the top right corner of the Customization Editor to save the object.

WARNING: the Panel Position must be set to Right for the script to work. This is so that the customisation script is rendered after the logon form. If you particularly need the information panel to be on the left, put the Swivel customisation script in the Copyright Panel instead, as that is always rendered at the bottom.

#### The following elements need to be modified in the script:

//Modify the value of primary to reflect the URL of your PINsafe server //if using on-demand SMS, url will need to be DCMessage rather the SCImage //if using an HA pair and you wish the page to try one server then the other to receive a TURING //set standby to be the url of the standby swivel virtual or hardware appliance and set ha to true; var primary='https://demo.swivelsecure.com:8443/proxy/SCImage?username='; var standby='https://demo.swivelsecure.com:8443/proxy/SCImage?username='; var pinsafeurl = primary; var ha = false ; //set HA to true if you want the page to try two servers var loadTimeout = 2500; //how long the page waits (in milliseconds) for the image to be served from the main server before trying the second var secondaryAuth = true; // set to true if you want to show a button that requests a security string var autoShow = true; // set to true to show the TURing image automatically after entering the username

#### Note that for the Pinpad version, SCImage will be replaced with SCPinPad.

The primary and standby should be modified. If a standby is not used then set var secondaryAuth = false

For a virtual or hardware appliance

var primary='https://demo.swivelsecure.com:8443/proxy/SCImage?username=';

For a software only install see Software Only Installation

To use multiple security strings in an SMS message, this can be modified to show the next security string which should be entered.

For a virtual or hardware appliance

var pinsafeurl='https://demo.swivelsecure.com:8443/proxy/DCIndexImage?username=';

For a software only install see Software Only Installation

The text can also be changed to reflect the request for a security string index number. See also Multiple Security Strings How To Guide

"Please enter your user name and click on Get OTP Index";

The Button to request the Security String Index can also be edited

obj[0].value="Get OTP Index";

The Logon Form can be edited to suit the language and secondary authentication password message. Select the Logon Form to display the fields available.

Swivel as the primary authentication server, AD as the secondary authentication server.

PINSAFE : Logon Page > Logon Form			
Title	Login		
Message	Please enter your username and password.		
Username Prompt	USERNAME:		
Secondary Username Prompt	2nd Username		
Password Prompt	PASSWORD:		
Secondary Password Prompt	AD Password		
Passcode Prompt	Passcode		
Secondary Passcode Prompt	2nd Passcode		
Internal Password Prompt	Internal Password:		
Hide Internal Password	No 💌		
Group Selector Prompt	GROUP:		
Button Text	Login		
Border Color	#858A91		
Title Font Color	#mm		
Title Background Color	#666666		
Font Color	#000000		
Background Color	#mm		

AD as the primary authentication server, Swivel as the secondary authentication server.

pinsafe : Logon Page > Logon Form		
Title	Login	
Message	Please enter your username and password.	
Username Prompt	USERNAME:	
Secondary Username Prompt	2nd Username	
Password Prompt	AD Password	
Secondary Password Prompt	OTC	
Passcode Prompt	Passcode	
Secondary Passcode Prompt	Passcode	
Internal Password Prompt	Internal Password:	
Hide Internal Password	No 🔻	
Group Selector Prompt	GROUP:	
Button Text	Login	
Border Color	#858A91	
Title Font Color	#11111	
Title Background Color	#666666	
Font Color	#000000	
Background Color	#11111	
# 88 Testing

Now the configuration is complete. You can use the configured Group URL to access the ASA with Swivel authentication.

	Login
Please enter your us	er name and click on Get OTP
USERNAME:	
OTP	

If configured, a Domain Password prompt will appear.

sco SSL	VPN Se	ervice
	Login	_
Please enter your us	er name and cl	ick on Get OTP
USERNAME:	L	
OTP		
Domain passwor	d:	
	Get OTP	

Before the user name is entered, the OTP (One Time Password) field is grayed out. Enter a user name and click on Get OTP.

				Lo	gin				
			Pleas	e ent	er you	ır OTF	2		
1	2	3	4	5	6	7	8	9	0
2	6	9	7	10	-	8	1	椽	3
					24.00				
	US	ERN	AME:	user	1				
	ОТ	P		••••	·				
				Lo	gin				

OTP login with Domain Password

CISCO SSL VPN Service
Login
Please enter your OTP
1 2 3 4 5 6 7 8 9 0
920748653Y
USERNAME: webvpn
OTP
Domain password:
Login

Use your PIN to extract the OTP and enter it in the OTP field. If everything is configured correctly, you will see the portal page after clicking on Login. Please note that the Javascript to retrieve the Turing image is executed at the user?s browser. Therefore, the user?s PC must have access to the Swivel URL. It is highly recommended that you configure your Swivel server to use SSL/https to protect the session. Also if you are using a Swivel virtual or hardware appliance, the image can be requested via the built-in image proxy.

The below screen shot shows the use of the Security String Index to tell the user which of their multiple security Strings to use.

Login	
Please enter your OTP	
00	
USERNAME: gfield	
0TP ••••	
AD Password	
Login	

The below security screen shows a login screen with Turing and SMS on Demand login options.

	Login
Please enter your (	user name and click on Get OTP
USERNAME:	
OTP	
AD Password	
Login Get	OTP Request SMS

				Lo	gin				
		8	Plea	se ent	er you	Ir OTF	Þ		
1	2	3	4	5	6	7	8	9	0
0	1	6	1	5	4	3	9	8	2
	USE	RNAN	1E:	gfiel	d				
	OTP			••••					
	AD P	assw	ord	••••	••••				
	Log	in	Get	OTP	F	Redne	est SN	1S	

	Login
Please enter your (	user name and click on Get (
	ational
USERNAME.	giieiu
OTP	••••
AD Password	•••••
Login Get	OTP Request SMS

## 89 Additional Configuration Options

The Cisco server can be configured to use multiple authentication servers such as Active Directory.

Two Stage and Challenge/Response authentication can also be configured.

The integration uses Swivel as the primary authentication server and AD as the secondary authentication server. It would be possible to change this order.

If you need to reference the secondary password label or field, the IDs are "secondary_password_field" and "secondary_password_input" respectively.

For example, if you want to change the secondary password prompt from within the customised script, use the following:

```
obj=document.getElementById("secondary_password_field");
if(obj) {
   obj.innerHTML="AD password";
```

### 89.1 Customisation for One Touch / Push

This section describes how to customise the Cisco ASA login page to support Push authentication (previously One Touch). In order to use One Touch with Cisco ASA, you must have the Swivel software version 3.11.5 or later.

Before applying this customisation, read the article on One Touch to ensure that the Swivel Secure Appliance is prepared.

Follow the instructions on customisation above up to the point where the information panel is enabled. Now insert the following in the information panel:

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/2.1.3/jquery.min.js"></script>
<script>
function redirect() {
 window.location.replace("https://<swivel_server>:8443/onetouch/onetouch?returnUrl="
 + encodeURIComponent(window.location.href) );
var QueryString = function () {
   // This function is anonymous, is executed immediately and
// the return value is assigned to QueryString!
  // the return value is assigned to QueryString!
var query_string = {};
var query = window.location.search.substring(1);
var vars = query.split("&");
for (var i=0;ivars.length;i++) {
var pair = vars[i].split("=");
// If first entry with this name
if (typeof query_string[pair[0]] === "undefined") {
    query_string[pair[0]] = pair[1];
// [I f accord ortru with this name
      11
           If second entry with this name
      } else {
         query_string[pair[0]].push(pair[1]);
      }
   return query_string;
}
  ();
$ (document) .ready (function() {
   usernamePassedIn = QueryString["username"];
passwordPassedIn = QueryString["password"];
   claimPassedIn = QueryString["claim"];
if(typeof claimPassedIn == 'undefined') {
      redirect();
   }
      else {
      $('[name=password]').val(claimPassedIn);
$('[name=username]').val(usernamePassedIn);
document.getElementById("unicorn_form").submit();
});
```

</script>

# 90 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.

#### TURing image doesn't change

If you are repeatedly shown the same TURing image for multiple logins, or after refreshing the page, this may be due to page caching settings in your browser. To avoid this problem, change one line in the customisation. Search for the string

obj.innerHTML += '
<img border="1" src="'+pinsafeurl+uname.value+'">';

and replace it with the following:

obj.innerHTML += '

<img border="1" src="'+pinsafeurl+uname.value+'&random='+Math.floor(Math.random()*10000)+'">';

This results in a different URL every time the TURing image is displayed, thereby avoid problems with caching.

# 91 Known Issues and Limitations

None

# 92 Additional Information

We have a prototype customised AnyConnect VPN client available for testing. Please see here for more details.

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

## 93 Cisco IPSEC Client Integration

### 93.1 Introduction

The Cisco IPSEC client allows authentication using the following methods from Swivel:

- SMS Text
- Mobile Phone Client
- TokenTaskbar Utility

This document outlines how to integrate PINsafe Turing image using the PINsafe Taskbar for Microsoft Windows, with the Cisco IPSEC VPN Client. If SMS use is only required then the below Taskbar steps are not required.

For the Cisco ASA PINsafe integration see Cisco ASA Integration

### 93.2 Prerequisites

PINsafe 3.x, 3.5 for RADIUS groups

Turing image available to user from across internet Cisco IPSEC VPN Client A Cisco Authentication device using PINsafe as a RADIUS server PINsafe Taskbar for Microsoft Windows

Cisco IPSEC Client

Cisco documentation

### 93.3 Baseline

PINsafe 3.5 Cisco IPSEC VPN Client 5.0.02 PINsafe Taskbar 1.3.01

### 93.4 Architecture

The user starts the Cisco IPSEC VPN client which starts up the PINsafe Taskbar utility and generates a Turing image for the user to use for the authentication.

## 94 Swivel Configuration

## 94.1 Configuring the RADIUS server

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

### 94.2 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.

#### 94.2.1 Setting up PINsafe Dual Channel Transports

See Transport Configuration

## 94.3 PINsafe Client Configration

### 94.3.1 PINsafe Dual Channel Configuration

No specific client requirements for Dual Channel integration.

### 94.3.2 PINsafe Single Channel Configuration

Follow the installation notes to install the PINsafe Taskbar utility. Ensure that a Single Channel image can be generated. See Taskbar How to Guide. Note the intehgration has only been tested with the Turing Single Channel Image.

## 94.4 Cisco VPN Server Configuration

Configure the VPN server according to the Cisco Documentation, configuring the Cisco VPN server to use PINsafe as a RADIUS authentication server.

## 94.5 Cisco IPSEC Client Configuration

#### 94.5.1 Cisco IPSEC Client with Dual Channel Authentication

No further configuration is required for the Cisco IPSEC client

#### 94.5.2 Cisco IPSEC Client with Single Channel Authentication

Follow the Cisco installation notes. Then open the VPN Client Options menu and choose Application Launcher. The VPN Client displays a dialog, click on Enable and then enter the PINsafe Taskbar utility path and the required syntax:

Example: C:\Program Files\Swivel Secure Ltd\PINsafe Taskbar\PINsafeTaskbar.exe show

Click Apply to activate the application.

Note: The Cisco IPSEC VPN Client may need to be restarted.

#### 94.5.3 Cisco IPSEC client with OTC and AD password

The Swivel server can be configured to use AD password and OTC. On the Swivel Administration console under RADIUS/NAS for the Cisco ASA set Check password with repository to Yes and apply the settings. The Password is entered first followed by the OTC, as passwordOTC. See also Password How to Guide.

## 94.6 Additional Configuration Options

### 94.7 Troubleshooting

Start the Cisco IPSEC VPN client, and click on connect. A Turing window should appear. A One Time Code can be obtained for authentication.

Check the PINsafe logs for Turing images and RADIUS requests.

#### No RADIUS connections seen

Check ports, Cisco uses 1645/1646 by default, Swivel uses 1812/1813 by default.

#### Cisco continues to use AD/other password instead of Swivel OTC

Rremove the Swivel RADIUS servers, apply the configuration then reenter them. Apply the configuration and then test to ensure RADIUS requests are seen in the Swivel logs.

#### 94.8 Known Issues and Limitations

None

#### 94.9 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

# 95 Cisco SA 520

### 95.1 Introduction

This document describes steps to configure a Cisco SA 520 with PINsafe as the authentication server for authentication using SMS, Mobile Phone Client or the PINsafe Taskbar utility.

For the Cisco IPSEC client PINsafe integration see Cisco IPSEC Client Integration

Many Thanks to Brian Norrie of NCI Systems in contributing to this article.

#### 95.2 Prerequisites

Cisco SA 520 Cisco documentation PINsafe 3.x, 3.5 for RADIUS groups

### 95.3 Baseline

Cisco SA 520 firmware version 2.1.51 PINsafe 3.8 PAP Authentication was tested in this setup

### 95.4 Architecture

The Cisco 520 makes authentication requests against the PINsafe server by RADIUS.

## 96 Swivel Configuration

## 96.1 Configuring the RADIUS server

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

## 96.2 Setting up PINsafe Dual Channel Transports

See Transport Configuration

## 96.3 Cisco SA 520 Configuration

On the Cisco SA 520 Administration console select the Administration tab then users and domains. Click on Add, and enter the PINsafe RADIUS server authentication details for the portal.

CISCO Security Appliance Configuration Utility										
Getting Started S	tatus Networking	Firewall IPS	6 ProtectLi	nk VPN	Administration					
✓ Users Domains	Domains									
Groups Users	Domains Configuration									
Firmware & Configuration	Dor	main Name: Pinsafe								
Diagnostics <ul> <li>Traffic Meter</li> </ul>	Authentic	cation Type: Radius-PA	√P <del>v</del>							
Time Zone	s	Select Portal SSLVPN	-							
<ul> <li>Logging Authentication</li> </ul>	Authentics	ation Server: 1.2.3.4								
RADIUS Server	Authentics	ation Secret: •••••								
License Management		Workgroup:								
	LDA	AP Base DN:								
	Active Direct	ory Domain:								
	Apply Rese	et								

CISCO Security Appliance Configuration Utility								
Getting Started S	tatus	Networking	g Firewall	IPS ProtectLin	k	VPN	Administration	
<ul> <li>▼ Users</li> <li>Domains</li> <li>Groups</li> <li>Users</li> </ul>	Don	nains t of Domains						
<ul> <li>Firmware &amp; Configuration</li> </ul>		Domain Name	Authentication Type	Portal Layout Name	Edit			
Diagnostics		SSLVPN *	Local User Database	SSLVPN	2			
Time Zone		test	Radius-PAP	SSLVPN	2			
<ul> <li>Logging Authentication</li> <li>RADIUS Server</li> <li>License Management</li> </ul>		Add D	elete					

## 96.4 Testing

Test authentication using a dual channel Security String or an image from the PINsafe Taskbar utility. You will need to enter your password followed immediately by the one time code into the Password field.

·ılı.ılı. cısco	Small Business Pro Security Appliance Configuration Utility 2.1.51	Username: Password:	Log In Problems logging in?
© 2010 Cisco	o Systems, Inc. All Rights Reserved.		

## 96.5 Additional Configuration Options

### 96.6 Troubleshooting

Check the PINsafe logs for RADIUS requests.

#### 96.7 Known Issues and Limitations

Dual Channel authentication and Taskbar only

#### 96.8 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

# 97 Citrix Access Gateway 5 VPX

### 97.1 Introduction

Please refer to the documentation located at:

Citrix Access Gateway Standard 5.x

## 98 Citrix Access Gateway Access Controller 5.0

PINsafe integrates with the Access Controller 5.0 using RADIUS authentication. The following authentication methods are supported:

- SMS
- Mobile Phone Client
- EmailTaskbar utility

Please refer to the Citrix Access Controller Administration guide for further information on configuring the Access Controller.

The single Channel graphical TURing image cannot currently be embedded into the login page when using the Access Controller 5.0, but we hope to offer this enhancement at a future date. Please contact Swivel Secure to register your interest.

# **100 Introduction**

This document covers the integration of Citrix Access Gateway Advanced edition 4.x.

## **101 Prerequisites**

PINsafe 3.x

The CAG 4.5 integration guide is available here: Citrix Access Gateway Advanced edition 4.5

The CAG 4.5.8 integration guide is available here: Citrix Access Gateway Advanced edition 4.5.8

Note: For PINsafe Single Channel authentication the PINsafe server IP needs to be reachable by the client (i.e. this means an external IP address or a NAT for the PINsafe server IP). An SSL certificate is usually installed on the PINsafe server to prevent the browser from displaying errors regarding self signed certificates or sites without SSL certification. Swivel Secure can assist with the deployment of the certificate, but this must be purchased and applied for by the end user or their reseller.

Additional Integration supplementary documentation is provided below

# **102 Installation**

Ensure on the Logon Point Properties, that under Visibility, the check box is ticked for 'Allow external (gateway appliance) users access to this logon point. If not set, only internal users will have access to this logon point. This option must be set on the default logon point.'

Logon Point Properties - swivel		X
<ul> <li>Name</li> <li>Select Home Page</li> <li>Authentication</li> <li>Authorization</li> <li>Presentation Server Farms</li> <li>Sound and Window Settings</li> <li>Workspace Control</li> <li>Clients</li> <li>Session Settings</li> <li>Session Timeouts</li> </ul>	<ul> <li>Allow external (gateway appliance) users access to this logon point. If not set, only internal users will have access to this logon point. This option must be set on the default logon point.</li> <li>Show logon page. If conditions are defined below, the logon page displays only when these conditions are met.</li> <li>Insert items to build a logical expression of conditions.</li> <li>Root</li> <li>AND</li> <li>NOI</li> <li>Endpoint Analysis Output</li> </ul>	
	Expression preview:	
	OK Cancel Apply	

## **103 Additional Installation Options**

## 103.1 Remove automatic TURing image automatically displaying

To prevent the auto-loading, remove (or comment out) the onBlur method on username:

```
// userField.onblur = ShowTuring;
to
userField.onblur = ShowTuring;
```

## 103.2 Prevent browser caching TURing image

To stop image caching, add a random number to the image request + "&random=" + Math.round(Math.random()*1000000);

```
Example:
```

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

## 103.3 Prevent the cursor from automatically entering the OTC field

Remove the following line from Login.ascx

```
//Set focus to the OTC input
document.getElementById(sNameOfOTCText).focus();
```

## 103.4 Change the TURing button text

To change the prompt for Turing, edit the Login.ascx file and look for the line:

turingBtn.value = "Turing"; and change it to turingBtn.value = "Refresh Image";

- 103.5 Verifying the Installation 103.6 Uninstalling the PINsafe Integration 103.7 Troubleshooting
- **103.8 Known Issues and Limitations**
- **103.9 Additional Information**

## **105 Introduction**

This document shows the steps required to integrate Swivel with the Citrix Access Gateway Enterprise Edition 10.0 (Netscaler VPN).

For version 10.1 refer to Citrix Netscaler Gateway 10.x

For versions 8.x to 9.1 refer to Citrix Access Gateway Enterprise Edition 8,

For other versions of 9.x see Citrix Access Gateway Enterprise Edition 9.

It covers the following steps.

- Configuring Swivel to accept authentication requests from the CAGEE
  Modifying the CAGEE login pages
  Configuring the CAGEE to authenticate via PINsafe

This gives the basics of the integration, with html and javascript skills the integration can be customised as required.

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 Network Address Translation, often with a proxy server. The Swivel appliance is configured with a proxy port to allow an additional layer of protection.

## **106 Prerequisites**

Access Gateway Enterprise Edition firmware version 10.x

An administrative logon account for the Access Gateway

A Secure Shell (SSH) programme (eg putty) and an SSH-based file transfer application such as WinSCP

A Unicode-aware text file editor such as TextPad or WordPad

Swivel 3.x

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, this is usually implemented by a NAT to the Swivel server. Ensure that only the required ports are allowed access.

CAGEE pages to modify and/or Swivel files for version 10.

# 107 Baseline

Tested with Swivel 3.8, 3.9, 3.9.4

Citrix Access Gateway Enterprise Edition Version NS10.0 Build 70.7, and NS10.1 Build 119.7.

## **108 Architecture**

The Citrix Advanced Access Gateway Enterprise Edition makes authentication requests against the Swivel server by RADIUS.

You can create different logon realms / pages called Virtual Servers, these can have different authentication servers/policies, SSL certificates and resources attached to them. However, the downside is they ALL use the same index.html/login.js/en.xml files, so you cannot have multiple landing pages with/without the Swivel modifications.

## **109 Swivel Configuration**

## 109.1 Configuring the RADIUS server

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

### 109.2 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.

## 109.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

# **110 Citrix Access Gateway Enterprise Edition Configuration**

The basis of the integration is to create new versions of the login pages. These pages are on the CAGEE and can be accessed via SSH. There are two approaches, firstly to overwrite the relevant files with those provided by Swivel Secure. The other is to actually modify those on the appliance. The latter approach has the advantage the modified pages will always be based on the latest version of the CAGEE files. The main requirement for modifying these pages is to include a TURing image and the button required to request that image. The same approach could also be used to include a button/image for SMS on-demand. If the single Channel TURing image is not to be used, then the login page does not need to be modified, unless other functions are required such as the Get Security String Index. Note: TURing Images, SMS Confirmed image and Get Security String Index Images require the Swivel server to be accessible from the internet, usually with a NAT.

### 110.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration

The CAGEE needs to be configured to use the Swivel server as a RADIUS authentication server. Where several Swivel appliances are used for resilience, configure the RADIUS request to be made against each of the Swivel servers together with the use of Session Sharing. Note: for appliances, the Swivel VIP should not be used as the RADIUS server IP address, see VIP on PINsafe Appliances

Swivel can be configured as the only authentication server or as an additional authentication server, usually this would be together with AD. The required steps are pretty much the same for both scenarios.

Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

Name Swivel RADIUS

#### Authentication type RADIUS

Secret Key The secret key configured on the Swivel NAS and also under Confirm Secret Key

Group Prefix CTXSUserGroups=

#### Group Separator ;

When complete click on Create.

If the Authentication option is not available check that the license allows authentication to be configured on the Netscaler licensing page.

🖃 🧔 NetScaler VPX 172.16.1.2	Authentication Policies an	d Servers		
G 💋 System	Policies Servers \			
Settings	Name	Туре	Server IP	
Diagnostics High Availability NTP Servers Groups Users Database Users Command Policies Authentication Reports Profiles Muditing	Active Directory	LDAP	172.16.1.33	
E 🧔 SNMP 🔻				

Name* S	wivel RADIUS			
Authentication Type R	ADIUS	•		
Server IP A <u>d</u> dress* 172 .	16 . 1 . 22	IPv <u>6</u> Por <u>t</u> 1812	Time-out (seconds	.) 3
Details				
Secret Key*	•••••	NAS ID		
Con <u>f</u> irm Secret Key		En <u>a</u> ble N.	AS IP address extraction	
Group Vendor Identi	fier	Group Prefix	CTXSUserG	Groups=
Group Attribute Type	e	Group S <u>e</u> para	itor	
IP Address <u>V</u> endor I	dentifier	IP Address At	tribute Type	
Pass <u>w</u> ord Vendor k	dentifier	Password Att	ribute Type	
Password Encoding	рар	<ul> <li>Accounting</li> </ul>	OFF	<b></b>
L				

NetScaler VPX 172.16.1.2	Authentication Policies an	nd Servers		
System Licenses	Policies Servers \			
Settings	Name	Туре	Server IP	
Diagnostics	Active Directory	LDAP	172.16.1.33	
High Availability	Swivel RADIUS	RADIUS	172.16.1.22	
NTP Servers				
Groups				
Users				
🗋 Database Users				
Command Policies				
Authentication				
Reports				
Profiles				
🗉 🧔 Auditing				
E 🥥 SNMP 🔻				

Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

Name Swivel RADIUS Policy

Authentication Type RADIUS

Server Swivel RADIUS

Named Expression True Value (Then click Add Expression so ns_true appears under Expression

🗉 🧔 NetScaler VPX 172.16.1.2 🔔	Authentication Policies	and Servers			
System	Policies \ Servers \				
Settings	Name	Туре	Rule		Req
Diagnostics High Availability High Availability NTP Servers Groups Users Database Users Command Policies Authentication Reports Profiles	Active Directory	LDAP	ns_true		Acti
< <u> </u>					
🔞 🕘 Feature is disabled.	Details				
Navigation Pane	No item selected.				
Favor <u>i</u> tes					
Quick Links	Add 🖉 Open	n 😰 <u>R</u> emove [	3 Sho <u>w</u> Bindings	Global Bindings	

Nam <u>e</u> *	Swivel RADIUS	
Authentication Type	RADIUS	
<u>S</u> erver	Swivel RADIUS Server	🔹 🛃 <u>N</u> ew 💋 Modi <u>f</u> y
Expression		
	Expression	
Match Any Expre	ession <b>V</b> Add Modify Remove	@ AND @ OR (+ )+ (- )-
Match Any Expre	ession <b>V</b> Add Modify Remove	AND      OR (+ )+ (- )-     Add Expression     Add Expression
Match Any Expre Named Expression Preview Expression	ession ▼ <u>A</u> dd <u>Modify</u> <u>Remove</u> s <u>General</u> ▼ <u>True value</u> n ns_true	AND OR (+ )+ (- )- Add Expression

anig	Swivel RADIUS Policy	
uthentication Type	RADIUS	
erver	Swivel RADIUS	di <u>f</u> y
Expression		
	Expression	
Match Any Expre	ession  ADD OR (+ )+ (-	)-
Match Any Expre	ession  Add  Add  Addify  Remove O AND O OR (+ )+ (-	)-

🗆 🧔 Net	tScaler VPX 172.16.1.2	Au	thentication Policies and	d Servers		
G System	P	Policies \ Servers \				
	Settings	Na	me	Туре	Rule	Requ
	Diagnostics	Sw	vivel RADIUS Policy	RADIUS	ns_true	Swiv
	High Availability	E Act	tive Directory	LDAP	ns_true	Activ
	NTP Servers					
	Groups					
	Users					
	Database Users					
	Command Policies					
	Authentication					
	Reports					
	Profiles					
Ŧ	🧔 Auditing					
÷	SNMP	-				

The authentication must be then added such as the Access Gateway/Virtual Servers menu. If just Swivel authentication is required then ensure that only the Swivel policy is active for the Primary. If you require AD and Swivel authentication then you need to make active the Swivel policy as the secondary. Save the settings.

<ul> <li>Access Gateway</li> <li>Global Settings</li> <li>Virtual Servers</li> <li>Groups</li> <li>Users</li> <li>Ø Policies</li> <li>Ø Resources</li> <li>Web Interface</li> </ul>		Certificates Authentication Bookmarks Policies Intranet Applications User Authentication If your Access Gateway is to be deployed in a manner where user auther you may turn off authentication below. Please apply this option with CAUT Image Enable Authentication Authentication Policies Primary Secondary
		Priority         Policy Name         Expression           100         Active Directory         ms_true
		Details : Active Directory Type: LDAP Request Profile: <u>Active Directory</u> Rule: <u>ns true</u>
	Details : CAG	Insert Policy 🔊 Unbind Policy 👔 Regenerate Priorities 📝 Mo

<ul> <li>Access Gateway</li> <li>Global Settings</li> <li>Virtual Servers</li> <li>Groups</li> <li>Users</li> <li>Ø Policies</li> <li>Ø Resources</li> <li>Web Interface</li> </ul>		Certificate User Auth If your A you may I Enable Authentic	Auth henticatio ccess Gi turn off le Auther ation Pol	nentication \ Bookma on ateway is to be dep authentication below ntication licies Secon <u>d</u> ary	arks \ Polic bloyed in a r v. Please a	ies \ Intranet App manner where us pply this option w	lication er auth
		Priority 100 Details No deta	Policy New Policy Active Swivel	Name olicy Directory RADIUS Policy able.	*	Expression	
Feature is disabled.	Details : CAG IP Address: 172.16 Authentication: (	Comments (	rt Policy	Unbind Policy	<u>îii R</u> ege	enerate Priorities	

### 110.2 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.

## **111 Additional Configuration Options**

### 111.1 Login Page Customisation

The login page can be modified to display the TURing image, PINpad or String Index as outlined in the following sections.

#### 111.1.1 Customisation Overview

See under **prerequisites** for the modified files that need to be uploaded to the Netscaler.

Note on editing files: If the files are edited in Winsdows based systems it may be possible that control code ^M are added to the end of the line. These can be viewed and removed by using vi.

The below describes how to modify the login page for additional functionality such as the below which require the Swivel server to be accessible by the client, usually through a NAT:

- TURing Image (Automatic or requested by a button)
- Display Security String Index
  Get SMS button

Because all files in /netscaler/ns_gui are overwritten upon a restart or power cycle, the script /nsconfig/rc.netscaler copies at boot the required files from /var/mods to /netscaler/ns gui.

#### 111.1.2 Login to Netscaler Command Line

Use WINscp to use a web file tool or SSH onto the appliance using an admin account. Once onto the box you need to type shell to get access to the command line.

```
>Last login: Wed Sep 10 19:12:45 2008
Done
> shell
Last login: Wed Sep 10 21:13:35 2008
```

#### 111.1.3 Backup Netscaler files

Navigate to the location of the pages to be modified, and make a local backup copy of them.

```
cd /netscaler/ns_gui/vpn
cp index.html index.html.bak
cd /netscaler/ns_gui/vpn/resources
mkdir bak
cp *.xml bak
```

#### 111.1.4 Customise the login script

#### 111.1.4.1 Requesting a TURing image

These files can be modified before uploading

Modify pinsafe.js. The sUrl setting in pinsafe.js needs to be changed to reflect the Hostname and port number of the relevant Swivel server.

For an Appliance this will normally be similar to:

```
sUrl="https://turing.swivelsecure.com:8443/proxy/SCImage?username=";
```

For a software only install see Software Only Installation

#### 111.1.5 Customise the login prompt

Modify the language resource files in /netscaler/ns_gui/vpn/resources. If you are only using the English language, then edit en.xml and search for

<String id="Password2">

this should be around line 59.

Replace the value for id="Password2" with "OTC:". Also, insert a new string for id="Password" with a value of "AD Password". You should therefore have 2 lines as follows:

<String id="Password">AD Password</String>
<String id="Password2">OTC:</String>

(Note that Password has no colon at the end, whereas Password2 has a colon).

#### 111.1.5.1 Additional Languages file modifications

If you will be using languages other than English, you will also need to edit any other language files you use, replacing the value for Password2 with the appropriate label for OTC (One-time code) and inserting a new string for Password1 with the label for AD (Active Directory) password.
Edit the file rc.netscaler to copy across any modified language pages, as for English which is included in the script.:

cp /var/mods/en.xml.mod /netscaler/ns_gui/vpn/resources/en.xml

#### 111.1.6 Upload files to Netscaler

Download the files under the prerequisites and copy them to the following locations:

index.html to /netscaler/ns_gui/vpn/index.html

pinsafe.js to /netscaler/ns gui/vpn/pinsafe.js

rc.netscaler to /nsconfig/rc.netscaler

Note that the files in /netscaler/ns gui/vpn are re-written when the server is rebooted therefore make sure so save these files elsewhere regularly to prevent work in progress being lost during development. How to manage these pages is covered later.

#### 111.1.7 Copy the modified files from run time to file storage

```
mkdir /var/mods
```

- cp /netscaler/ns_gui/vpn/index.html /var/mods/index.html.mod cp /netscaler/ns_gui/vpn/pinsafe.js /var/mods/pinsafe.js.mod cp /netscaler/ns_gui/vpn/resources/en.xml /var/mods/en.xml.mod

#### Also copy across any additional language files modified.

Because all files in /netscaler/ns gui are overwritten upon a restart or power cycle. At boot time the /nsconfig/rc.netscaler script copies /var/mods/ files back to /netscaler/ns_gui.

#### 111.1.8 Reboot Netscaler to verify files are copied across

Reboot the Netscaler to ensure that the files are copied across at boot time.

#### 111.2 Additional Login Customisation options

#### 111.2.1 Automated TURing Display

With the automated TURing display, when the user leaves the username field, the TURing will be automatically displayed. A login using the TURing image is expected for that user.

#### Edit the index.html file

search for onFocus="loginFieldCheck()"

Add a new attribute after this, as follows:

onBlur="showTuring()"

#### Example:

onFocus="loginFieldCheck()" onBlur="showTuring()" style="width:100%;"

#### 111.2.2 Changing the button labels

If you want to want to change the button text such for sending security strings to SMS or email on-demand, rather than showing a TURing image, or change the GET Image text you may want to change the label of the button. You can do this as follows:

Edit the index.html file and locate the code that renders the button by searching for "btnTuring". You will find the following code within the line:

id="btnTuring" value="Get Image"

Change the value attribute to an appropriate alternative, such as "Send Message".

#### 111.2.3 Requesting the string Index

#### See also Multiple Security Strings How To Guide

Modify pinsafe.js. The sUrl setting in pinsafe.js needs to be changed to reflect the hostname and port number of the relevant Swivel server.

For an Appliance this will normally be similar to:

sUrl="https://turing.swivelsecure.com:8443/proxy/DCIndexImage?username=";

For a software only install see Software Only Installation

#### 111.2.4 PINpad

Netscaler 93 PINpad is a version of the 9.3 customisation modified for Pinpad. Note that in order to use PINpad you will need a Swivel Appliance version 2.0.13 or higher. For earlier versions, you can get this from Downloads.

PINpad pre-req

#### 111.2.5 Requesting an SMS

See also Challenge and Response below

Modify pinsafe.js. The sUrl setting in pinsafe.js needs to be changed to reflect the hostname and port number of the relevant Swivel server.

For an Appliance this will normally be similar to:

sUrl="https://turing.swivelsecure.com:8443/proxy/DCMessage?username=";

For a software only install see Software Only Installation

### 111.3 Challenge and Response

Citrix Access Gateway Enterprise Edition 9.2 and 10.x support RADIUS Challenge and Response. RADIUS Challenge and Response can be optionally configured to enter a username and Password, which will then ask for a One Time Code. Configure the Swivel server to use Two Stage Authentication and Check Password With Repository, see also Challenge and Response How to Guide

Challenge and response is usually configured with Username, and AD password for LDAP authentication, and Swivel configured to use AD password in order to request the SMS message to be sent to the user. It is possible to modify the login page so that the AD password need only be entered once. A modified page can be downloaded from here: CAGEE Two Stage Login page

To install the login page use the same procedure as the Single Channel login page.

#### 111.4 Image Request button displayed when needed

The following code allows the Single Channel Image request button to be only shown when required. This is useful for refreshing an image or when SMS/Mobile client authentication is used, since when a Single Channel image is generated, either automatically or manually, it then expects a single channel login (within 2 minutes by default).

# 112 Testing

Browse to the login page and check that a Turing image appears and the One time Code can be entered to login.

User name:	oraham	
AD Password:	••••	
OTC:		
	Get Image	Log On
1 2 3	4 5 6 7	8 9 0
572	4968	013

For SMS or Mobile Phone Apps do not click on the Get Image button, but enter the OTC

User name:	graham	
AD Password:	••••	
OTC:	••••	
	Get Image	Log On

If the incorrect credentials are used then the login should fail

		- <u>-</u>
	User name:	
	Password 1:	
	Password 2:	
		Log On
help of	redentials you typed are incor desk or system administrator.	rect. Please try again or contact you

Where the TURing image is not used, then the Get Image page modification can be omitted

Please log on to o	continue.		
	User name:	graham	
	Password 1:	•••••	
	Password 2:	••••	
		Log O	n

## 113 Uninstall/Removing the integration

If the login pages have been modified restore the default login page and remove the added files.

Remove Swivel as the authentication server.

## **114 Troubleshooting**

Check the Swivel logs for Turing images and RADIUS requests.

#### Image from PINsafe server absent

The CAGEE Netscaler checks each password/OTC in turn, so if the AD password is checked first and is incorrect then the secondary authentication will not be tested.

#### Files moved but have a ? appended to the end

If the script to move the files on login contains the control code ^M at the end of each line (usually introduced by Windows based text editors), then the files may appear with a ? at the end of the filename. Use vi to remove the ^M

## **115 Known Issues and Limitations**

The CAGEE caches the javascript so when you make modifications on the CAGEE they are not reflected on the log-in page as rendered. A way round this is to change the name of the .js file and edit the index.html file to use this new .js file. see How To Modify Access Gateway Logon Fields

## **116 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

## 117 Citrix Access Gateway Enterprise Edition 8

## 117.1 Introduction

This document shows the steps required to integrate PINsafe with the Citrix Access Gateway Enterprise Edition (Formerly Netscaler VPN) version 8.x to 9.1. Version 9.2 is covered in a separate document see Citrix Access Gateway Enterprise Edition 9.

It covers the following steps.

- Configuring PINsafe to accept authentication requests from the CAGEE
  Modifying the CAGEE login pages
  Configuring the CAGEE to authenticate via PINsafe

This gives the basics of the integration, with html and javascript skills the integration can be customised as required.

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

### 117.2 Prerequisites

Access Gateway Enterprise Edition firmware version 8.x to 9.1.

An administrative logon account for the Access Gateway

A Secure Shell (SSH) programme (eg putty) and an SSH-based file transfer application such as WinSCP

A Unicode-aware text file editor such as TextPad or WordPad

PINsafe 3.x

PINsafe server must be accessible by client when using Single Channel Images, such as the Turing Image, this is usually implemented by a NAT to the PINsafe server. Ensure that only the required ports are allowed access.

CAGEE pages to modify and/or PINsafe files File:CAGEE_8_files.zip for versions 8 - 9.1

### 117.3 Baseline

PINsafe 3.5

Citrix Access Gateway Enterprise Edition 8.0. Also tested with 9.1.

### 117.4 Architecture

The Citrix Advanced Access Gateway Enterprise Edition makes authentication requests against the PINsafe server by RADIUS.

You can create different logon realms / pages called Virtual Servers, these can have different authentication servers/policies, SSL certificates and resources attached to them. However, the downside if they ALL use the same index.html/login.js/en.xml files, so you cannot have multiple landing pages with/without the pinsafe modifications.

## **118 Swivel Configuration**

### **118.1 Configuring the RADIUS server**

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

#### 118.2 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.

#### 118.2.1 Setting up PINsafe Dual Channel Transports

See Transport Configuration

### 118.3 Citrix Access Gateway Enterprise Edition Configuration

The basis of the integration is to create new versions of the login pages. These pages are on the CAGEE and can be accessed via SSH. There are two approaches, firstly to overwrite the relevant files with those provided by Swivel Secure. The other is to actually modify those on the virtual or hardware appliance. The latter approach has the advantage the modified pages will always be based on the latest version of the CAGEE files. The main requirement for modifying these pages is to include a TURing image and the button required to request that image. The same approach could also be used to include a button/image for SMS on-demand. Note: TURing Images, SMS Confirmed image and Get Security String Index Images require the PINsafe server to be accessible from the internet, usually with a NAT. See also Multiple Security Strings How To Guide

#### 118.3.1 Login Page Customisation

SSH onto the virtual or hardware appliance using an admin account. Once onto the box you need to type shell to get access to the command line.

>Last login: Wed Sep 10 19:12:45 2008 Done > shell Last login: Wed Sep 10 21:13:35 2008

Navigate to the location of the pages to be modified, and make a local backup copy of them

>cd /netscaler/ns_gui/vpn >cp index.html index.html.bak >cp login.js login.js.bak

## Note that the files in /netscaler/ns_gui/vpn are re-written when the server is rebooted therefore make sure so save these files elsewhere reguarlarly to prevent work in progress being lost during development. How to manage these pages is covered later.

The index.html file now needs to be edited (or replaced). The tool vi can be used to do this but an application such as WinSCP will make this easier. The required files can be found in the prerequisites.

A pinsafe is file that is a modification of the existing login is file is required. Make a copy of login is called pinsafe is The showTuring function shown below needs to be added to this file. Note the sUrl setting needs to be changed to reflect the IP address and port number of the relevant PINsafe server. There are other changes that can be made, eg changing the prompt to read One-Time code instead of password.

For a virtual or hardware appliance this will normally be similar to:

sUrl="https://turing.swivelsecure.com:8443/proxy/SCImage?username=";

#### For a software only install see Software Only Installation

Because all files in /netscaler/ns_gui are overwritten upon a restart or power cycle, a script must be created that runs at startup to copy the modified files back to this location. The nsafter.sh or rc.netscaler shell scripts can be created or modified to accomplish this. For example via ssh:

```
> shell
# mkdir /var/mods
# cp /netscaler/ns_gui/vpn/index.html /var/mods/index.html.mod
# cp /netscaler/ns_gui/vpn/pinsafe.js /var/mods/pinsafe.js.mod
# touch /nsconfig/rc.netscaler
# echo cp /var/mods/index.html.mod /netscaler/ns_gui/vpn/index.html >> /nsconfig/rc.netscaler
# echo cp /var/mods/pinsafe.js.mod /netscaler/ns_gui/vpn/pinsafe.js >> /nsconfig/rc.netscaler
```

#### 118.3.2 Citrix Advanced Access Gateway Enterprise Edition RADIUS Cofiguration

The CAGEE needs to be configured to use the PINsafe server as a RADIUS authentication server. Where a VIP is being used on the PINsafe server then configure the RADIUS request to be made against each of the PINsafe servers together with the use of Session Sharing.

PINsafe can be configured as the only authentication server or as an additional authentication server, usually this would be together with AD. The required steps are pretty much the same for both scenarios.

Create a new Authentication policy (under the Netscaler->System->Authentication menu). The policy must specify RADIUS and then the PINsafe server must be added as a RADIUS server.



ame*	PinsafeRadius		
uthentication Type	RADIUS	×	
Server			
IP Address	,	Port 1812 Ti	me-out (seconds) 3
Details		252	
Secret Key*		NASID	
Confirm Secret Key	*	Enable NAS IP a	address extraction
Group Vendor Cod	e	Attribute Value Prefix	x CTXSUserGroups=
Group Attribute Ty	pe	Separator	i
Vendor Identifier		Attribute Type	
	. [	-	

On the SSL-> Virtual Server menu, the created policy must be activated. If just PINsafe authentication is required then you ensure that only the PINsafe policy is active. If you require AD and PINsafe authentication then you need to make active the PINsafe policy as the secondary. Save the settings.

🧁 NetScaler	Access Gatev	vay Virtual Servers			
표 🛄 System			In A L		
🗄 🗀 Network	Name	State	IP Address	Port	Protocol
🗉 🗀 DNS	Cag	🕚 UP	-	443	SSL
🗉 🗀 SSL					
표 🗀 SSL Offload		Configure Acc	ess Gateway Virtua	Server	
표 🗀 Compression					
표 🗀 Integrated Caching		Name* Cagl	4		IP Addres
표 📁 Protection Features		Protocol SSI			T Dout
🗄 🗀 Load Balancing 🛛 🖊		FI00000 [332			Pun
🗉 🗀 Content Switching 🛛 🖊		Network VSer	ver Range 1		Max User:
표 🗀 Cache Redirection 🛛 🖊		Down state fi	ueh		
🕀 🖾 GSLB 🛛 🖊		Down state in	4011		
🗄 🞑 Rewrite		Certificates	uthentication \ Bookma	irks \ Policies \ Inti	ranet Applications $\setminus$ Intra
🖃 🧁 Access Gateway 🖌				1	
Clobal Settings		Bound to Pr	Inary Secondary		
🚺 Virtual Servers 🌖		Activate All De	activate All Add Policy		
Groups					
🗋 Users		Active Policy	/Name		Туре
🕀 🧰 Policies		Auth_	policy_Domene		Authentio
🕀 🧰 Resources	Details : Cag	F Auth_	policy_Domene 🍧		Authentio
🕀 🧰 Application Firewall					
	Authenti	: C·			

## **118.4 Additional Configuration Options**

#### 118.4.1 Challenge and Response

Citrix Access Gateway Enterprise Edition 9.1 supports RADIUS Challenge and Response

#### 118.4.2 Image Request button displayed when needed

The following code allows the Single Channel Image request button to be only shown when required.

```
function ns_showpinsafe()
{
    var pspwc = ns_getcookie("pwcount");
    if ( pspwc == 2 )
    {
        document.write('<img src="/vpn/images/LoginButtonRolloverGlow.gif"/>');
        document.write('img src="/vpn/images/LoginButtonRolloverGlow.gif"/>');
        document.write('imput type="button" id="btnTuring" value="Get Image" ');
        document.write('onclick="showTuring();" class="CTX_CaxtonButton" ');
        document.write("'CTX_CaxtonButton_Hover';");
        document.write("'CTX_CaxtonButton_Hover';");
        document.write("'CTX_CaxtonButton';");
        document.write(''/_CaxtonButton';");
        document.write(''/_CaxtonButton';");
        document.write(''/_/;');
    }
}
```

### 118.5 Testing

Browse to the login page and check that a Turing image appears and the One time Code can be entered to login.

1	og in	
	User Name: test One-Time Code: GetImage	
	1 2 3 4 5 6 7 8 9 0 <b>3</b> 2 1 4 9 6 7 8 9 5	

## 118.6 Troubleshooting

Check the PINsafe logs for Turing images and RADIUS requests.

Image from PINsafe server absent

## **118.7 Known Issues and Limitations**

The CAGEE caches the javascript so when you make modifications on the CAGEE they are not reflected on the log-in page as rendered. A way round this is to change the name of the .js file and edit the index.html file to use this new .js file. see [1]

### **118.8 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

## **119 Citrix Access Gateway Enterprise Edition 9**

## 119.1 Introduction

This document shows the steps required to integrate Swivel with the Citrix Access Gateway Enterprise Edition 9.2 and 9.3 (Formerly Netscaler VPN). for versions 8.x to 9.1 refer to Citrix Access Gateway Enterprise Edition 8.

It covers the following steps.

- Configuring Swivel to accept authentication requests from the CAGEE
  Modifying the CAGEE login pages
  Configuring the CAGEE to authenticate via PINsafe

This gives the basics of the integration, with html and javascript skills the integration can be customised as required.

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 Network Address Translation, often with a proxy server. The Swivel virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection.

### **119.2 Prerequisites**

Access Gateway Enterprise Edition firmware version 9.2 or 9.3

An administrative logon account for the Access Gateway

A Secure Shell (SSH) programme (eg putty) and an SSH-based file transfer application such as WinSCP

A Unicode-aware text file editor such as TextPad or WordPad

Swivel3.x

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, this is usually implemented by a NAT to the Swivel server. Ensure that only the required ports are allowed access.

CAGEE pages to modify and/or Swivel files for version 9.2 or version 9.3.

#### 119.3 Baseline

Swivel 3.5

Citrix Access Gateway Enterprise Edition Version 9.2

and also Swivel 3.8

Citrix Access Gateway Enterprise Edition Version 9.3

### 119.4 Architecture

The Citrix Advanced Access Gateway Enterprise Edition makes authentication requests against the Swivel server by RADIUS.

You can create different logon realms / pages called Virtual Servers, these can have different authentication servers/policies, SSL certificates and resources attached to them. However, the downside is they ALL use the same index.html/login.js/en.xml files, so you cannot have multiple landing pages with/without the Swivel modifications.

## **120 Swivel Configuration**

## 120.1 Configuring the RADIUS server

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

### 120.2 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.

#### 120.2.1 Setting up Swivel Dual Channel Transports

See Transport Configuration

## 120.3 Citrix Access Gateway Enterprise Edition Configuration

The basis of the integration is to create new versions of the login pages. These pages are on the CAGEE and can be accessed via SSH. There are two approaches, firstly to overwrite the relevant files with those provided by Swivel Secure. The other is to actually modify those on the virtual or hardware appliance. The latter approach has the advantage the modified pages will always be based on the latest version of the CAGEE files. The main requirement for modifying these pages is to include a TURing image and the button required to request that image. The same approach could also be used to include a button/image for SMS on-demand. If the single Channel TURing image is not to be used, then the login page does not need to be modified, unless other functions are required such as the Get Security String Index. Note: TURing Images, SMS Confirmed image and Get Security String Index Images require the Swivel server to be accessible from the internet, usually with a NAT.

#### 120.3.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration

The CAGEE needs to be configured to use the Swivel server as a RADIUS authentication server. Where a VIP is being used on the Swivel server then configure the RADIUS request to be made against each of the Swivel servers together with the use of Session Sharing.

Swivel can be configured as the only authentication server or as an additional authentication server, usually this would be together with AD. The required steps are pretty much the same for both scenarios.

Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

Name Swivel RADIUS

#### Authentication type RADIUS

Secret Key The secret key configured on the Swivel NAS and also under Confirm Secret Key

Group Prefix CTXSUserGroups=

#### Group Separator ;

When complete click on Create.

🖃 🧔 NetScaler VPX 172.16.1.2 🔔	Authentication Policies an	d Servers		
G 🥥 System	Policies Servers			
Settings	Name	Туре	Server IP	
Diagnostics High Availability NTP Servers Groups Users Database Users Command Policies	Active Directory	LDAP	172.16.1.33	
Reports				
🖽 🜙 SNMP				

<u>N</u> ame*	Swivel RA	DIUS			
Authentication Type	RADIUS		•		
Server IP A <u>d</u> dress* 172	. 16 . 3	1.22	Pv <u>6</u>	Por <u>t</u> 1812 Ti <u>m</u> e-	out (seconds) 3
Details					
Secret Key*		•••••		NAS ID	
Con <u>f</u> irm Secret K	ey*	•••••		En <u>a</u> ble NAS IP address	extraction
Group Vendor Ide	ntifier			Group Prefix	CTXSUserGroups=
Group Attribute Ty	уре	8		Group S <u>e</u> parator	
IP Address Vendo	or Identifier			IP Address Attribute Type	
Pass <u>w</u> ord Vendo	r Identifier			Password Attribute Type	
Password Encodi	ing	рар	•	Accounting	OFF 💌

NetScaler VPX 172.16.1.2	Authentication Policies an	nd Servers		
System Licenses	Policies Servers			
Settings	Name	Туре	Server IP	
Diagnostics	Active Directory	LDAP	172.16.1.33	
High Availability	Swivel RADIUS	RADIUS	172.16.1.22	
NTP Servers				
Groups				
Users				
🗋 Database Users 🚽				
Command Policies				
Authentication				
Reports				
Profiles				
🗉 🧔 Auditing				
E 🥥 SNMP 🔻				

Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

Name Swivel RADIUS Policy

Authentication Type RADIUS

Server Swivel RADIUS

Named Expression True Value (Then click Add Expression so ns_true appears under Expression

🗉 🧔 NetScaler VPX 172.16.1.2 🔔	Authentication Policies	and Servers			
System	Policies \ Servers \				
Settings	Name	Туре	Rule		Req
Diagnostics High Availability High Availability NTP Servers Groups Users Database Users Command Policies Authentication Reports Profiles	Active Directory	LDAP	ns_true		Acti
< <u> </u>					
is disabled.	Details				
Navigation Pane	No item selected.				
Favor <u>i</u> tes					
Quick Links	Add 🖉 Oper	n 😰 <u>R</u> emove	] Sho <u>w</u> Bindings	Global Bindings	

Nam <u>e</u> *	Swivel RADIUS	
Authentication Type	RADIUS	
<u>S</u> erver	Swivel RADIUS Server	▼ 🛃 <u>N</u> ew 🗹 Modi <u>f</u> y
Expression		
	Expression	
Match Any Expre	ession V Add Modify Remove	@ AND @ OR (+ )+ (- )-
Match Any Expre Named Expression	s General V True value	AND OR (+ )+ (- )- Add Expression
Match Any Expre Named Expression Preview Expressio	s General  True value	AND OR (+ )+ (- )- Add Expression

RADIUS				
)+ (- )-				
dd Expression				
÷.				

🗆 🧔 Net	tScaler VPX 172.16.1.2	Au	thentication Policies and	d Servers			
Ξ 💋	System Licenses	P	Policies \ Servers \				
	Settings	Na	me	Туре	Rule	Requ	
	Diagnostics	Sw	vivel RADIUS Policy	RADIUS	ns_true	Swiv	
	High Availability	E Act	tive Directory	LDAP	ns_true	Activ	
	NTP Servers						
	Groups						
	Users						
	Database Users						
	Command Policies						
	Authentication						
	Reports						
	Profiles						
Ŧ	🧔 Auditing						
÷	SNMP	-					

The authentication must be then added such as the Access Gateway/Virtual Servers menu. If just Swivel authentication is required then ensure that only the Swivel policy is active for the Primary. If you require AD and Swivel authentication then you need to make active the Swivel policy as the secondary. Save the settings.

<ul> <li>➡ ✓ Access Gateway</li> <li>➡ Global Settings</li> <li>➡ Virtual Servers</li> <li>➡ Groups</li> <li>➡ Users</li> <li>➡ ✓ Policies</li> <li>➡ ✓ Resources</li> <li>➡ ✓ Web Interface</li> </ul>		Certificates Authentication Bookmarks Policies Intranet Applications User Authentication If your Access Gateway is to be deployed in a manner where user auther you may turn off authentication below. Please apply this option with CAUT If Enable Authentication Authentication Policies Primary Secondary
		Priority         Policy Name         Expression           100         Active Directory         ms_true
		Details : Active Directory Type: LDAP Request Profile: <u>Active Directory</u> Rule: <u>ns true</u>
	Details : CAG	Insert Policy 🔊 Unbind Policy 👔 Regenerate Priorities 📝 Mo

<ul> <li>☐ Access Gateway</li> <li>☐ Global Settings</li> <li>☐ Virtual Servers</li> <li>☐ Groups</li> <li>☐ Users</li> <li>④ Policies</li> <li>④ Resources</li> <li>④ Web Interface</li> </ul>		Certificate: User Auth If your Ac you may f Imable Authentic	s Authoricatio ccess Ga turn off a e Authen ation Poli	entication \ Bookma n ateway is to be dep authentication below tication cies	arks \ Polici bloyed in a r w. Please a	ies \ Intranet Applicat manner where user a pply this option with C	tior tuth CA
		Priority 100 Details No deta	Policy N New Po Active Swivel	Name Name Directory RADIUS Policy	•	Expression	
Feature is disabled.	Details : CAG IP Address: 172.16 Authentication: 4	Comments	rt Policy	Unbind Policy	<b>111</b> Rege	enerate Priorities 🖉	3

## 120.4 Additional Configuration Options

#### 120.4.1 Login Page Customisation

The below describes how to modify the login page for additional functionality such as the below which require the Swivel server to be accessible by the client, usually through a NAT:

- TURing Image (Automatic or requested by a button)
  Display Security String Index
  Get SMS button

Because all files in /netscaler/ns_gui are overwritten upon a restart or power cycle we create a script that copies at boot the required files from /var/mods.

See under prerequisites for the modified files that need to be uploaded to the Netscaler.

Use WINscp to use a web file tool or SSH onto the virtual or hardware appliance using an admin account. Once onto the box you need to type shell to get access to the command line.

```
>Last login: Wed Sep 10 19:12:45 2008
Done
> shell
Last login: Wed Sep 10 21:13:35 2008
```

Navigate to the location of the pages to be modified, and make a local backup copy of them

>cd /netscaler/ns_gui/vpn
>cp index.html index.html.bak
>cp login.js login.js.bak

In version 9.2 and 10.x, you will also need to modify any resource language files you use. After the above commands, do the following:

>cd resources >mkdir bak >cp *.xml bak

Note that the files in /netscaler/ns_gui/vpn are re-written when the server is rebooted therefore make sure so save these files elsewhere regularly to prevent work in progress being lost during development. How to manage these pages is covered later.

#### 120.4.1.1 index.html

The index.html file now needs to be edited (or replaced). The tool vi can be used to do this but an application such as WinSCP will make this easier. The required files can be found in the prerequisites.

Normally, you can use the index.html file as it is, but there are two possible modifications you may want to consider.

Currently, the TURing image is only shown (or security string sent) when you click on the appropriate button. You may prefer that this happens as soon as the username is entered. To do this, you need to add an attribute to the username field, as follows:

Firstly, find the field. If you search for "loginFieldCheck", you should locate the following:

onFocus="loginFieldCheck()"

Add a new attribute after this, as follows:

onBlur="showTuring()"

Make sure that you leave a space before and after the new attribute.

If you want to want to send security strings to SMS or email on-demand, rather than showing a TURing image, you may want to change the label of the button. You can do this as follows:

First, locate the code that renders the button by searching for "btnTuring". You will find the following code within the line:

id="btnTuring" value="Get Image"

Change the value attribute to an appropriate alternative, such as "Send Message".

#### 120.4.1.2 pinsafe.js

A pinsafe.js file that is a modification of the existing login.js file is required. Make a copy of login.js called pinsafe.js The sUrl setting needs to be changed to reflect the IP address and port number of the relevant Swivel server.

For a virtual or hardware appliance this will normally be similar to:

sUrl="https://turing.swivelsecure.com:8443/proxy/SCImage?username=";

#### For a software only install see Software Only Installation

To request a security string on demand, instead of a TURing image, replace SCImage with DCMessage, for example:

sUrl="https://IP_address:8443/proxy/DCMessage?username=";

Note that using message on demand will display a "CONFIRMED" image instead of a TURing image. If you prefer not to have this visual confirmation, remove the following line which you will find a little lower down:

varImg.style.visibility = "visible";

#### 120.4.1.3 Language resource files

Modify the language resource files, which can be found in the resources sub-folder of the vpn folder. If you are only using the English language, then edit en.xml and search for

<String id="Password2">

Replace the value for id="Password2" with "OTC:". Also, insert a new string for id="Password1" with a value of "AD Password". You should therefore have 2 lines as follows:

```
<String id="Password1">AD Password</String>
<String id="Password2">OTC:</String>
```

(Note that Password1 has no colon at the end, whereas Password2 has a colon).

If you will be using languages other than English, you will also need to edit any other language files you use, replacing the value for Password2 with the appropriate label for OTC (One-time code) and inserting a new string for Password1 with the label for AD (Active Directory) password.

Because all files in /netscaler/ns_gui are overwritten upon a restart or power cycle, a script must be created that runs at startup to copy the modified files back to this location. The nsafter shor rc.netscaler shell scripts can be created or modified to accomplish this. For example via ssh:

shell

- # mkdir /var/mods
  # cp /netscaler/n
- cp /netscaler/ns_gui/vpn/index.html /var/mods/index.html.mod

ccp /netscaler/ns_gui/vpn/pindex.html /var/mods/hindex.html.mod ccp /netscaler/ns_gui/vpn/pinsafe.js /var/mods/pinsafe.js.mod touch /nsconfig/rc.netscaler echo cp /var/mods/index.html.mod /netscaler/ns_gui/vpn/index.html >> /nsconfig/rc.netscaler echo cp /var/mods/pinsafe.js.mod /netscaler/ns_gui/vpn/pinsafe.js >> /nsconfig/rc.netscaler cp /netscaler/ns_gui/vpn/resources/en.xml /var/mods/en.xml.mod echo cp /var/mods/en.xml.mod /netscaler/ns_gui/vpn/resources/en.xml >> /nsconfig/rc.netscaler

#### 120.4.1.4 PINpad

This is a version of the 9.3 customisation modified for Pinpad. Currently in beta testing. Note that in order to use PINpad you will need a Swivel virtual or hardware Appliance with the latest proxy application installed. You can get this from here.

PINpad pre-req

#### 120.4.2 Challenge and Response

Citrix Access Gateway Enterprise Edition 9.2 and 10.x support RADIUS Challenge and Response. Configure the Swivel server to use Two Stage Authentication and Check Password With Repository, see also Challenge and Response How to Guide

Challenge and response is usually configured with Username, and AD password for LDAP authentication, and Swivel configured to use AD password in order to request the SMS message to be sent to the user. It is possible to modify the login page so that the AD password need only be entered once. A modified page can be downloaded from here: CAGEE Two Stage Login page

To install the login page use the same procedure as the Single Channel login page.

#### 120.4.3 Image Request button displayed when needed

The following code allows the Single Channel Image request button to be only shown when required. This is useful for refreshing an image or when SMS/Mobile client authentication is used, since when a Single Channel image is generated, either automatically or manually, it then expects a single channel login (within 2 minutes by default).

```
function ns_showpinsafe()
{
  var pspwc = ns_getcookie("pwcount");
    if ( pspwc == 2 )
    {
      document.write('<img src="/vpn/images/LoginButtonRolloverGlow.gif"/>');
      document.write('<ingu type="button" id="btnTuring" value="Get Image" ');
      document.write('onclick="showTuring();" class="CTX_CaxtonButton" ');
      document.write('TX_CaxtonButton_Hover';");
      document.write('"CTX_CaxtonButton_Hover';");
      document.write('"CTX_CaxtonButton';");
      document.write('"/>');
      document.write('
```

### 120.5 Testing

Browse to the login page and check that a Turing image appears and the One time Code can be entered to login.

For SMS or Mobile Phone Apps do not click on the Get Image button, but enter the OTC

User name:	graham
AD Password:	••••
OTC:	••••
	Get Image Log On

If the incorrect credentials are used then the login should fail

Welcom	ie	
Please log o	n to continue. User name: Password 1: Password 2:	
		Log On
The c help d	redentials you typed are incori lesk or system administrator.	ect. Please try again or contact your
	CITRE	

Where the TURing image is not used, then the Get Image page modification can be omitted

Please log on	to continue.		
	User name:	graham	
	Password 1:	•••••	
	Password 2:	••••	
		Log Or	

### 120.6 Uninstall/Removing the integration

If the login pages have been modified restore the default login page and remove the added files.

Remove Swivel as the authentication server.

### **120.7 Troubleshooting**

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

The CAGEE Netscaler checks each password/OTC in turn, so if the AD password is checked first and is incorrect then the secondary authentication will not be tested.

### 120.8 Known Issues and Limitations

The CAGEE caches the javascript so when you make modifications on the CAGEE they are not reflected on the log-in page as rendered. A way round this is to change the name of the .js file and edit the index.html file to use this new .js file. see [1]

### **120.9 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

# 121 Citrix Access Gateway Standard 4.x

## **122 Introduction**

This document covers the integration of Swivel with the Citrix Access Gateway Standard edition. The standard edition allows authentication using SMS, Email, Mobile Phone applet, PINsafe Taskbar, but does not allow the single channel image to be embedded into the login page. To allow the single channel image to be embedded into the login page, the Advanced Access Controller is required, see Citrix Access Gateway Advanced 4.x

# **123 Prerequisites**

Swivel 3.x Citrix Access Gateway 4.x

## 124 Baseline

## **125 Architecture**

Authentications are made against Swivel using RADIUS.

# 126 Installation

## **127 Swivel Configuration**

## 127.1 Configuring the RADIUS server

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

## 127.2 Setting up PINsafe Dual Channel Transports

See Transport Configuration

## 127.3 Citrix Access Gateway Standard Edition Integration

Follow the Citrix Access Gateway Standard Edition Administration guide to configure RADIUS authentication.

## **128 Additional Information**

For additional features use the Advanced Access Controller. This allows customised login pages and the Single Channel Turing Image authentication, see Citrix Access Gateway Advanced 4.x

# 129 Citrix Access Gateway Standard 5.x

## **130 Introduction**

This document covers the integration of Swivel with the Citrix Access Gateway Standard edition. The standard edition allows authentication using SMS, Email, Mobile Phone applet, Swivel Taskbar, but does not allow the single channel image to be embedded into the login page. To allow the single channel image to be embedded into the login page, the following options are available:

- Advanced Access Controller is required, see Citrix Access Gateway Advanced 4.x
  Proxy the login request to a Web Interface login Citrix Access Gateway Web Interface Proxy

# **131 Prerequisites**

Swivel 3.x Citrix Access Gateway 5.x
## 132 Baseline

PINsafe 3.8 CAG Standard 5.0.3

## **133 Architecture**

Authentications are made against Swivel using RADIUS.

# 134 Installation

# **135 Swivel Configuration**

#### 135.1 Configuring the RADIUS server

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

#### 135.2 Setting up PINsafe Dual Channel Transports

See Transport Configuration

### **136 Citrix Access Gateway Standard Edition Integration**

Follow the Citrix Access Gateway Standard Edition Administration guide to configure RADIUS authentication.

#### **136.1 CAG RADIUS Properties**

On the CAG Configuration, configure one or more PINsafe instances as a RADIUS server.

		General Prop	erties		
Profile name:	*	Swivel			
Description:		Swivel			
Single sign-on domain:		IGroup			
		RADIUS Serv	ers		
Network time-out:		5 🔺 s	econds		
Servers list:	*	Server	Port	Accounting	Priority
		1,1.1.1	1812	1813	1
		New	Remove	1	Nove: 🕇 🖡
		Group Author	ization		
Attribute value prefix:		CTXSUserGrou	ips=		
Separator:		1			
Vendor attribute:		0			
Vendor code:					

#### **136.2 CAG logon Point Properties**

Configure Swivel as an authentication server. Swivel would usually be configured as a secondary authentication server with AD as the primary authentication server using RADIUS. In this example Single Sign ON is being used to the Citrix Web Interface, and has been created as a basic logon point.

	General Properties		Logon Point Visibility	User Remediation Message
Name:	* swivel		Control visibility	Show message
Description:	Swivel desktop	Device profiles:		
	Disable			
Туре:	Basic   •			
	Authenticate with Web Interface	Hataba		
Web Interface:	https:// /Citrbc/C	Match:	All	
	Authentication Profiles		Provide Description	
Primary:	LDAP V		Session Properties	
Secondary:	Swivel 🔹		Uvernoe user inactivity time-out	
	Require user name		(un)	
	Single sign-on		Override network inactivity time-out:	
	to Web Interface		(011)	
	Authorization Profiles		Override session time-out.	
Primary:	None		1 minutes	
Secondana	Room		10	

# **137 Additional Installation Options**

# 138 Verifying the Installation

Browse to the CAG login page and enter username, AD Password and OTC from the SMS or Mobile Phone Client. Check the PINsafe logs to ensure that a RADIUS request has been seen.

Welcome	e on to continue
User name:	Group
Password:	
Password:	•••••
	Submit
	CITRIX

# 139 Uninstalling the PINsafe Integration

# 140 Troubleshooting

# 141 Known Issues and Limitations

## **142 Additional Information**

For additional features use the Advanced Access Controller. This allows customised login pages and the Single Channel Turing Image authentication, see Citrix Access Gateway Advanced 4.x

# 143 Citrix Access Gateway Web Interface Proxy

## **144 Introduction**

This document is to supplement the Citrix Access Gateway and Citrix Web Interface documentation for the deployment of PINsafe on the Web Interface and using the Secure Ticket Authority to pass authentication from the Citrix Access Gateway to the Citrix Web Interface.

# **145 Prerequisites**

Citrix Access Gateway 5.x Citrix Web Interface 5.x PINsafe 3.x

## 146 Baseline

Citrix Access Gateway 5.0 Citrix Web Interface 5.4

PINsafe 3.8

## 147 Architecture

When a user authenticates to the Citrix Access Gateway, the authentication is passed to the Web Interface and the user may use PINsafe authentication.

#### 148 Installation

#### 148.1 PINsafe and Web Interface Integration Configuration

Follow the steps for the appropriate version of PINsafe Web Interface Integration on the PINsafe server see Integrations. Test that this integration is fully working.

#### 148.2 CAG Standard and CAG VPX configuration and installation

Configure the Access Gateway with networking information in the required deployment scenario. On the CAG enter under Name Service Providers the IP address and Fully Qualified Hostname of the Web Interface server under the section HOSTS File.

	Domain Name Servers	WINS Ser	ver	
First DNS Server:	8.8.8.8			
Second DNS Server:	8.8.4.4			
Third DNS Server:				
HOSTS File			DNS Suffixes	
Click New to add the domain name to the	e IP address and fully qualified HOSTS file.		Do not precede a s DNS server as site.	uffix with a period. Specify the com, not .site.com.
Click New to add the domain name to the IP Address	e IP address and fully qualified HOSTS file. Fully qualifi	ied domain name	Do not precede a s DNS server as site. Suffix	suffix with a period. Specify the com, not .site.com. Priority
Click New to add th domain name to the IP Address 192.168.1.102	e IP address and fully qualified HOSTS file. Fully qualifi TSWIDMZ	ied domain name	Do not precede a a DNS server as site. Suffix	suffix with a period. Specify the com, not .site.com.

Under Deployment Mode set the Access Gateway Mode to Appliance Only.

Configure the settings t appliance.	to use the Delivery Services Console for Access Controller	r to configure the Access Gateway
	Access Gateway Settings	
Identifier:	* best to be the second se	Сору
Access Gateway mode	e: <ul> <li>Appliance only</li> <li>Access Controller</li> </ul>	
S	elect your preferred mode for configuring settings to manage coess Gateway.	
_	Access Controller Settings	, ,
Shared key:	*	Сору
Server address:	*	
	Secure connection	
Port:	* 80	
Indicates required field	4	

Set the Logon Point as home.

nable users to r	og on with a user name and password, ar	a their connect to resources in t	ine internal networ	ĸ.
Name	Description	Туре	Enabled	Default
Br		Basic	4	6

Configure the Logon Point Properties to authenticate with the Web Interface, using the hostname allows the DMZ IP address range to be hidden.

Properties	Customization			
	General Properties		Logon Point Visibility	User Remediation Me
Name:	<mark>⊧</mark> βr			Show message
Description:		Device profiles:		
	Disable			
Туре:	Basic			
	Authenticate with Web Interface	Match:	All	
	Website Configuration			
			Session Properties	
	Authentication Profiles		Override user inactivity time-out:	
Primary:	None v		0 (off)	
Secondary:	None		Override network inactivity time-out:	
			0 (off)	
	Authorization Profiles		Override session time-out:	
Primary:	None		1 minutes	
Secondary:	None			

Enter the Web Interface server for the Web Address and Application Type should be WEBINTERFACE.

of addresses to which Access Gate	way will allow access.		
Beginning IP Address	Ending IP Address	Protocol	Por
192.168.0.1	192.168.0.200	ICA	1494

Configure the Web Interface as the STA (Secure Ticket Authority).

Secure Ticket A	uthority (STA	<ul> <li>issues tickets in respons</li> <li>Click New to configure STA</li> </ul>	e to connection requests	for published applications
gured in the we	b interiace.	click new to configure STA	servers on Access Gate	way.
Server	Port	Path	Identifier	Connection Type
Server	Port 8080	Path /Scripts/CtxSTA.dll	Identifier STA150	Connection Type unsecure

#### 148.3 Citrix Web Interface configuration and installation

On the Citrix Web Interface edit the Secure Access Settings, Access Methods to be Gateway Direct.

Secure Acc	ess Setti	ngs - XenApp	
			CITRIX
Specify	Acces	s Methods	
ipecify detals iccess metho Jser device a	of the DM d. <u>More</u> ddresses (ir	2 settings, including IP addre order):	ss, mask, and associated
IP address	Mask	Access method	Move Up
Derault		dialeway direct	Move Down
Add	Edit.	Remove	

The (FQDN) Fully Qualified Domain Name needs to be entered for the Gateway Settings

dit Secure Access	Settings - Xe	enApp			×
					CITRIX
Specify Ga	teway Se	ettings			
Specify gateway se the Access Gatewa	rver details for ly <u>or Secure Ga</u>	any user device ateway. <u>More</u>	es that access	this site throug	h 
Address (FQDN):	citrix.swivelse	cure.com			
Port:	443				
Enable session	reliability				
E Request tick	kets from two S	TAs, where avai	lable		
			< Back	Next >	Cancel

#### 148.4 Additional Installation Options

# 149 Verifying the Installation

Browse to the login page and authenticate with PINsafe credentials.

# 150 Uninstalling the PINsafe Integration

# 151 Troubleshooting

# 152 Known Issues and Limitations

# **153 Additional Information**

154 Citrix Netscaler Gateway 10.x

### **155 Introduction**

This document shows the steps required to integrate Swivel with the Citrix Access Gateway Enterprise Edition 10.1 and 10.5 (Netscaler VPN). 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.

For version 10.0 refer to Citrix Access Gateway Enterprise Edition 10

For versions 8.x to 9.1 refer to Citrix Access Gateway Enterprise Edition 8,

For other versions of 9.x see Citrix Access Gateway Enterprise Edition 9.

It covers the following steps.

- Configuring Swivel to accept authentication requests from the CAGEE
  Modifying the CAGEE login pages
  Configuring the CAGEE to authenticate via PINsafe

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 Network Address Translation, often with a proxy server. The Swivel virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection. The Netscaler can be configured using its load balancing bridging feature to allow a Swivel Severs IP to provide Single Channel images, such as TURing and PINpad.

Citrix Netscaler 10.5 has a new HTML GUI interface for management, although the customisation pages using java script remains the same.

### **156 Prerequisites**

Access Gateway Enterprise Edition firmware version 10.1 or higher

An administrative logon account for the Access Gateway

A Secure Shell (SSH) programme (eg putty) and an SSH-based file transfer application such as WinSCP

A Unicode-aware text file editor such as TextPad or WordPad

Swivel 3.x

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, this is usually implemented by a NAT to the Swivel server. Ensure that only the required ports are allowed access.

Netscaler pages to modify and/or Swivel files for version 10.x default theme or the Green Bubble 10.x theme

The following pages are for 10.5: only the language resources are different from 10.x. Version 10.5 default theme. Green Bubble 10.x theme.

#### 156.1 Note on upgrading the Netscaler

When upgrading see the note below if custom pages are used upgrading Netscalers with Custom Pages

## 157 Baseline

Tested with Swivel 3.9.6 Citrix Netscaler Gateway NS10.1 Build 121.10 Citrix Netscaler Gateway NS10.5

## **158 Architecture**

The Citrix Advanced Access Gateway Enterprise Edition makes authentication requests against the Swivel server by RADIUS.

You can create different logon realms / pages called Virtual Servers, these can have different authentication servers/policies, SSL certificates and resources attached to them. However, the downside is they ALL use the same index.html/login.js/en.xml files, so you cannot have multiple landing pages with/without the Swivel modifications.

### **159 Swivel Configuration**

#### 159.1 Configuring the RADIUS server

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

#### 159.2 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.

#### 159.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

## **160 Citrix Netscaler Gateway Configuration**

The Swivel integration uses RADIUS authentication, and where the login page is modified it uses the Netscaler custom web pages which are configured and then copied into an archive file which is deployed at boot time.

#### 160.1 Citrix Advanced Access Gateway Enterprise Edition RADIUS Configuration

The CAGEE needs to be configured to use the Swivel server as a RADIUS authentication server. Where several Swivel virtual or hardware appliances are used for resilience, configure the RADIUS request to be made against each of the Swivel servers together with the use of Session Sharing. Note: for virtual or hardware appliances, the Swivel VIP should not be used as the RADIUS server IP address, see VIP on PINsafe Appliances

Swivel can be configured as the only authentication server or as an additional authentication server, usually this would be together with AD. The required steps are pretty much the same for both scenarios.

Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

#### Name Swivel RADIUS

#### Authentication type RADIUS

Secret Key The secret key configured on the Swivel NAS and also under Confirm Secret Key

Group Prefix CTXSUserGroups=

#### Group Separator ;

When complete click on Create.

If the Authentication option is not available check that the license allows authentication to be configured on the Netscaler licensing page.

🗉 🧔 NetScaler VPX 172.16.1.2 📤	Authentication Policies an	id Servers		
System Licenses	Policies Servers			
Settings	Name	Туре	Server IP	
<ul> <li>Diagnostics</li> <li>High Availability</li> <li>NTP Servers</li> <li>Groups</li> <li>Users</li> <li>Database Users</li> <li>Command Policies</li> <li>Authentication</li> <li>Reports</li> <li>Profiles</li> </ul>	Active Directory	LDAP	172.16.1.33	
🗉 词 Auditing				
E 🧔 SNMP 🔻				

<u>N</u> ame*	Swivel RADIUS	]	
Authentication Type	RADIUS	)	
Server IP A <u>d</u> dress* 172	. 16 . 1 . 22	7 <u>6</u> Por <u>t</u> 1812 Ti <u>m</u> e	-out (seconds) 3
Details			
Secret Key*	ev#	NAS ID	s extraction
Group Vendor Ide	entifier	Group Prefix	CTXSUserGroups=
IP Address Vendo	or Identifier	IP Address Attribute Type	
Pass <u>w</u> ord Vendo	r Identifier	Password Attribute Type	
Password Encod	ing pap	<ul> <li>Accounting</li> </ul>	OFF •
🕑 <u>H</u> elp 👍 Quick I	Link		<u>C</u> reate Close

NetScaler VPX 172.16.1.2	Authentication Policies an	id Servers		
System Licenses	Policies Servers \			
Settings	Name	Туре	Server IP	
Diagnostics	Active Directory	LDAP	172.16.1.33	
High Availability	Swivel RADIUS	RADIUS	172.16.1.22	
NTP Servers				
Groups				
Users				
🗋 Database Users				
Command Policies				
Authentication				
Reports				
Profiles				
🗉 🧔 Auditing				
E 🥥 SNMP 🔻				

Under the Netscaler->System->Authentication select the Servers Tab and then click add, enter the following information:

Name Swivel RADIUS Policy

Authentication Type RADIUS

Server Swivel RADIUS

Named Expression True Value (Then click Add Expression so ns_true appears under Expression

🗉 🧔 NetScaler VPX 172.16.1.2 🔔	Authentication Policies	and Servers				
System	Policies Servers					
Settings	Name	Туре	Rule		Req	
Diagnostics High Availability High Availability NTP Servers Groups Users Database Users Command Policies Authentication Reports Profiles	Active Directory	LDAP	ns_true		Acti	
< <u> </u>						
🔞 🧿 Feature is disabled.	Details No item selected.					
Navigation Pane						
Favor <u>i</u> tes						
Quick Links	Add 🖉 Open	n 😰 <u>R</u> emove [	3 Sho <u>w</u> Bindings	Global Bindings		
Nam <u>e</u> *	Swivel RADIUS					
----------------------------------------------------------	----------------------------	-----------------------------------				
Authentication Type	RADIUS					
Server	Swivel RADIUS Server	🔻 🖪 New 🖉 Modi <u>f</u> y				
Expression						
	Expression					
Match Any Expre	ession V Add Modify Remove	AND OR (+ )+ (- )-				
Match Any Expre Named Expression	s General V True value	AND OR (+ )+ (- )- Add Expression				
Match Any Expre Named Expression Preview Expressio	s General  True value	AND OR (+ )+ (- )- Add Expression				

am <u>e</u> *	Swivel RADIUS Policy	
uthentication Type	RADIUS	
erver	Swivel RADIUS	di <u>f</u> y
Expression		
	Expression	
	ession  ADD OR (+ )+ (-	
Match Any Expre		)-
Named Expression	s General 👻 True value 🔹 🗘 A <u>d</u> d Express	)- sion

🗆 🧔 Net	tScaler VPX 172.16.1.2	Au	thentication Policies and	d Servers		
System Licenses		P	olicies \ Servers \			
	Settings	Na	me	Туре	Rule	Requ
	Diagnostics	Sw	vivel RADIUS Policy	RADIUS	ns_true	Swiv
High Availability	E Act	Active Directory	LDAP	ns_true	Activ	
	NTP Servers					
	Groups					
	Users					
	Database Users					
	Command Policies					
	Authentication					
	Reports					
	Profiles					
Ŧ	🧔 Auditing					
÷	SNMP	-				

The authentication must be then added such as the Access Gateway/Virtual Servers menu. If just Swivel authentication is required then ensure that only the Swivel policy is active for the Primary. If you require AD and Swivel authentication then you need to make active the Swivel policy as the secondary. Save the settings.

<ul> <li>Access Gateway</li> <li>Global Settings</li> <li>Virtual Servers</li> <li>Groups</li> <li>Users</li> <li>Ø Policies</li> <li>Resources</li> <li>Web Interface</li> </ul>		Certificates Authentication Bookmarks Policies Intranet Applications User Authentication If your Access Gateway is to be deployed in a manner where user auther you may turn off authentication below. Please apply this option with CAUT I Enable Authentication Authentication Policies Primary Secondary
		Priority         Policy Name         Expression           100         Active Directory <ul></ul>
		Details : Active Directory Type: LDAP Request Profile: Active Directory Rule: ns true
	Details : CAG	Insert Policy 🔐 Unbind Policy 👔 Regenerate Priorities 📝 Mo

<ul> <li>Access Gateway</li> <li>Global Settings</li> <li>Virtual Servers</li> <li>Groups</li> <li>Users</li> <li>Ø Policies</li> <li>Ø Resources</li> <li>Web Interface</li> </ul>		Certificate User Auth If your A you may I Enable Authentic	s Auth nenticatio ccess Ga turn off a le Auther ation Pol ary	entication \ Bookma on ateway is to be dep authentication below ntication icies Secondary	loyed in a r v. Please a	ies \ Intranet Application nanner where user auth pply this option with CA
		Priority 100 Details No deta	Policy Po	Name Directory RADIUS Policy	*	Expression
Feature is disabled.	Details : CAG IP Address: 172.16 Authentication: 0	Comments	rt Policy	Unbind Policy	<b>11</b> Rege	enerate Priorities 📝

# 160.2 Citrix Receiver with Netscaler configuration

See Citrix Netscaler configuration for Receiver

# **161 Additional Configuration Options**

## 161.1 Netscaler RADIUS Monitor and RADIUS Load Balancer

See Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer

## 161.2 Netscaler SSL Bridge

The Netscaler allows a SSL Bridge to be created that allows a Network Address Translation to allow access to the Swivel instance to provide single channel images or Mobile App security strings. On the Netscaler Gateway Administration Console Configuration tab select Traffic Management, Load balancing, Virtual Servers, then click on Add, to open a Create Virtual Server (Load Balancing) window.

The Netscaler requires an external NAT to the Swivel server, and the Netscaler Network bridge allows this to be done using the Netscaler. The Swivel appliance is usually use to provide the proxy port on 8443 or 443

Name Name of the SSL Bridge

Select IP Adress Based

Protocol select SSL_Bridge

IP address Enter the public IP Address

Port Enter the Swivel instance port number, usually 8443

The following should be ticked Directly Accessible', State, AppFlow Logging

Create Virtu	al Server (Load Balancing	g)				
Name*	Swivel-SSL-Bridge		IP Addres	ss Based 🔿 IP Patte	rn Based	
Protocol*	SSL_BRIDGE		✓ IP Address*	10 . 10 .	10 . 10	
🗌 Networ	k VServer Range 1		Port*	8443		
Directly	Addressable 🖌 State	AppFlow Logging	Traffic Dom	ain ID		
Enable	DNS64 DBvpass AAAA	Requests				
Services	Sanvisa Ground Dali	rice Method and Persist		Slar Settings	ř.	
Activate	Service Groups   Poli	cies   Method and Persist		lies 552 Settings		
Active	Service Name	IP Address	Port Protocol Stat	e	Weight	D
	Swivel_8443	192.168.12.111	8443 SSL_BRID @ U	JP	1	
Add.	. 📝 O <u>p</u> en <u> R</u> emov	e				
Comment	5					
@ <u>H</u> elp						Create

Click Add and enter the required details.

ate Service						
ervice <u>N</u> ame*	Swivel_8443		Ser <u>v</u> er* 192.1	68.12.111		
ro <u>t</u> ocol*	SSL_BRIDGE	-	Port* 443			
raffic Domain						
Enable Servi	ice		Number of A	ctive Clients		
Change Stat	te Enable Health <u>M</u> onitori	ng 🗹 AppFlow Lo	ogging	L		
Available	Policies   Profiles   Advanced	SSL Settings	- Configured			
Monitors		1	Monitors	Weight	State	Passive
arp	*		tcp	1	Image: Second	
nd6						
ping						
http	_		1			
tcp-ecv	-	Add >				
http-ecv		< <u>R</u> emove				
udp-ecv						
dns						
ftp						
tcps						
	*					

Service Name Name of the SSL Bridge

Server Swivel server address

Protocol select SSL_Bridge from the drop down menu

port select the port used to connect to the SSL bridge, usually 443

From the Monitors tab select TCP then Add it to the list of Configured so that it appears on the right hand side with the State box checked., then click on Create.



## 161.3 Login Page Customisation

This step only needs to be followed if login page customisation is required.

## 161.4 Upgrading Netscalers with Custom Pages

Citrix recommend when upgrading a Netscaler with custom pages, the custom pages should be set back to use default pages, upgrade and then the custom pages reapplied. When upgrading it is recommended to make a backup or snapshot of the existing system.

When upgrading a Netscaler 10.1 with custom pages to 10.5, backup the modified pages and scripts, then set the login page back to default. Upgrade, test the Administration console, then upload the modified pages as if carrying out a new Swivel install as given below, then recreate the custom tar file as below as this will then include the updated GUI.

### 161.5 Customisation Overview

#### **One Touch**

One touch is a different approach as the user is redirected to a separate page to authenticate and therefore does not actually see the Netscaler login page.

#### Refer to VPN OneTouch Integration

To customise the page for one touch you need to include the following in the header section of index.html where <swivelappliance> is the hostname of the associated Swivel Appliance

```
//-> Swivel elements
function redirect() {
window.location.replace("https://<swivelappliance>:8443/onetouch/onetouch?returnurl=" + window.location.href );
var QueryString = function () {
 if (typeof query_string[pair[0]] === "undefined") {
   query_string[pair[0]] = pair[1];
   // alert(pair[0] + "," + pair[1]);
   // If second entry with this name
} else if (typeof query_string[pair[0]] === "string") {
   var arr = [ query_string[pair[0]], pair[1] ];
   query_string[pair[0]] = arr;
   //alert(pair[0] + "," + arr);
   // If third or later entry with this name
} else {
     } else {
        query_string[pair[0]].push(pair[1]);
     }
 }
    return query_string;
} ();
$(document).ready(function(){
    usernamePassedIn = QueryString["username"];
    passwordPassedIn = QueryString["password"];
if(typeof passwordPassedIn == 'undefined') {
  redirect();
   else {
$('[name=passwd]').val(passwordPassedIn);
document.getElementsByName("vpnForm")[0].submit();
```

});

Before the closing </SCRIPT> tag

See under **prerequisites** for the modified files that need to be uploaded to the Netscaler.

Note on editing files: If the files are edited in Winsdows based systems it may be possible that control code ^M are added to the end of the line. These can be viewed and removed by using vi.

The below describes how to modify the login page for additional functionality such as the below which require the Swivel server to be accessible by the client, usually through a NAT:

- TURing Image (Automatic or requested by a button)
   Display Security String Index
- Get SMS button

Because all files in /netscaler/ns_gui are overwritten upon a restart or power cycle, they are incorporated into the archive deployed at boot time.

### 161.5.1 Login to Netscaler Command Line

Use WINscp to use a web file tool or SSH onto the virtual or hardware appliance using an admin account. Once onto the box you need to type shell to get access to the command line.

```
>Last login: Wed Sep 10 19:12:45 2008
Done
 shell
Last login: Wed Sep 10 21:13:35 2008
```

### 161.5.2 Backup Netscaler files

Navigate to the location of the pages to be modified, and make a local backup copy of them.

```
cd /netscaler/ns_gui/vpn
cp index.html index.html.bak
```

#### 161.5.3 Customise the login script

The login page can be customised using the standard theme or the Green bubble theme, or possibly another theme. Download the required theme from the pre-requisites above. Note that to use the customised Green Bubble theme, you first have to select the standard Green Bubble theme, then apply the customisation.

#### 161.5.3.1 Requesting a TURing image

These files can be modified before uploading

Modify pinsafe.js. The pinsafeUrl variable value in pinsafe.js needs to be changed to reflect the Hostname and port number of the relevant Swivel server.

For an virtual or hardware appliance this will normally be similar to:

pinsafeUrl="https://turing.swivelsecure.com:8443/proxy/";

For a software only install see Software Only Installation

#### 161.5.4 Customise the login prompt

Modify the language resource files in /netscaler/ns_gui/vpn/resources. If you are only using the English language, then edit en.xml and search for

<String id="Password2">

this should be around line 59.

Replace the value for id="Password2" with "OTC:". Also, insert a new string for id="Password" with a value of "AD Password". You should therefore have 2 lines as follows:

<String id="Password">AD Password</String>
<String id="Password2">OTC:</String>

(Note that Password1 has no colon at the end, whereas Password2 has a colon).

#### 161.5.4.1 Additional Languages file modifications

If you will be using languages other than English, you will also need to edit any other language files you use, replacing the value for Password2 with the appropriate label for OTC (One-time code) and inserting a new string for Password1 with the label for AD (Active Directory) password.

Edit the file rc.netscaler to copy across any modified language pages, as for English which is included in the script.:

cp /var/mods/en.xml.mod /var/netscaler/gui/vpn/resources/en.xml

#### 161.5.5 Upload files to Netscaler

On the Netscaler ensure that either the default or green bubbles theme is used. On the Netscaler Gateway, select Netscaler Gateway/Global Settings, then click on Change Global Settings, and under the Client Experience tab check the UI Theme. After modifying the pages, this will be set to custom.

Download the files under the prerequisites and modify as described above, then copy them to the following locations:

index.html to /var/netscaler/gui/vpn/index.html

pinsafe.js to /var/netscaler/gui/vpn/pinsafe.js

#### 161.5.6 Create the boot archive file

mkdir /var/ns_gui_custom

cd /netscaler

tar -zcvf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*

This should create the customtheme.tar.gz file used at boot time, and list all the files used.

#### 161.5.7 Tell the Netscaler to use the customised login pages

/netscaler/ns_gui is a symbolic link that by default points to /var/netscaler/gui, by setting the custom login, this link changes to the custom pages i.e. /var/ns_gui_custom/ns_gui. Therefore it is important that the above boot archive be created before switching to custom. Also note that WinSCP may cache the symbolic link and give the wrong location, so may need to be refreshed in the /netscaler folder.

On the Netscaler Gateway, select Netscaler Gateway/Global Settings, then click on Change Global Settings, and under the Client Experience tab change the UI Theme to Custom, then click on OK

Note: If the Netscaler pages are changed back from Custom to Default, then the index.html is replaced with the default index.html, and if a new custom page is required, then the custom index.html will need to be copied back.



### 161.5.8 Reboot Netscaler to verify files are copied across

Reboot the Netscaler to ensure that the files are copied across at boot time and that the login page has been modified as required.

### 161.6 Additional Login Customisation options

### 161.6.1 Automated TURing Display

With the automated TURing display, when the user leaves the username field, the TURing will be automatically displayed. A login using the TURing image is expected for that user.

#### Edit the index.html file

search for onFocus="loginFieldCheck()"

#### Add a new attribute after this, as follows:

```
onBlur="showTuring()"
```

#### Example:

```
onFocus="loginFieldCheck()" onBlur="showTuring()" style="width:100%;"
```

#### 161.6.2 Changing the button labels

If you want to want to change the button text such for sending security strings to SMS or email on-demand, rather than showing a TURing image, or change the GET Image text you may want to change the label of the button. You can do this as follows:

Edit the index.html file and locate the code that renders the button by searching for "btnTuring". You will find the following code within the line:

id="btnTuring" value="Get Image"

Change the value attribute to an appropriate alternative, such as "Send Message".

#### 161.6.3 Requesting the string Index

See also Multiple Security Strings How To Guide

Modify pinsafe.js. The pinsafeUrl setting in pinsafe.js needs to be changed to reflect the hostname and port number of the relevant Swivel server.

For a virtual or hardware appliance this will normally be similar to:

pinsafeUrl="https://turing.swivelsecure.com:8443/proxy/DCIndexImage?username=";

For a software only install see Software Only Installation

#### 161.6.4 PINpad

This is a version of the 9.3 customisation modified for Pinpad. Currently in beta testing. Note that in order to use PINpad you will need a Swivel virtual or hardware appliance with the latest proxy application installed. You can get this from here.

PINpad pre-req

#### 161.6.5 Requesting an SMS

See also Challenge and Response below

Modify pinsafe.js. The pinsafeUrl setting in pinsafe.js needs to be changed to reflect the hostname and port number of the relevant Swivel server.

For an virtual or hardware appliance this will normally be similar to:

pinsafeUrl="https://turing.swivelsecure.com:8443/proxy/DCMessage?username=";

For a software only install see Software Only Installation

### 161.7 Challenge and Response

Citrix Access Gateway Enterprise Edition 9.2 and 10.x support RADIUS Challenge and Response. RADIUS Challenge and Response can be optionally configured to enter a username and Password, which will then ask for a One Time Code. Configure the Swivel server to use Two Stage Authentication and Check Password With Repository, see also Challenge and Response How to Guide

Challenge and response is usually configured with Username, and AD password for LDAP authentication, and Swivel configured to use AD password in order to request the SMS message to be sent to the user. It is possible to modify the login page so that the AD password need only be entered once. A modified page can be downloaded from here: CAGEE Two Stage Login page

To install the login page use the same procedure as the Single Channel login page.

If Single Channel is not being used at all, then a TURing image is not required. Therefore, if you configured a message Resend button (which would replace a Show Image button), then in the pinsafe.js, the parameter:

onclick= "showTuring();"

Must be changed to:

onclick= "sendMessage();"

Optionally, you can remove the showTuring function altogether. Which is in addition to the above step of changing onClick=.

#### Example fucnction code:

function showTuring() {showImage(pinsafeUrl + "SCImage");}

### 161.8 Image Request button displayed when needed

The following code allows the Single Channel Image request button to be only shown when required. This is useful for refreshing an image or when SMS/Mobile client authentication is used, since when a Single Channel image is generated, either automatically or manually, it then expects a single channel login (within 2 minutes by default).

```
function ns_showpinsafe()
{
  var pspwc = ns_getcookie("pwcount");
    if ( pspwc == 2 )
    {
        document.write('');
        document.write('');
        document.write('<img src="/vpn/images/LoginButtonRolloverGlow.gif"/>');
    }
}
```

```
document.write('');
document.write('cinput type="button" id="btnTuring" value="Get Image" ');
document.write('onnouseover="this.className=');
document.write("'cTX_CaxtonButton_Hover';");
document.write("" onnouseout="this.className=');
document.write("" onnouseout="this.className=');
document.write("" cTX_CaxtonButton';");
document.write("'cTX_CaxtonButton';");
document.write('" />');
document.write('' />');
}
```

}

# 162 Testing

Browse to the login page and check that a Turing image appears and the One time Code can be entered to login.

llser name:	oraham	
user hame.	granam	
AD Password:		
OTC:	••••	
	Get Image	Log On
1 2 3	4 5 6 7	8 9 0
572	4968	015

For SMS or Mobile Phone Apps do not click on the Get Image button, but enter the OTC

$(\mathbf{n})$	User name:	graham	
	AD Password:	••••	
	OTC:	••••	
		Get Image	Log On

If the incorrect credentials are used then the login should fail

	User name:	
	Password 1:	
	Password 2:	
		Log On
The cr	edentials you typed are incorr esk or system administrator.	ect. Please try again or contact you

Where the TURing image is not used, then the Get Image page modification can be omitted

Please log on to o	continue.		
	User name:	graham	
	Password 1:	•••••	
	Password 2:	••••	
		Log O	n

# 163 Uninstall/Removing the integration

If the login pages have been modified restore the default login page and remove the added files.

Remove Swivel as the authentication server.

# **164 Troubleshooting**

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

The CAGEE Netscaler checks each password/OTC in turn, so if the AD password is checked first and is incorrect then the secondary authentication will not be tested.

### 164.1 Error Messages

#### Files moved but have a ? appended to the end

If the script to move the files on login contains the control code ^M at the end of each line (usually introduced by Windows based text editors), then the files may appear with a ? at the end of the filename. Use vi to remove the ^M

#### Username field length incorrect

If the username field is too short it can be increased. Edit the index.html file and locate the below section setting the size="40"

<span id="User_name" class="CTXMSAM_LogonFont"></span> style="padding-right:8px;"><input id="Enter user name" class="CTXMSAM_ContentFont" style="font-size: 8pt" type="text" title="" name="login" size="40" maxlength="127" onFocus="loginFieldCheck()" style="width:100%;" />

#### login command failed over API. Reason: Response not of type text/xml: text:html

This error can be seen on the Netscaler Administration console when upgrading with a custom theme. This will preventy login to the Netscaler Administration, although the user login pages should continue to work. To enable login to the Administration console, login to the Netscaler through the command line, backup and then and edit the /nsconfig/ns.config file and set the CUSTOM page to DEFAULT.

Look for the line containing -UITHEME CUSTOM and change it to DEFAULT as below:

set vpn parameter -localLanAccess ON -defaultAuthorizationAction ALLOW -proxy BROWSER -clientCleanupPrompt OFF -forceCleanup none -clientOp

#### After making the changes, reboot the system to login.

# **165 Known Issues and Limitations**

The CAGEE caches the javascript so when you make modifications on the CAGEE they are not reflected on the log-in page as rendered. A way round this is to change the name of the .js file and edit the index.html file to use this new .js file. see [1]

# **166 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

167 Citrix Netscaler Gateway 11

## **168 Introduction**



Netscaler PINpad

This document shows the steps required to integrate Swivel with the Citrix NetScaler 11.0. Swivel can provide Two Factor authentication with SMS, Token, and Mobile Phone Client and strong Single Channel Authentication with TURing or Pinpad, or in the Taskbar using RADIUS.

It covers the following steps.

- Configuring Swivel to accept authentication requests from the CAGEE
  Modifying the CAGEE login pages
  Configuring the CAGEE to authenticate via PINsafe

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 Network Address Translation, often with a proxy server. The Swivel virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection. The Netscaler can be configured using its load balancing bridging feature to allow a Swivel Severs IP to provide Single Channel images, such as TURing and PINpad.

There is an alternative solution using Rewrite/Responder policies, which is recommended in preference to the solution outlined below. It is described in the Netscaler 12 article, but it applies to version 11 as well. Please check Citrix Netscaler Gateway 12.

# **169 Prerequisites**

NetScaler version 11.0. The single channel customisation was created using build 62, and there may be minor cosmetic issues with other versions.

An administrative logon account for the Access Gateway

A Secure Shell (SSH) programme (eg putty) and an SSH-based file transfer application such as WinSCP

A Unicode-aware text file editor such as TextPad or WordPad

Swivel 3.x

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, this is usually implemented by a NAT to the Swivel server. Ensure that only the required ports are allowed access.

Netscaler pages to modify and/or Swivel files for version 11.0 default theme.

Netscaler pages to modify and/or Swivel files for version 11.0 Green Bubble theme.

If you would prefer to deploy ready-made themes, see the following:

- Default theme TURing image
  Default theme PINpad
  Green Bubble theme TURing image
  Green Bubble theme PINpad

See below for details on deploying these themes.

### 169.1 Note on upgrading the Netscaler

When upgrading see the note below if custom pages are used upgrading Netscalers with Custom Pages

# 170 Baseline

Tested with Swivel 3.10.4 Citrix Netscaler Gateway NS11.0 Build 62.0

# **171 Architecture**

The Citrix NetScaler makes authentication requests against the Swivel server by RADIUS.

You can create different logon realms / pages called Virtual Servers, these can have different authentication servers/policies, SSL certificates and resources attached to them. However, the downside is they ALL use the same index.html/login.js/en.xml files, so you cannot have multiple landing pages with/without the Swivel modifications.

# **172 Swivel Configuration**

## 172.1 Configuring the RADIUS server

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

## 172.2 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.

## 172.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

# **173 Citrix Netscaler Gateway Configuration**

The Swivel integration uses RADIUS authentication, and where the login page is modified it uses the Netscaler custom web pages which are configured and then copied into an archive file which is deployed at boot time.

## 173.1 Citrix NetScaler RADIUS Configuration

The NetScaler needs to be configured to use the Swivel server as a RADIUS authentication server. Where several Swivel virtual or hardware appliances are used for resilience, configure the RADIUS request to be made against each of the Swivel servers together with the use of Session Sharing. Note: for virtual or hardware appliances, the Swivel VIP should NOT be used as the RADIUS server IP address, see VIP on PINsafe Appliances

Swivel can be configured as the only authentication server or as an additional authentication server, usually this would be together with AD. The required steps are pretty much the same for both scenarios.

Under System->Authentication->RADIUS, select the Servers Tab, click "Add" and enter the following information:

Name Swivel RADIUS

Server Name The name or IP address of the Swivel server

Port 1812

Secret Key The secret key configured on the Swivel NAS and also under Confirm Secret Key

Group Prefix CTXSUserGroups=

Group Separator ;

When complete click on Create.

If the Authentication option is not available check that the license allows authentication to be configured on the Netscaler licensing page.

Pátřa 🗖 🗖 🔊	<u> </u>
Strix NetScaler VPX - Con ×	(1) เริ่มสุข รองมางวิทยายของพิทธิสารีที่ชี (1) เริ่มสุข รองมางวิทยายของพิทธิสารีที่ชี
← → C 🕺 🗟 bttp5://192.168.12.100/menu/neo#noAnch 🏠 🕚 💭 🚍	Alter (Soldan (Soldar))
🔡 Apps 🕌 Google 😭 Cinemas 🗍 Financial 🗍 G & S 🗍 Games 🗎 Home 🔹 »	international and the second statement
NetScaler VPX (10)	
Deshboerd Configuration Reporting	
4 Back	
Create Authentication RADIUS Server	and a material second statement of the second statement
Name*	
Swivel RADIUS	
Server Name Server IP	
Server Name*	T BETTER DE SAN KANDANS MANANANA MANANA
192.168.12.111	
Port*	
1812	
Time-out (seconds) 3	
Secret Key*	
000000	Carry Constant
Confirm Secret Key*	
200000	
> More	Car ala in the shirt with
Create	
4	

rix NetScaler VPX - Con ×	)/menu/neo#noAnchor	an O Java Siter O A	Aurir C One and One C Reference	
NetScaler VPX (10)			HA Status Not Configured	In N
Dashboard Configuration	Reporting			Do
- System	NetScaler > System > A	Authentication > RADIU	S > Servers	
- Licenses - Settings - Diagnostics - High Availability	Policies Servers Add Edit	Delete		
NTP Servers	Name	Server Name	IP Address	
Reports	Swivel RADIUS		192.168.12.111	
Profiles				
+ Partition Administration				
+ User Administration				
- Authentication				
Local				
RADIUS				
LDAP				
TACACS				
+ Auditing				
+ SNMP				
+ AppFlow				
+ Cluster				
+ Network				
+ Web Interface				
+ WebFront				

Now select the Policies Tab, click "Add" and enter the following information:

Name Swivel RADIUS Policy Server Swivel RADIUS Expression select "ns_true" under Saved Policy Expressions

Citrix NetScaler VP	X - Con ×	A (2) 1981.	Contraction of the local division of the loc	Contraction of the local division of the loc	Contractions	Contraction of the local division of the loc	i in a
- → C fi [	* https://192.168.12	2.100/menu	/neo#noA	nchor			
Apps 🙁 Google	🗀 Cinemas 📋 Financi	ial 🗀 G & S	🗀 Games	🗀 Home	📋 Java Sites	🗀 Music	C One a
💦 NetScal	er VPX (10)					HA Sta	^{tus} t Configur
Dashboard	Configuration	Reporting	1				
4 n							
Back							
Configure Autho	entication RADIUS Po	olicy					
Name							
Swivel							
Server*							
Swivel RADIUS	• +	1					
Expression*							
Operators -	Saved Policy Expression	ns 👻 Fre	quently Used	Expressions	•		
ns_true							
OK Close							
OK Close							
OK Close							
OK Close							

The authentication must be then added such as the Access Gateway/Virtual Servers menu. If just Swivel authentication is required then ensure that only the Swivel policy is active for the Primary. If you require AD and Swivel authentication then you need to make active the Swivel policy as the secondary. Save the settings.

🕄 Google  🗎 Cine	mas 📋 Financial 📋 G & S 🦳 Gz	ames 🗀 Home 🗀 Java Sites 🗀 Music 🗀 (	One and One 📋 Reference
+ Back			
PN Virtual Sen	ver		
Basic Settings			
Name IPAddress Port	Demo 10.40.242.185 443	Maximum Users Max Login Attempts Failed Login Timeout	0
State RDP Server Profile Login Once	⊜ Up - false	ICA Only Enable Authentication Windows EPA Plugin Upgrade	true true
Double Hop Down State Flush DTLS	false true false	Linux EPA Plugin Upgrade Mac EPA Plugin Upgrade ICA Proxy Session Migration	false
AppFlow Logging	Taise	Enable Device Certificate	Talse
Certificates			
1 Server Certificat	e		
No CA Certificate			
Authentication			
Primary Authenticat	tion		
1 LDAP Policy			
Secondary Authenti	ication		
1 RADIUS Policy			
Profiles			

# 173.2 Citrix Receiver with Netscaler configuration

See Citrix Netscaler configuration for Receiver

# **174 Additional Configuration Options**

## 174.1 Netscaler RADIUS Monitor and RADIUS Load Balancer

See Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer

## 174.2 Netscaler SSL Bridge

The Netscaler allows a SSL Bridge to be created that allows a Network Address Translation to allow access to the Swivel instance to provide single channel images or Mobile App security strings. On the Netscaler Gateway Administration Console Configuration tab select Traffic Management -> Load Balancing -> Virtual Servers, then click on Add, to open a Create Virtual Server (Load Balancing) window.

Name Name of the SSL Bridge

Protocol select SSL_Bridge

Select IP Adress Based

IP address Enter the public IP Address

Port Enter the internet-facing port number, usually 443

Security NetScaler VPX - Con 🗙			mXm	, interaction of the second
C ↑ C ↑ C http://192.168.1	2.100/menu/neo#noAnchor	\$ 0 S		
Apps [ Google 🗊 Cinemas 🗊 Finar	cial (]]] G & S (]]] Games []]] Home ([	] Java Sites (j]] Music	29	Merchand Straining Training Training
NetScaler VPX (10)		HA Status 💭 Not Coofigured	Drifo MSI:	ing tay magnetic to a gran detailer of
Destation Configuration	Reporting		Docur	
+ Back				
Load Balancing Virtual Server				an ann an an an ann an an an an an an an
Basic Settings				
Internet, the virtual server by specifying a m Internet, the virtual server IP (VIP) addre (LAN) or wide area network (WAN), the You can configure multiple virtual serve client requests. Name*	ess is a public IP address, a port, and a protocol syp ess is a public IP address. If the application is a VIP is usually a private (ICANN non-routable) rs to receive client requests, thereby increasin	ccessible only from the local area net IP address. g the availability of resources to proce	vork Iss	
Swivel-SSL-Bridge	0			CARLENGER FOR
Protocol*				
SSL_BRIDGE	7			Contraction Contraction
IP Address Type*				1997
IP Address	7			
IP Address*				
10 , 40 , 242 , 188	EPv6			
Port*	_			
443	0			
▶ More				2257776-1096
OV Careal				
				an Shana kan Araba
			>	A REAL PROPERTY OF THE REAL PROPERTY OF

pps 🔀 Gooxile 🌐 Cinemas 🗍 Financial (	)]] 6 & S (]]] 6 ames ]]	]] Home (Î	]] Java Sites 🏼 🎒 M	usic 📋 One and	One III	Reference	] Shopping (11)
👫 NetScaler VPX (10)				Land		HA Status • Not Configu	Info Info NS11.0 67
Dashboard Configuration	Reporting						Documenta
+ System	NetScaler > Traffic I	Vlanagemen	t 🗲 Load Balancin	g 〉 Virtual Serv	ers		
+ AppExpert	Add E	dit	Delete Ena	ble Disable	S	tatistics	Action 💌
Traffic Management	Name	State	Effective State	IP Address	Port	Protocol	Method
Utitual Servers	▶ Swivel-SSL-Bridge	<b>()</b> Up	<b>⊕</b> Up	10.40.242.188	8443	SSL_BRIDGE	LEASTCONNECT
Services	▶ 192.168.12.102_80	() Down	() Down	192.168.12.102	80	HTTP	LEASTCONNECT
Service Groups	▶ 78.40.242.185_80	() Down	Down	78.40.242.185	80	HTTP	LEASTCONNECT
Monitors	▶ 192.168.12.114_80	() Down	() Down	192.168.12.114	80	HTTP	LEASTCONNECT
Metric Tables	Swivel LB RADIUS	() Up	() Up	192.168.12.115	1812	RADIUS	ROUNDROBIN
Servers	4						
Persistency Groups							
+ Content Switching							
+ DNS							

After creating the virtual server, select it and then Edit

1 NetScelo	ar VPX (10)		HA Status 💭 Not Configure	Enifo d NS3	1.0 62.30.nc
Dashboard	Configuration Reportin	ß		Doca	mentation Do
+ Back					
Load Baland	ting Virtual Server   Export as a T	emplate			
Basic Setting	js			1	Help
Name Protocol State IP Address Port	Swivel-SSL-Bridge SSL_BRIDGE O Up 10.40.242.188 8443	Listen Priority Listen Policy Expression Range Redirection Mode BHI State	NONE 1 IP PASSIVE		Advanced Settings
Traffic Domain	0	AppFlow Logging	ENABLED		• e Method
Services and	Service Groups				🕂 Protection
1 Load Balanc	ing Virtual Server Service Binding			>	• Profiles
No Load Balar	ncing Virtual Server ServiceGroup Bin	ding		>	· Traffic Settings
Persistence			1	X	
Persistence \$	SLSESSION	Time-out (mins) 2			
Done					

### Select "Load Balancing Virtual Server Service Binding"

Citrix NetScaler VP	X - Con X	12.100/manu/aa	attaoAnchor					[ <u>8</u> 357]
Apps 🛐 Google	S steeps://192.108	ncial (]]] G&S (]]]	Games 🛄 Home (	🔟 Java Sites	🝈 Music 🌐 (	One and One	Reference	ン : []] Shopping (]]]:
NetScale	er VPX (10)				HA Status Not Con	Ir figured N	ro \$11.0 62.10.nd	▼ Logout
Dashboard	Configuration	Reporting				Do	cumentation	Downloads
- Bres		Load Balancing \	firtual Server Service I	Binding				
Load Balanc		Load Balancing	g Virtual Server Ser Edit Binding Unt	vice Bindin	ng it Service Bour	nd Monitors		
		Service Name	19216812111	Port R443	Protocol SSL BRIDGE	State	Weight	Persistence Cookie
Mania Protocol State IP Address Port Traffic Complex	Swieless Ender SSI, 88/068 (p.U) 10/40,252,188 (2143) (0	Close	132-100-12-111	C++4	33E_DRIDGE	<b>0</b> 0p	1	-1494-

Now click "Add Binding", then under "Select Service", click "+"

→ C 🖞 (	k https://192.168.	12.100/menu/neo#noAnchor			5
pps 📳 Google	🗐 Cinemas 🎒 Fina	ncial 🗍 G & S 🗍 Games 📋 Home 🎒 Java Sites 🎒	Music 📋 One and )	One 🛄 Reference 🛄	Shopping (
l NetScal	er VPX (10)		HA Status Not Configured	Info NS11.0 62.10.nc 🔻	Logout
Dashboard	Configuration	Reporting		Documentation	Downloads
		Load Balancing Viriual Server Service Finding $>$ Service Bi	nding 👌 Load Balar	nding Service	
		Load Balancing Service			
		Basic Settings		Help	
		Service Name*			
	Swive)-SSL/Bridge	Swivel_8443			
		New Server Existing Server			
		Samar*			
		192.168.12.111 (192.168.12.111) 7			
		Protocol*			
		SSL_BRIDGE 7			
		Port*			
	ing Vitrol Strivessor	443			
		h Mara			
		/ More			
		Cancel			

### Service Name Name of the SSL Bridge

Select "New Server" and enter the IP address of the Swivel server.

Protocol select SSL_Bridge from the drop down menu

port select the port used to connect to Swivel server, usually 8443 for the proxy application.

From the Monitors tab select TCP then Add it to the list of Configured so that it appears on the right hand side with the State box checked., then click on Create.

## 174.3 Login Page Customisation

This step only needs to be followed if login page customisation is required. Many of the steps described below are derived from the following articles:

This article describes creating a custom theme on NetScaler 10.x:

http://docs.citrix.com/en-us/netscaler-gateway/10-5/ng-connect-users-wrapper-con/ng-connect-users-cr-integration-con/ng-connect-custom-theme-page-tsk.html

This article describes the additional steps required for NetScaler 11:

http://discussions.citrix.com/topic/367268-netscaler-11-custom-theme/ - item #13.

Thanks to the originators of these articles.

Update: we recommend using rewrite / responder actions to customise the login page, as suggested by Stuart Carroll in the Additional Information section. We have adapted and updated his original solution, which is now available in the NetScaler 12 article. Despite the name, it will also work with NetScaler 11.

### 174.3.1 Using Existing Customisations

If you already have a customisation including Swivel TURing or PINpad, from version 10.x, it may still work with version 11. Results are mixed on this. However, the customisations described on these articles are based on the assumption that you are starting from the default or green bubble theme for version 11. They will not work if you are starting from a 10.x theme. In this case, you should start from one of the built-in themes for version 11 and customise those.

### 174.3.2 First Steps

Follow these steps whether you plan to use a pre-built theme or to customise your own theme.

Citrix recommend when upgrading a Netscaler with custom pages, the custom pages should be set back to use default pages, upgrade and then the custom pages reapplied. When upgrading it is recommended to make a backup or snapshot of the existing system.

When upgrading a Netscaler 10.1 or 10.5 with custom pages to 11.0, backup the modified pages and scripts, then set the login page back to default. Upgrade, test the Administration console, then upload the modified pages as if carrying out a new Swivel install as given below, then recreate the custom tar file as below as this will then include the updated GUI.

Similarly, we recommend that you select the Default theme initially, before starting the customisation.

Ensure that the folder for the custom theme exists:

• Log on to the NetScaler Gateway command line and enter the following commands:

shell mkdir /var/ns_gui_custom

You may get the response "File exists".

Copy the theme files for either the Default or Green Bubble theme using the following commands:

cd /var/netscaler/logon/themes cp -r Default Custom

or for the Green Bubble theme

cp -r Greenbubble Custom

If you are using one of the ready-made themes linked above, skip to the section Deploying a Ready-Made Theme. If you are customising an existing theme, continue to the next section.

### 174.3.3 Customising an Existing Theme

#### 174.3.3.1 Preparing the Custom Theme

Assuming that you have copied the appropriate theme as described in First Steps, select the Custom theme in order to ensure it is deployed. The files you need to modify will now be in /var/netscaler/logon/themes/Custom. Prepare the new custom theme as follows:

tar -cvzf /var/ns_gui_custom/customtheme.tar.gz /var/ns_gui_custom/ns_gui/*

Now use the NetScaler administration console to select the custom theme: select NetScaler Gateway -> Global Settings, then click on Change Global Settings, select the Client Experience tab, and at the bottom of the tab, switch the UI Theme to Custom.

#### 174.3.3.2 Login to Netscaler Command Line

Use WINscp to use a web file tool or SSH onto the virtual or hardware appliance using an admin account. Once onto the box you need to type shell to get access to the command line.

>Last login: Wed Sep 10 19:12:45 2008 Done > shell Last login: Wed Sep 10 21:13:35 2008

#### 174.3.3.3 Backup Netscaler files

Navigate to the location of the pages to be modified, and make a local backup copy of them.

- cd /var/ns_gui_custom/ns_gui/vpn
- cp index.html index.html.bak cd js

cp gateway_login_form_view.js gateway_login_form_view.js.bak
#### 174.3.3.4 Customise the login script

See under prerequisites for the modified files that need to be uploaded to the Netscaler.

Note on editing files: If the files are edited in Windows-based systems it may be possible that control code ^M are added to the end of the line. These can be viewed and removed by using vi.

It is assumed that your custom theme has already been deployed under /var/ns_gui_custom/ns_gui. As noted above, it is also assumed that the theme is based on one of the built-in version 11 themes. If you have a version 10 x customisation that you cannot get to work with version 11, please contact support@swivelsecure.com for further advice.

Download the customised files from the pre-requisites above. This contains 5 files, in the appropriate folders:

- /vpn/index.html a replacement for the existing file, containing additional lines to insert the swivel files below
- /vpn/js/gateway_login_form_view.js a replacement for the existing file, containing a single additional line, which calls a script from swivel.is to insert the customisation.
- /vpn/js/swivel.js a new file, containing the JavaScript to insert the customisation
- /vpn/images/swivel.css a new file, containing the stylesheet for the Swivel customisation
   /vpn/images/pinpadBlank.png an optional blank image for the PINpad buttons.

Before you copy these files across, you will need to modify the first part of swivel.js as shown here:

// Set this to be the correct URL for the required image. // Set this to be the correct own for the required image. var swivellor1 = "https://citriximage.swivelsecure.com/proxy/"; // Set this to "turing" or "pinpad". Anything else will result in no image. var swivelImageType = "pinpad"; // Set this to the ID of the password field to populate: "passwd" or "passwd1" var pinpadField = "passwd1";

- swivelUrl should contain the public URL for your image. Do not add "SCImage" or "SCPinPad" this will be done for you.
  swivelImageType should be "turing" or "pinpad" as described
  pinpadField defines which password field should be filled by the PINpad buttons. If Swivel is the primary authentication, use "passwd", or for secondary authentication use "passwd1".

#### 174.3.3.5 Customise the OTC field and TURing image button text

This is an optional step.

Modify the language resource files in /netscaler/logon/themes/Default/resources. If you are only using the English language, then edit en.xml and search

<Partition id="logon">

#### Just below this, look for

<String id="Password2">Password 2</String>

Replace "Password 2" with "OTC".

If you want to change the label on the TURing button, insert a new line just below this:

<Property id="New_Turing" property="value">New Image</Property>

Replace "New Image" with the appropriate text.

If you want to change the label on the PINpad refresh button, insert the following line:

<Property id="Refresh_Pinpad" property="value">Refresh</Property>

Replace "Refresh" with the appropriate text.

#### 174.3.3.6 Additional Languages file modifications

If you will be using languages other than English, you will also need to edit any other language files you use, following the pattern above.

174.3.3.7 Upload files to Netscaler

Download the files under the prerequisites and modify as described above, then copy them to the appropriate locations under /var/ns_gui_custom/ns_gui.

#### 174.3.3.8 Create the boot archive file

cd /var/ns_gui_custom tar -zcvf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*

This should create the customtheme.tar.gz file used at boot time, and list all the files used.

#### 174.3.3.9 Select the custom theme

• Log on to the NetScaler Administration Console and select the "Custom" theme. Save customisation changes.

## 174.3.3.10 Create Backup and Script to Deploy Files

Once you have a working configuration, you should back up the modified files to a suitable location off the NetScaler. It is recommended that the backup directory structure reflects the deployed structure - e.g. put the .js files in a js subdirectory, and the .css file(s) in a images subdirectory. This makes it easier to carry out the next step.

As NetScaler often replaces files after a reboot, you also need to take precautions to ensure the custom files are restored after a reboot. To do this, you need to copy the backups you just created into a folder on the NetScaler: the recommended location is to create a folder "custom" under /var/mods. As described above, the directory structure under custom should reflect the directory structure under vpn.

To restore these files on reboot, you need to edit the file /nsconfig/rc.netscaler. Insert the following line at the beginning of the file:

cp -r /var/mods/custom/* /var/netscaler/ns_gui/vpn/*

This assumes that your web directory is /var/netscaler/ns gui - modify accordingly.

#### 174.3.3.11 Reboot Netscaler to verify files are copied across

Reboot the Netscaler to ensure that the files are copied across at boot time and that the login page has been modified as required.

The following section can be skipped if you are customising an existing theme.

#### 174.3.4 Deploying a Ready-Made Theme

These instructions assume you are using one of the pre-built themes listed above.

- Copy the chosen theme to /var/ns_gui_custom. We recommend WinSCP to copy the files, but any suitable file transfer file will do.
  Go to /var/netscaler/logon/themes/Custom/resources and edit en.xml (again, you can use WinSCP for this):
  - Search for "Password2"
  - ♦ If required, change the text for <String id="Password2"> to "OTC":

<String id="Password2">OTC</String>

Insert a new line below this:

<String id="SwivelUrl">https://swivel.mycompany.com/proxy/</String> (Substitute the public URL for your Swivel images (TURing or Pinpad) in the above.)

Save the file.

If you need to support multiple languages, repeat this process for all supported language files.
 Log on to the NetScaler Administration Console and select the "Custom" theme.

- Save customisation changes.

If you prefer, as an alternative to inserting the Swivel URL in the resources file(s), you can manually modify swivel.js, as described below. However, if you do this, you will also need to rebuild the custom theme, again as described above.

## 174.4 Additional Login Customisation options

#### 174.4.1 Requesting the String Index

See also Multiple Security Strings How To Guide

To request the string index, use the "turing" option.

Modify swivel.js. Search for the following line:

swivelUrl += "/SCImage?username=";

Replace "SCImage" with "DCIndexImage".

#### 174.4.2 Requesting an SMS

See also Challenge and Response below

To request an SMS on demand, use the "turing" option.

Modify swivel.js. Search for the following line:

swivelUrl += "/SCImage?username=";

Replace "SCImage" with "DCMessage".

#### 174.4.3 One Touch

DISCLAIMER: the following One Touch solution is based on NetScaler 10.5, and has not yet been tested on version 11.

One touch is a different approach as the user is redirected to a separate page to authenticate and therefore does not actually see the Netscaler login page.

#### Refer to VPN_OneTouch_Integration

To customise the page for one touch you need to include the following in the header section of index.html where <swivelappliance> is the hostname of the associated Swivel Appliance

```
//-> Swivel elements function redirect(){
window.location.replace("https://<swivelappliance>:8443/onetouch/onetouch?returnurl=" + window.location.href );
var QueryString = function () {
    // This function is anonymous, is executed immediately and
    // the return value is assigned to QueryString!
 var query_string = {};
 var query = window.location.search.substring(1);
var vars = query.split("&");
```

#### Before the closing </SCRIPT> tag

#### 174.5 Challenge and Response

To use two-stage authentication - also known as challenge and response - you will need these custom files. These files are for the Green Bubble theme: for different themes, see the detailed customisation section below. Also note that these files only support TURing in the second stage: for other options, see below.

See Challenge and Response How to Guide for details on setting up challenge/response on the Swivel server. In particular, note that the option "Send username with challenge" must be set to "Yes" to use single-channel challenge-response, so if your version of the Swivel software is too old to have that option, you will need to upgrade in order to use challenge-response with TURing.

#### 174.5.1 Customisation

See above for details on where the custom files need to be put. Always take backups of the original files before making any changes. If you are using dual channel, you may not need to make any of these changes: see comments below.

You should always download the custom files linked above, even if you are not using the Green Bubble theme with TURing, as you will need the file swivel.js at least. This should be put in the js folder. The other files that need to be changed are index.html, nsshare.js and js/gateway_login_form_view.js.

The only change to index.html is to insert a single line:

```
<script type="text/javascript" src="/vpn/js/swivel.js"></script>
```

somewhere in the <head> section.

The only change required to gateway_login_form_view.js is as follows:

Locate the following line:

changePage(); // Prefill names if cert auth

#### Insert before it the following line:

customLoginPage(form);

This calls a function from swivel is to add the Swivel customisation to the first login page. This hides the Swivel password field, and copies the first password field to it before submitting the page. This assumes that you are using the "Check repository password" option. If you don't want to use that, don't make this change.

The second login page is rendered by nsshare.js, so you need to make the following changes to it, only if you want to show TURing in the second page. In the custom files, these are inserted before the DialogInclude function, but they can go anywhere in the file:

```
// Alter this URL as appropriate.
var swivelUrl = "https://citriximage.swivelsecure.com/proxy/SCImage?username=";
function showTuring(sUser) {
    if (sUser!="") {
        // Find the image field.
        var varImg = document.getElementById("imgTuring");
        // Set the image SRC and make it visible
        varImg.src = swivelUrl + sUser + "&random=" + Math.round(Math.random()*100000);
        varImg.style.display = "";
    }
}
function showTuringImageChallenge() {
    var challengeDiv = document.getElementById("dialogueStr");
    if (challengeDiv) {
        var challenge = challengeDiv.innerHTML;
        var colonPos = challenge.lastIndexOf(":");
        if (colonPos > 0) {
```

```
var username = challenge.substr(0, colonPos).trim();
challenge = challenge.substr(colonPos+1);
challengeDiv.innerHTML = challenge;
showTuring(username);
}
```

Then, in the function DialogueBodyII, look for

```
ln += '';
```

#### and insert the following line before it:

}

ln += '<img id="imgTuring" style="display:none" />';

Then, at the end of DialogueBodyII, insert the following line:

showTuringImageChallenge();

If you are unclear about any of these changes, they are clearly labelled in the custom files provided.

## 174.6 Image Request button displayed when needed

The following code allows the Single Channel Image request button to be only shown when required. This is useful for refreshing an image or when SMS/Mobile client authentication is used, since when a Single Channel image is generated, either automatically or manually, it then expects a single channel login (within 2 minutes by default).

```
function ns_showpinsafe()
{
  var pspwc = ns_getcookie("pwcount");
    if ( pspwc == 2 )
    {
      document.write('<d>');
      document.write('<img src="/vpn/images/LoginButtonRolloverGlow.gif"/>');
      document.write('input type="button" id="btnTuring" value="Get Image" ');
      document.write('input type="button" id="btnTuring" value="Get Image" ');
      document.write('onnouseover="this.className=');
      document.write(''onmouseout="this.className=');
      document.write("'CTX_CaxtonButton_Hover';");
      document.write("'CTX_CaxtonButton';");
      document.write(''
```

# 175 Testing

Browse to the login page and check that a TURing or PINpad image appears and the One time Code can be entered to login.



# 176 Uninstall/Removing the integration

If the login pages have been modified restore the default login page and remove the added files.

Remove Swivel as the authentication server.

## **177 Troubleshooting**

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

The CAGEE Netscaler checks each password/OTC in turn, so if the AD password is checked first and is incorrect then the secondary authentication will not be tested.

## 177.1 Error Messages

#### Files moved but have a ? appended to the end

If the script to move the files on login contains the control code ^M at the end of each line (usually introduced by Windows based text editors), then the files may appear with a ? at the end of the filename. Use vi to remove the ^M

#### Username field length incorrect

If the username field is too short it can be increased. Edit the index.html file and locate the below section setting the size="40"

<span id="User_name" class="CTXMSAM_LogonFont"></span> style="padding-right:8px;"><input id="Enter user name" class="CTXMSAM_ContentFont" style="font-size: 8pt" type="text" title="" name="login" size="40" maxlength="127" onFocus="loginFieldCheck()" style="width:100%;" />

#### login command failed over API. Reason: Response not of type text/xml: text:html

This error can be seen on the Netscaler Administration console when upgrading with a custom theme. This will preventy login to the Netscaler Administration, although the user login pages should continue to work. To enable login to the Administration console, login to the Netscaler through the command line, backup and then and edit the /nsconfig/ns.config file and set the CUSTOM page to DEFAULT.

Look for the line containing -UITHEME CUSTOM and change it to DEFAULT as below:

set vpn parameter -localLanAccess ON -defaultAuthorizationAction ALLOW -proxy BROWSER -clientCleanupPrompt OFF -forceCleanup none -clientOp

#### After making the changes, reboot the system to login.

# **178 Known Issues and Limitations**

The CAGEE caches the javascript so when you make modifications on the CAGEE they are not reflected on the log-in page as rendered. A way round this is to change the name of the .js file and edit the index.html file to use this new .js file. see [1]

Potential File Locations:

/netscaler/ns_gui/vpn

/var/ns_gui/vpn

/var/ns_gui_custom/vpn

/var/netscaler/gui/vpn

# **179 Additional Information**

NOTE: there is an alternative solution to this that uses the NetScaler rewrite feature, and so doesn't require you to make changes to any files. It also has the advantage that it can be applied selectively. Many thanks to Stuart Carroll for finding this approach:

http://www.stuartc.net/blog/tech/netscaler-11-0-swivel-integration-using-netscaler-rewrite/

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

180 Citrix Netscaler Gateway 12

## **181 Introduction**

This article covers how to adjust an integration between pinsafe protocol and Citrix Netscaler Gateway 12.

Swivel can provide Two Factor authentication with SMS, Token, and Mobile Phone Client and strong Single Channel Authentication with TURing or Pinpad, or in the Taskbar using RADIUS. For all the methods which do not require an image at the article Citrix_Netscaler_Gateway_11 covers them.

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 Network Address Translation, often with a proxy server. The Swivel virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection. The Netscaler can be configured using its load balancing bridging feature to allow a Swivel Severs IP to provide Single Channel images, such as TURing and PINpad. Both the authentication methods need an image for which there are a set of rules to be applied. This document covers the application of those rules through the NS command line.

## **181.1 Integration Architecture**

Swivel Secure ? Radius ? Nas ? Netscaler ? login page ? AD ? login customised page

## **182 Turing Image Integration**

This solution uses the NetScaler Rewrite and Responder features: please make sure these features are enabled before proceeding. The custom actions and policies can be added through the web administration console, but we provide them below as NetScaler shell commands.

This solution will work with NetScaler 11 as well, and is recommended in preference to the previous article.

You can customise the labels from the web console. Under NetScaler Gateway, select Portal Themes, then the theme you are using, and Edit. On the right, click Logon Page, and the text can be edited there.

There is need to have a valid certificate for the turing image to appear. As a trial you can try a self signed certificate that is trusted by the host: cd /usr/local/share/ca-certificates/swivel.crt

It has been reported that the rewrite and responder actions used for version 11 do not work with the latest release of version 12. Below is an updated set of actions & policies that need to be installed. Before you install them, edit the responder action and change the URL following pinsafeUrl to the correct URL for your TURing. You don't need the "SCImage" part - that will be added automatically.

To install the rules, you need to open a command prompt on the NetScaler. You can just paste the entire file contents to the shell window. Once you have installed them, they have to be bound to a virtual server. There isn?t a script for that as it will be different for each installation. It's easiest to do this right at the netscaler?s web admin console.

#### **182.1 Rewrite Rules**

Copy the lines from the text below to a text editor: note that each action should be on a single line. Edit the URL as described above, then copy and paste the result into your NetScaler?s command line. Be sure to have complete lines without additional spaces or line breaks.

# The action Act_Sentry_Username_Blur and the associated policy is optional, and shows the TURing image as soon as you tab away from the username. If you prefer users to click a button to get the image, then do not include this action/policy.

add rewrite action Act_pinsafe.js insert_before_all "HTTP.RES.BODY(12000)" q{"<script type=\"text/javascript\" src=\"/vpn/pinsafe.js\"></scri add rewrite action Act_Sentry_Mod insert_after_all "HTTP.RES.BODY(1000000)" q| "\n\tvar pinsafe_button=\$('<div></div>').addClass('field').add add rewrite action Act_Sentry_AppendEULA replace_all "HTTP.RES.BODY(1000000)" "\"form.append(eula_section,field_login,pinsafe_button,pinsafe_ add rewrite action Act_Sentry_Append replace_all "HTTP.RES.BODY(1000000)" "\"form.append(field_login,pinsafe_button,pinsafe_image)\"" -search add rewrite action Act_Sentry_Username_Blur replace_all "HTTP.RES.BODY(1000000)" q|".focus(function(){loginFieldCheck();}).blur(function(){sho add rewrite policy Pol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/index.html\")" Act_pinsafe.js add rewrite policy Pol_Sentry_Mod "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Mod add rewrite policy Pol_Sentry_AppendeULA "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Append add rewrite policy Pol_Sentry_AppendEULA "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Append add rewrite policy Pol_Sentry_AppendEULA "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Append add rewrite policy Pol_Sentry_AppendEULA "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendEULA add rewrite policy Pol_Sentry_Username_Blur "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendEULA add rewrite policy Pol_Sentry_Username_Blur "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendEULA add responder action ResAct_pinsafe.js respondwith "\"HTTP/1.1 200 OK\r\n\r\n\r\"+\"var pinsafeUrl = \\\"https://sentry.swiveldev.com:8443/prox add responder policy ResPol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/pinsafe.js\")" ResAct_pinsafe.js

#### 182.1.1 Binding the applied rules

This is done at the netscaler GUI.

Select the virtual server you are going to use, and edit it. Scroll down to the Policies section and click "+". Select Responder policy, then click Continue. Click "Add Binding" and select the policy "ResPol_pinsafe.js". Click Bind. Click Close, then click + again. This time, select "Rewrite" as the policy, and "Response" as the type. Click "Add Binding" and then select the rewrite policies just added, one at a time. After each one, make sure the GOTO expression is "NEXT", to ensure that all policies are executed. This doesn?t apply to the responder policy. In the end there should be 5 rewrite policies in total (4 if you don't want automatic TURing), and one responder policy. It doesn't matter which order you add them.

The last thing you will need to do is to persuade NetScaler not to use the cached version of its JavaScript. Go back to the command prompt, and open a shell. The following have been tested successfully for Netscaler?s web files, and we recommend trying both to ensure the result:

cd /netscaler/ns_gui/vpn/js

cd /var/netscaler/gui/vpn/js

After getting to those locations apply touch as Netscaler seems to cache JavaScript files.

touch gateway_login_form_view.js

You should now get the TURing image embedded into the login page.

## 182.2 Green Bubble Theme

#### Use the following rules for the Green Bubble theme.

add rewrite action Act_pinsafe.js insert_before_all "HTTP.RES.BODY(12000)" q{"<script type=\"text/javascript\" src=\"/vpn/pinsafe.js\"></scri add rewrite action Act_Sentry_ModGB insert_after_all "HTTP.RES.BODY(1000000)" q| "\n\tvar pinsafe_image=\$(\"<div></div>\").attr({'id':'divTur add rewrite action Act_Sentry_AppendEULAGB replace_all "HTTP.RES.BODY(1000000)" "\"form.append(eula_section,field_login,pinsafe_image)\"" -se add rewrite action Act_Sentry_AppendGB replace_all "HTTP.RES.BODY(1000000)" "\"form.append(field_login,pinsafe_image)\"" -se add rewrite action Act_Sentry_AppendGB replace_all "HTTP.RES.BODY(1000000)" "\"form.append(field_login,pinsafe_image)\"" -se add rewrite action Act_Sentry_Username_Blur replace_all "HTTP.RES.BODY(1000000)" "\"form.append(field_login,pinsafe_image)\"" -search "text(\"form add rewrite action Act_Sentry_Username_Blur replace_all "HTTP.RES.BODY(100000)" q|".focus(function(){loginFieldCheck();}).blur(function(){sho add rewrite policy Pol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/index.html\")" Act_pinsafe.js add rewrite policy Pol_Sentry_Mod "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_ModGB add rewrite policy Pol_Sentry_Append "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendGB add rewrite policy Pol_Sentry_AppendEULA "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendEULAGB add rewrite policy Pol_Sentry_Username_Blur "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendEULAGB add rewrite policy Pol_Sentry_Username_Blur "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Username_Blur add responder action ResAct_pinsafe.js respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"var pinsafeUrl = \\\"https://sentry.swiveldev.com:8443/prox add responder policy ResPol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/pinsafe.js\")" ResAct_pinsafe.js

The action names have been changed, so that you can have actions for multiple themes in the configuration and simply change the policies to point to the appropriate actions.

## 182.3 RfWebUI theme

Unfortunately, the RfWebUI theme doesn't support responder actions. Instead, you have to replace the file script.js with the one below, or if it is already modified, add the attached scripts to the existing file.

The file can be found under /var/netscaler/logon/themes/RFWebUI/. If you have copied the original RFWebUI theme, the last part of the path will be whatever the new theme is named as.

As with other customisations, you will need to modify the first line to set swivelUrl to the correct public URL for your system.

#### Customised script.js

## 182.4 X1

#### Here are the actions and policies for the X1 theme. Only one action needs to be changed here.

add rewrite action Act_pinsafe.js insert_before_all "HTTP.RES.BODY(12000)" q{"<script type=\"text/javascript\" src=\"/vpn/pinsafe.js\"></scri add rewrite action Act_Sentry_ModX1 insert_after_all "HTTP.RES.BODY(1000000)" q| "\n\tvar pinsafe_button=\$(\"<div></div>\").addClass('field') add rewrite action Act_Sentry_AppendEULA replace_all "HTTP.RES.BODY(1000000)" "\"form.append(eula_section,field_login,pinsafe_button,pinsafe_ add rewrite action Act_Sentry_Append replace_all "HTTP.RES.BODY(1000000)" "\"form.append(field_login,pinsafe_button,pinsafe_image)\"" -search add rewrite action Act_Sentry_Append replace_all "HTTP.RES.BODY(1000000)" q|".focus(function(){loginFieldCheck();}).blur(function(){sho add rewrite action Act_Sentry_Username_Blur replace_all "HTTP.RES.BODY(1000000)" q|".focus(function(){loginFieldCheck();}).blur(function(){sho add rewrite policy Pol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/index.html\")" Act_pinsafe.js add rewrite policy Pol_Sentry_Mod "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_ModX1

add rewrite policy Pol_Sentry_Append "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Append

add rewrite policy Pol_Sentry_AppendEULA "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendEULA

add rewrite policy Pol_Sentry_Username_Blur "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Username_Blur

add responder action ResAct_pinsafe.js respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"var pinsafeUrl = \\\"https://sentry.swiveldev.com:8443/prox add responder policy ResPol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/pinsafe.js\")" ResAct_pinsafe.js

## **183 Pinpad Integration**

The following document provides the rules which need to be applied for Pinpad integration. Before applying the responder action you'll need to edit the url for the swivel server to match yours: swivel.mycompany.com:8443/proxy/SCPinPad.

Be sure you have 2 rewrite actions (one of which is big), 2 rewrite policies, 2 responder actions and 2 responder policies. Avoid adding extra spaces when copying the rules onto the netscaler's shell.

add rewrite action ReAct_pinpad_js insert_before_all "HTTP.RES.BODY(12000)" q{"\r\n<script type=\"text/javascript\" src=\"/vpn/pinpad.js\"></ add rewrite action ReAct_Insert_Pinpad replace_all "HTTP.RES.BODY(1000000)" q|"form.append(field_errormsg);\r\n\tvar refresh_button=\$(\"<inpu

add rewrite policy RePol_pinpad_js "HTTP.REQ.URL.EQ(\"/vpn/index.html\")" ReAct_pinpad_js

add rewrite policy RePol_Insert_Pinpad "HTTP.REQ.URL.EQ(\"/vpn/js/gateway_login_form_view.js\")" ReAct_Insert_Pinpad

add responder action ResAct_pinpad.js respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"var pinpadUrl=\\\"https://swivel.mycompany.com:8443/proxy/SC

add responder action ResAct_pinpad.css respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"div.pinpadHidden { display : none; }\r\n\"+\"div.pinpadVisi

add responder policy ResPol_pinpad.js "HTTP.REQ.URL.EQ(\"/vpn/pinpad.js\")" ResAct_pinpad.js  $\$ 

add responder policy ResPol_pinpad.css "HTTP.REQ.URL.EQ(\"/vpn/pinpad.css\")" ResAct_pinpad.css

# **184 Delete previous rules**

The optimal option is to unbound all the rules through the NS GUI and after delete them. Also bear in mind the need to touch the .js files mentioned throughout the article as NS caches the previous versions - so changes might not be visible or immediately available.

# 185 Adjust Buttons at the login page

For further adjustments of the login page read the following section. Bear in mind X1 theme allows a quick editing of some features so the following might not apply. Normally the login page can be slightly edited, we are not going onto details regarding aesthetics and branding but only renaming of some sections which report to this integration.

## 185.1 Edit Password to OTC

The example below describes the use of the english language at the login interface.

> shell root@VLABSRV0# cd /var/netscaler/logon/themes/Default/resources root@VLABSRV0# chmod +w en.xml root@VLABSRV0# vi en.xml

[change word directly ? beginning of the word - cw ? write ? escape - :wq!]

ng> <String id="User_name">User name</String> <Property id="Enter user name" property="title">Enter user name</Property> <String id="Password">OTC</String> <String id="Password2">Password2">Password2</String> <String id="Enter password">Enter password>String > Property id="Log_On" property="value">Log On</Property> <String id="You need to enter login name">You need to enter login name</String> <String id="You need to enter passwd">You need to enter a password</String> * <String id="Enter_password2_Alert">You need to enter login name</String> <String id="You </String> <String id="domain">Domain</String> <String id="eula_title">End User License Agreement</String> <String id="eula_agreement">I accept the </String> <String id="terms">Terms&nbsp;&&nbsp;Conditions</String> <String id="erorMessageLabelBase">erorMessageLabelA001">String> <String id="erorMessageLabelA001">String> <String id="erorMessageLabelA002">You do not have permission to log on at t his time.</String> <String id="erorMessageLabel4003">Cannot connect to server. Try connecting en.xml: 597 lines, 51853 characters. root@VLABSRV015# exit shell

• You can also change ?You need to enter a password? to ?You need to enter an OTC?. We recommend avoiding obvious naming, mainly as a security measure.

# **186 Troubleshooting**

If the logging in is not working please check the certificate and if the netscaler as the same valid certificate. Also if there as been made any change to the ip?s check if there is a firewall blocking the content.

It has been reported that sometimes the JavaScript file gets cached. To resolved this you should touch gateway_login_form_view.js and try to log after. NetScaler tends to cache JavaScript files, and doesn't detect changes made by rewrite rules. You have to force it to refresh its cache.

If the pinsafe.js file is coming through OK it means that some of the rules are working.

For further assistance please write to supportdesk@swivelsecure.com

# 187 Netscaler Upgrade from 11 to 12

As recommended by CITRIX, for previous versions the upgrade should be made gradually, eg from NS 11.0 to NS 11.1 prior to get to NS 12. The upgrade should be easily done through the NS GUI but if you bump into trouble the CLI upgrade version is also easy.

Download the build file from Citrix page, Netscaler Gateway 12, upload it to /flash through Filezilla/WinSCP. Example below:

soc@support ~ \$ ssh nsroot@10.10.10.21 > save config > shell root@VLABSRV0# cd /nsconfig root@VLABSRV0# cp ns.conf ns.conf11.ns root@VLABSRV0# cd /var/nsinstall

root@VLABSRV0# mkdir nsinstall12 root@VLABSRV0# cd nsinstall12 root@VLABSRV0# mv /flash/build-12.0-53.13_nc_32.tgz . root@VLABSRV0# tar -xvzf build-12.0-53.13_nc_32.tgz (...) root@VLABSRV0# ./installns installns: [36026]: VERSION ns-12.0-53.13.gz (...) installns: [36026]: installns version (12.0-53.13) kernel (ns-12.0-53.13.gz)

The Netscaler version 12.0-53.13 checksum file is located on http://www.mycitrix.com under Support > Downloads > Citrix NetScaler. Select the Release 12.0-53.13 link and expand the "Show Documentation" link to view the SHA2 checksum file for build 12.0-53.13.

There may be a pause of up to 3 minutes while data is written to the flash. Do not interrupt the installation process once it has begun.

Installation will proceed in 5 seconds, CTRL-C to abort Installation is starting ... installns: [36026]: Installation is starting ... installns: [36026]: Installation is starting ... installation >= NS6.0 installans: [36026]: Installation path for kernel is /flash (...) installns: [36026]: Installing Linux EPA and Linux EPA version file... (...) Installation has completed. Reboot NOW? [Y/N] Y Rebooting ? installans: [36026]: Rebooting ...

# 188 nFactor ? Customizing UI to Display Images

Please also check the following article at the Citrix website: https://support.citrix.com/article/CTX225938

# **189 Backup Configuration**

We'd also recommend backing up the configuration in case after a reboot the configuration gets messed up: https://ogris.de/howtos/netscaler-restore.html

# 190 Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer

# **191 Introduction**

Citrix 10.5 allows the RADIUS to be monitored and load balanced in a number of ways. Earlier versions such as 10.1 also have this capability but have different configuration screens.

Where Swivel Single Channel Sessions (TURing, Pinpad), and SMS by On Demand Authentication and Mobile Provision Codes, it is expected that Appliance Synchronisation will also be used.

# **192 Prerequisites**

Swivel HA solution

Netscaler 10.x

# 193 Baseline

Swivel 3.10.3 Netscaler 10.5

## **194 Swivel Configuration**

The Swivel servers should be setup as indicated in the integration guide.

Configure a RADIUS NAS entry for the Netscaler SNIP interface, see RADIUS Configuration

Optionally set Authenticate non-user with just password: to Yes and configure a non Swivel user with a static password, see RADIUS Static Password.

# **195 Netscaler Configuration**

The Netscaler Configuration should be setup and tested to be working before attempting these steps.

## 195.1 Create a Swivel Radius Monitor

On the Netscaler Administration console Configuration Tab select Traffic management/Load Balancing/Monitors, then Add

Expand the Special Parameters and add Response Codes to 3 for Access Reject and add 2 for Access Accept

Set Username to an appropriate test user

Set Password to the required value if Authenticate non-user with just password if authenticate non Swivel user is used (or random if not)

Set RADIUS Key to the value for the Swivel RADIUS NAS

Leave other settings as default

Click Create to create the Monitor

Create Monitor	Configure Monitor
Norma*	Name
Swivel RADIUS Monitor	Swivel RADIUS Monitor
Type*	Туре
RADIUS	RADIUS
Standard Parameters Special Parameters	Standard Parameters Special Parameters
Response Codes	Response Codes
+ 3 <b>×</b>	2-3 ×
User Name*	User Name*
Password*	Password*
•••••	•••••
RADIUS Key*	RADIUS Key*
•••••	••••••
NAS ID	NASID
NAS IP	NAS IP 0.0.0.0
Create	OK Close

The Monitor should appear in the list.

Dashboard Configuration	Reporting
+ System	NetScaler > Traffic Management > Load Balancing > Monitors
+ AppExpert	Add Edit Delete Action -
<ul> <li>Traffic Management</li> </ul>	
<ul> <li>Load Balancing</li> <li>Virtual Servers</li> <li>Services</li> <li>Service Groups</li> </ul>	Swivel RADIUS Monitor     ping-default     tcp-default
Monitors	▶ arp
Metric Tables Servers Persistency Groups + Content Switching + DNS + SSL Optimization + Security + NetScaler Gateway Show Unlicensed Features	<pre>&gt; nd6 &gt; ping &gt; tcp &gt; tcp &gt; http &gt; tcp-ecv &gt; http-ecv &gt; udp-ecv &gt; dns &gt; ftp &gt; tcps</pre>
Integrate with Citrix Products	<ul> <li>https</li> <li>tcps-ecv</li> </ul>
XenApp and XenDesktop	<ul> <li>https-ecv</li> <li>Idns-ping</li> </ul>
	↓ Idns-tcp
	▶ Idns-dns
	▶ xdm
	▶ xnc

## 195.2 Create Entries for the Swivel RADIUS Servers

On the Netscaler Administration console Configutration Tab select Traffic management/Load Balancing/**Servers**, then Add. Enter the details for each of the Swivel RADIUS servers. If the Swivel servers are already configured, then this step can be skipped over.

Enter Server Name' and IP Address/Hostname

Server Name*	
Swivel Primary	
IP Address O Domain Name	
IPAddress*	
192 . 168 . 12 . 116	IPv6
Traffic Domain	+ / 0
<ul> <li>Enable after Creating</li> <li>Comments</li> </ul>	I

Server Name*						
Swivel St	andby				]	
IP Add	dress 🔘 [	)omain	Nam	ie		
[PAddress	*					
192 .	168 .	12		117		IPv6 🕜
Fraffic Dor	main			•	+	/
Enable Comment	e after Crea s	ting			-	

Click Create to create the Server



N	etScaler >	Traffic Man	Load Balancing > Servers		
	Add	Edit	Delete	Action	
Na	me			State	
	Swivel Stand	lby		igeneration Enabled	
	Swivel Prima	ary		Enabled	
•	192.168.12.1	11		Enabled	

Enabled

## 195.3 Create a Swivel Load Balance Service Group

On the Netscaler Administration console Configutration Tab select Traffic management/Load Balancing/Service Group, then Add.

Enter the Name, Protocol RADIUS, then click OK, and

Basic Settings	
Name*	
Swivel LB Service Group	
Protocol*	
RADIUS	
Traffic Domain	2
Cache Type*	
SERVER 🔽 🕐	
AutoScale Mode	
Cacheable State	
<ul> <li>Health Monitoring</li> <li>AppFlow Logging</li> </ul>	
Number of Active Connections	
Comments	
	0

Click below the Service Group members to add members to the group, select the Server Based radio button to add in the Swivel RADIUS servers and enter Port 1812. Repeat for each Swivel server to be added.

Service Group Member	
	Service Group Member
🔘 IP Based 🔘 Server Based	
Server Name*	IP Based Server Based
Swivel Primary	Server Name*
Port*	Swivel Standby
1812	Port*
Weight	1812
1	Weight
Server Id	1
	Server Id
Hash Id	
	Hash Id
✓ State	
	✓ State
Create Close	
	Create Close

## 195.3.1 Add the Monitor to the Load Balance Server Group

From the Right Handside select Monitor so it appears at the bottom then click it again to add the Swivel RADIUS Monitor.

	ServiceGroup Binding 🚿 Load Balancing Service Group 🚿 Load Balancing Monitor Binding
	Load Balancing Monitor Binding
	Select Monitor*
	Swivel RADIUS Monitor > +
	Binding Details
	Weight
	State Passive
	Bind Close
-	

## 195.4 Create A Virtual Server

On the Netscaler Administration console Configutration Tab select Traffic management/Load Balancing/Virtual Servers, then Add. Enter a Name for the Virtual Server IP Address, Protocol and Port.

Basi	c Set	tings						
Name	*							
Swiv	el LB	Virtua	al Se	rver				
Proto	col*							
RAE	DIUS						•	
IP Ad	dress	Type*					0	
IP A	ddre	ss					-	
IP Ad	dress*	ė.						
192		168		12		115	; [	] IP
Port*								
1812	2						6	)
▶ Me	ore							
	ОК			Can	cel			

Click OK to create the entry

### 195.4.1 Add the Service Group to the Virtual Server

After configuring the Virtual Server, the Service section will appear, click on OK to bring up the Service Group on the right hand side.

# Load Balancing Virtual Server

## **Basic Settings**

Name	Swivel LB RADIUS	Listen Priority	250
Protocol	RADIUS	Listen Policy Expression	-
State	DOWN	Range	1
IP Address	192.168.12.115	Redirection Mode	IP
Port	1812	RHI State	PAS
Traffic Domain	0	AppFlow Logging	ENA

## Service

No Load Balancing Virtual Server Service Binding

#### **Traffic Settings** Health Threshold 0 Priority Queuing OFF Client Idle Time-out 120 Sure Connect OFF Minimum Autoscale Members Down State Flush ENABLED 0 Maximum Autoscale Members 0 ICMP Virtual Server Response PASSIVE

# Service Group No Load Balancing Virtual Server ServiceGroup Binding Done

Click on the Service Group, it will appear at the bottom allowing it to be seleceted, and then click on **Select Service Group Name** to choose the required service group created earlier.

Add	Edit	Delete	Manage Member	s Statistics	Action	-		
Service (	Group Name	2	State	Effective State	Protocol	Max Clients	Max Requests	N
Swivel	LB Service G	Group	ENABLED	OUP	RADIUS	0	0	

Then click Bind

## 195.4.2 Add the Method to the Virtual Server

Select Method and then from the Load Balancing Method drop down select ROUNDROBIN then click on OK.

Load Balancing Method*	
ROUNDROBIN	• 0
New Service Startup Reque	st Rate
New Service Request unit*	
PER_SECOND	•
Increment Interval	

Click Done and the Virtual server should be created.
NetScaler	> Traffic Man	agement > l	Load Balancing	) > Virtual	Servers				
Add	Edit	Delete	Enable	Disable	Statis	tics	•	]	
Filters:	RADIUS	×							
Name			State	Effective	State	IP Address	Port	Protocol	Method
RADIUS	Virtual Server		🔘 Up	<b>O</b> Up		192.168.12.115	1812	RADIUS	ROUNDROB

## **195.5 Netscaler RADIUS configuration**

The Netscaler can now be configured to use the new Virtual Server as its RADIUS servers following the original documentation.

# 196 Testing

When functioing RADIUS entries will be seen in the Swivel RADIUS logs for each test.

Try RADIUS authentications and see which Swivel server that recieves them. Stopping one RADIUS server should indicate on the Virtual Servers that health is degraded, i.e. 50% for two servers.

# 197 Known Issues

The load balancing can produce a large number of logs.

# 198 Troubleshooting

# **199 Citrix Products Integration Matrix**

## 199.1 A guide to PINsafe and Citrix Product Integration

Product Integration

Product	SMS Text	Mobile Phone Client	Taskbar Utility	TURing Image	Index number display	Token
CAG Standard 4 or 5	Yes	Yes	Yes	No	No	Yes
CAG VPX 5	Yes	Yes	Yes	No	No	Yes
CAG VPX 5 with WI authentication	Yes	Yes	Yes	Yes	Yes	Yes
Xen App (Web Interface 4/5)	Yes	Yes	Yes	Yes	Yes	Yes
CAG Advanced AAC 4.5	Yes	Yes	Yes	Yes	Yes	Yes
CAG Advanced AC	Yes	Yes	Yes	No	No	Yes
CAG Enterprise (Netscaler) 8 or 9 or 10 10.x	Yes	Yes	Yes	Yes	Yes	Yes
WI 4.5, 4.6, 5.0, 5.1, 5.2, 5.3, 5.4	Yes	Yes	Yes	Yes	Yes	Yes
Xen App (Web Interface 4/5)	Yes	Yes	Yes	Yes	Yes	Yes
PS 4 with WI	Yes	Yes	Yes	Yes	Yes	Yes
Citrix Receiver	Yes	Yes	Yes	Yes*	Yes*	Yes

CAG = Citrix Access Gateway

AAC = Advanced Access Controller (AAC 4.x)

PS = Presentation Server

WI = Web Interface

Index Number Display is the ability to display the index number in the login page

Yes* When viewed in browser before receiver starts

## 200 Citrix Web Interface 4 with Presentation Server 4

### 200.1 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix Presentation Server 4 web interface. This also works with Citrix Secure Gateway v3.0. If the Single Channel Image for authentication is to be used a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

## 200.2 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 45083 of the Citrix web interface and have been tested with versions 4.0 and 4.2, for later versions please contact your PINsafe reseller for an update.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- · login.aspx ? Customised login page.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
  login.js ? Customised login page client script.
  loginButtons.inc ? Customised login form buttons.
  loginMainForm.inc ? Customised login form.

- login View.cs ? Customised login logic constants.
  login.cs ? Customised login logic.
  web.config.PINsafe ? Additional configuration entries for PINsafe integration.

The files can be downloaded from here: File:Citrix_PS_4.0_Integration.zip

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\AccessPlatform

## 200.3 Baseline

PINsafe 3.x

Citrix Web Interface build 3.x, 4.0, 4.2

### 200.4 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by XML.

## 200.5 PINsafe Configuration

### 200.5.1 Configuring the PINsafe Agent

On the PINsafe server:

Select Server then Agents, and create an agent for the Web Interface server, required parameters are:

Name: a Descriptive name

Hostname/IP: Web Interface server details

Shared Secret: To be also used on the Web Interface server

Click Apply to save settings.

### 200.5.2 Enabling Session creation with username

The PINsafe server can be configured so that it returns a Single Channel image by presenting the username via the XML API or the SCImage servlet. On the PINsafe server:

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

Click Apply to save settings.

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

Virtual or hardware appliance (use 8080/pinsafe and not the proxy port)

https://PINsafe server IP:8080/pinsafe/SCImage?username=testuser

Software install

### 200.6 Citrix Web Interface Configuration

#### 200.6.1 Copy across the Web Interface Files

On the Citrix Web Interface Server:

The following files need to be copied to the listed locations, below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date.

PINsafeClient.dll to /bin.

login.aspx and pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginButtons.inc and loginMainForm.inc to /app_data/auth/include.

loginView.cs and login.cs to /app_data/auth/serverscripts.

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

#### 200.6.2 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URL's under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

#### The default settings are:

```
<add key="PINsafe_SSL" value="false" />
```

- <add key="PINsafe_Server" value="192.168.2.254" />
- <add key="PINsafe_Port" value="8080" />
- <add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />
<add key="PINsafe_Server" value="192.168.2.254" />
<add key="PINsafe_Port" value="8080" />
<add key="PINsafe_Context" value="pinsafe" />
```

```
<add key="PINsafe_Secret" value="" />
```

## 200.7 Additional Configuration Options

### 200.8 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Citrix Web Interface login with SMS (Do not click on the Turing Button)

Log in		G
User name	э:	
Password	:	
Domain:		
One Time	Code:	
	Advanced	l Options >>
	TURina	Loa In

Citrix Web Interface login with Turing

Log in					0
User name:					
user1					
Password:					
••••					
Domain:					
my domain					
One Time Code:					
Advanced	Option	ns >>>			
		URing		Log	In
1 2 3 4 5	6	7	8	9	0
17400	0	1	0	T	E
41020	13	-1-1		2	9

## 200.9 Troubleshooting

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

## 200.10 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

## 200.11 Known Issues and Limitations

Self signed certificates are not supported with this version of the integration, either use a valid certificate, or non SSL communications or upgrade the Web Interface version.

The integration does not support the use of the virtual or hardware appliance proxy port for Agent-XML authentication, use port 8080 and the context pinsafe.

## 200.12 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

## 201 Citrix Web Interface 4.5 Integration

## 201.1 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 4.5 web interface. If the Single Channel Image for authentication is to be used a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

## 201.2 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 4.5.1.8215 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- login.aspx ? Customised login page.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
   login.js ? Customised login page client script.
- loginButtons.inc ? Customised login form buttons.
   loginMainForm.inc ? Customised login form.

- login.aspxf ? Customised login logic.
  web.config.PINsafe ? Additional configuration entries for PINsafe integration.

The files can be downloaded from here

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\MetaFrame

## 201.3 Baseline

PINsafe 3.5

Citrix Web Interface build 4.5.1.8215

## 201.4 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by XML.

## 201.5 PINsafe Configuration

### 201.5.1 Configuring the PINsafe Agent

On the PINsafe server:

Select Server then Agents, and create an agent for the Web Interface server, required parameters are:

Name: a Descriptive name

Hostname/IP: Web Interface server details

Shared Secret: To be also used on the Web Interface server

Click Apply to save settings.

### 201.5.2 Enabling Session creation with username

The PINsafe server can be configured so that it returns a Single Channel image by presenting the username via the XML API or the SCIMage servlet. On the PINsafe server:

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

Click Apply to save settings.

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

Virtual or hardware appliance (use 8080/pinsafe and not the proxy port)

https://PINsafe server IP:8080/pinsafe/SCImage?username=testuser

#### Software install

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

## 201.6 Citrix Web Interface Configuration

### 201.6.1 Copy across the Web Interface Files

On the Citrix Web Interface Server:

The following files need to be copied to the listed locations, below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date.

PINsafeClient.dll to /bin.

login.aspx and pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginButtons.inc and loginMainForm.inc to /app_data/auth/include.

loginView.aspxf and login.aspxf to /app_data/auth/serverscripts.

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

### 201.6.2 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

#### The default settings are:

```
<add key="PINsafe_SSL" value="false" />
```

- <add key="PINsafe_Server" value="192.168.2.254" />
- <add key="PINsafe_Port" value="8080" />
- <add key="PINsafe_Context" value="pinsafe" />
- <add key="PINsafe_Secret" value="" />

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />
<add key="PINsafe_Server" value="192.168.2.254" />
<add key="PINsafe_Port" value="8080" />
<add key="PINsafe_Context" value="pinsafe" />
```

<add key="PINsafe_Secret" value="" />

## 201.7 Additional Configuration Options

### 201.7.1 Optional: Using Static Password

On the Citrix Web Interface Server:

When using a static PINsafe password with the OTC, edit the login.aspxf file as follows:

change the following line from

if (!pc.Login(user, "", otc))

```
to
```

if (!pc.Login(user,password, otc))

## 201.8 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Citrix Web Interface with TURing image (For SMS do not click on Get Code button)

Log in	0
User name:	
name	]
Password:	
•••••	]
One Time Code:	
II	]
Advance	d Options >>>
Get code	Log In
1 2 3 4 5 6 7 8	8 9 0
1012000	K 7 1
40122051	3/1 9

## 201.9 Troubleshooting

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

### 201.9.1 Error Messages

Server Error in ?/Citrix/AccessPlatformSwivel? Application

Parser Error Message: An error occurred while parsing EntityName. Line 86, position 63.

Source Error gives line with <add key=?PINsafe_Secret? value=?&&&&&&? />

Source File: c:\inetpub\wwwroot\Citrix\AccessPlatformSwivel\web.config

You cannot use some special characters in the secret key file, such as &</nowiki>

### 201.10 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

### 201.11 Known Issues and Limitations

The integration does not support the use of the virtual or hardware appliance proxy port for Agent-XML authentication, use port 8080 and the context pinsafe.

## 201.12 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

## 202 Citrix Web Interface 4.6 Integration

## 202.1 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 4.6 web interface. If the Single Channel Image for authentication is to be used a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

## 202.2 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 4.6.0.18291 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- login.aspx ? Customised login page.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
   login.js ? Customised login page client script.
- loginButtons.inc ? Customised login form buttons.
   loginMainForm.inc ? Customised login form.

- login.aspxf ? Customised login logic.
  web.config.PINsafe ? Additional configuration entries for PINsafe integration.

The files can be downloaded from here

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\AccessPlatform

## 202.3 Baseline

PINsafe 3.5

Citrix Web Interface build 4.6.0.18291

## 202.4 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by XML.

## 202.5 PINsafe Configuration

### 202.5.1 Configuring the PINsafe Agent

On the PINsafe server:

Select Server then Agents, and create an agent for the Web Interface server, required parameters are:

Name: a Descriptive name

Hostname/IP: Web Interface server details

Shared Secret: To be also used on the Web Interface server

Click Apply to save settings.

### 202.5.2 Enabling Session creation with username

The PINsafe server can be configured so that it returns a Single Channel image by presenting the username via the XML API or the SCImage servlet. On the PINsafe server:

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

Click Apply to save settings.

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

Virtual or hardware appliance (use 8080/pinsafe and not the proxy port)

https://PINsafe server IP:8080/pinsafe/SCImage?username=testuser

#### Software install

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

## 202.6 Citrix Web Interface Configuration

### 202.6.1 Copy across the Web Interface Files

On the Citrix Web Interface Server:

The following files need to be copied to the listed locations, below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date.

PINsafeClient.dll to /bin.

login.aspx and pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginButtons.inc and loginMainForm.inc to /app_data/auth/include.

loginView.aspxf and login.aspxf to /app_data/auth/serverscripts.

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

### 202.6.2 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URL's under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

#### The default settings are:

```
<add key="PINsafe_SSL" value="false" />
```

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

```
<add key="PINsafe_Context" value="pinsafe" />
```

<add key="PINsafe_Secret" value="" />

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />
<add key="PINsafe_Server" value="192.168.2.254" />
<add key="PINsafe_Port" value="8080" />
<add key="PINsafe_Context" value="pinsafe" />
```

<add key="PINsafe_Secret" value="" />

## 202.7 Additional Configuration Options

### 202.7.1 Optional: Using Static Password

On the Citrix Web Interface Server:

When using a static PINsafe password with the OTC, edit the login.aspxf file as follows:

change the following line from

if (!pc.Login(user, "", otc))

```
to
```

if (!pc.Login(user,password, otc))

## 202.8 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Citrix Web Interface with Turing image (For SMS do not click on Get Code button)

Log in	0
User name:	
name	
Password:	
•••••	
One Time Code:	
II	
Advanced Options	>>>
Get code Log	In
1 2 3 4 5 6 7 8 9	0
1 1 3 1 A A A A	T
14012302011	7

## 202.9 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

## 202.10 Troubleshooting

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

### 202.10.1 Error Messages

Server Error in ?/Citrix/AccessPlatformSwivel? Application

Parser Error Message: An error occurred while parsing EntityName. Line 86, position 63.

Source Error gives line with <add key=?PINsafe_Secret? value=?&&&&&&? />

Source File: c:\inetpub\wwwroot\Citrix\AccessPlatformSwivel\web.config

You cannot use some special characters in the secret key file, such as &</nowiki>

### 202.11 Known Issues and Limitations

The integration does not support the use of the virtual or hardware appliance proxy port for Agent-XML authentication, use port 8080 and the context pinsafe.

## 202.12 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

## 203 Citrix Web Interface 5.0 Integration

## 203.1 Introduction

This document outlines the necessary steps to integrate Swivel authentication into the Citrix 5.0 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the Swivel server as the Image is proxied through the Web Interface server.

## 203.2 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.0.1.29110 of the Citrix web interface, if you have a later version please contact your Swivel reseller for an update. Your Swivel server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- PINsafeClient.dll ? Swivel authentication client library.
- include.aspxf ? Customised include file.
- include.aspxt ? Customised include file.
  pinsafe_image.aspx ? Serves single channel images from Swivel to users.
  login.js ? Customised login page client script.
  loginstyle.inc ? Customised login form style.
  loginMainForm.inc ? Customised login form.
  Constants.java ? Customised login logic constants.
  web.config.PINsafe ? Additional configuration entries for Swivel integration.
  Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here: File:Citrix_WI_5.0_Integration.zip

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\XenApp

### 203.3 Baseline

Swivel 3.5

Citrix Web Interface build 5.0.1.29110

## 203.4 Architecture

The Citrix Web Interface makes authentication requests against the Swivel server by RADIUS.

## **204 Swivel Configuration**

## 204.1 Configuring the RADIUS server

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

### 204.2 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.

### 204.2.1 Setting up Swivel Dual Channel Transports

See Transport Configuration

## 204.3 Citrix Web Interface Configuration

### 204.3.1 Copy accros the Web Interface Files

The required files (see prerequisites) need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

PINsafeClient.dll to /bin.

include.aspxf to /app_data/serverscripts

pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app_data/include.

Constants.java to /app_code/PagesJava/com/citrix/wi/pageutils

Radius_secret.txt to /

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

### 204.3.2 Edit the Radius_secret.txt

On the Citrix Web Interface server

Edit the radius_secret.txt file so that it has the same shared secret as has been entered on the Swivel server.

### 204.3.3 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be coied into the <appSettings> section of the web.config file. Adjust the key values to reflect your Swivel installation.

#### The default settings are:

```
<add key="PINsafe_SSL" value="false" />
```

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />

If using a Swivel virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />
```

```
<add key="PINsafe_Server" value="192.168.2.254" />
```

```
<add key="PINsafe_Port" value="8443" />
```

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />

### 204.3.4 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, the select Radius from the dropdown list.

General	Two-Factor Authentication	Two-Factor Authentication				
Explicit     Authentication Type     Two-Factor Authentication     Password Settings     Account Set-Service	Two-factor setting: RADIUS authentication is enabled. RADIUS server addresses (in order	US  Check the settings below: er):	)			
	Add Edit	Berrove	Move Do <u>wr</u>			
	✓ Use the <u>s</u> erver list for load bala	ancing				

## 204.4 Additional Configuration Options

see Citrix Web Interface 5.X additional login page options

## 204.5 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct Swivel one time code is entered in addition to the Citrix credentials should the user be logged in.

## 204.6 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the dropdown list. Remove the Swivel RADIUS entries.

## 204.7 Troubleshooting

Check the Swivel logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a Swivel virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the Swivel server or for testing the client can accept the certificate (load Image URL into browser)
- Swivel server not accessible, check networking and firewalls. Check the Swivel server logs for a session started message.
- Incorrect Swivel URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

#### 204.7.1 Error Messages

#### INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the Swivel NAS setting do not match.

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

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

### 204.8 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the Swivel settings and files so the Swivel integration may need to be applied again.

## 204.9 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

## 205 Citrix Web Interface 5.1 Dual Channel button

## 205.1 Citrix Web Interface Dual Chanel Integration Notes

This outlines how to replace the Single Channel Image request button with a Dual Channel button. This is a supplement to the Citrix Web Interface 5.1 Integration guide.

## 205.2 Log-in page Customisation

On the Swivel Administration console under Server/Dual Channel, ensure Allow message request by username: is set to Yes.

On the Citrix Web Interface Installation create a copy of auth/pinsafe_image.aspx, and call it pinsafe_message.aspx

You will also need to ensure that pinsafe_message.aspx is included in the list of unprotected pages.

In auth/clientscripts/login.js, make a copy of the function onTuringButtonClick(), calling it onMessageButtonClick (). Change image.src in this function to point to pinsafe_message.aspx.

Edit app_data/include/loginMainForm.inc. Locate the text '<div class="otcButtonPane". Copy from here up to the ending </div>, and paste it immediately after this div. Change "href=javascript:onTuringButtonClick" to "href=onMessageButtonClick".

Change the title and id of this div, as well as the id of the enclosed img and span elements. The new div element should be something like this:

```
<div class="otcButtonPane"><a
    href="javascript:onMessageButtonClick()" title="Click this button to retrieve a PinSafe message."
    onmouseover="changeOtcBtnColor(true);" onmouseout="changeOtcBtnColor(false);"
    onfocus="changeOtcBtnColor(true);" onblur="changeOtcBtnColor(false);"
    tabIndex="<%=Constants.TAB_INDEX_FORM%>"
    id="dcmessage"
    name="dcmessage"
    ><img id="msgButtonBg" src="../media/LoginButtonGlow.gif" alt="" /><span id="msgButtonWrapper">Get Message/a></div>
```

To make sure the new button looks right, you will also need to edit app_data/include/loginStyle.inc. Look for occurrences of #otcButtonWrapper and add ", #msgButtonWrapper". Also, for the entry #<%=Constants.ID_OTC_BTN%>, add ", #dcmessage".

## 205.3 Testing

Test the button from the login page. Check the Swivel logs for the dual channel requests.

# 206 Citrix Web Interface 5.1 Integration

# **207 Introduction**

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.1 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

## **208 Prerequisites**

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.1.1 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- PINsateClient.dll ? PINsate authentication client library.
  include.aspxf ? Customised include file.
  pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
  login.js ? Customised login page client script.
  loginstyle.inc ? Customised login form style.
  loginMainForm.inc ? Customised login form.
  Constants.java ? Customised login logic constants.
  web.config.PINsafe ? Additional configuration entries for PINsafe integration.
  Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here: File:Citrix_WI_5.1_Integration.zip

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\XenApp

# 209 Baseline

PINsafe 3.5 Citrix Web Interface build 5.1.1

# **210 Architecture**

The Citrix Web Interface makes authentication requests against the PINsafe server by RADIUS.

# **211 Swivel Configuration**

## 211.1 Configuring the RADIUS server

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

## 211.2 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.

## 211.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

## 212 Citrix Web Interface Configuration

## 212.1 Copy across the Web Interface Files

The required files (see prerequisites) need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

PINsafeClient.dll to /bin.

include.aspxf to /app_data/serverscripts

pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app_data/include.

Constants.java to /app_code/PagesJava/com/citrix/wi/pageutils

Radius_secret.txt to /Conf

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

## 212.2 Edit the Radius_secret.txt

On the Citrix Web Interface server

Edit the radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server.

## 212.3 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be coied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

#### The default settings are:

```
<add key="PINsafe_SSL" value="false" />
```

```
<add key="PINsafe_Server" value="192.168.2.254" />
```

```
<add key="PINsafe_Port" value="8080" />
```

```
<add key="PINsafe_Context" value="pinsafe" />
```

```
<add key="PINsafe_Secret" value="" />
```

<add key="PINsafe_AcceptSelfSigned" value="false" />

If using a Swivel virtual or hardware appliance, then the following settings may need to be used.

<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="true" />

## 212.4 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the dropdown list.

∃-General	Two-Factor Authentication				
Domain Restriction Explicit Authentication Type Two-Factor Authentication Password Settings	Two- <u>factor setting</u> : RADIUS authentication is enabled. ( RADIUS server addresses (in order	S  Check the settings below:			
	Address 10.7.142.128 10.7.142.129	Port 1812 1812	Move Up Move Do <u>w</u>		
	Add Edit,	Remove			
	Bypass any failed server for:	1 Hours	•		

# **213 Additional Configuration Options**

see Citrix Xen App 5.x additional login page options

## 213.1 Self Reset

This outlines how to add the self reset option to the Citrix Web Interface.

The Citrix Web Interface 5.1 self reset files can be downloaded here: File:Citrix_WI_5.1_SelfReset.zip

Download PINsafeClient.dll and copy to the bin folder overwriting the existing file installed above. Copy reset.aspx and reset.aspx.cs into the auth folder.

Add reset.aspx to the list of unprotected pages in web.config. Locate key="AUTH:UNPROTECTED_PAGES", and at the end of the value field, insert ",./reset.aspx".

Insert a link on the Citrix login page to open the reset page.

Edit app_data\include\loginMainForm.inc, and insert the following line after the login button row, immediately before the tag.

<a href="./reset.aspx" target="_blank">Forgotten my PIN</a>

# 214 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

# 215 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the dropdown list. Remove the PINsafe RADIUS entries.

# **216 Troubleshooting**

Check the PINsafe logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a Swivel virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

### 216.1 Error Messages

#### INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the PINsafe NAS setting do not match.

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

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

# 217 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the PINsafe settings and files so the PINsafe integration may need to be applied again.

# **218 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
# 219 Citrix Web Interface 5.2 Integration

# **220 Introduction**

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.2 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

### **221 Prerequisites**

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.2 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- include.aspxf ? Customised include file.
  pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
  login.js ? Customised login page client script.
  loginstyle.inc ? Customised login form style.
  loginMainForm.inc ? Customised login form.
  Constants.java ? Customised login logic constants.
  web.config.PINsafe ? Additional configuration entries for PINsafe integration.
  Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here: File:Citrix_WI_5.2_Integration.zip

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\XenApp

# 222 Baseline

PINsafe 3.5 Citrix Web Interface build 5.2

## 223 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by RADIUS.

### 224 Swivel Configuration

### 224.1 Configuring the RADIUS server

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

### 224.2 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.

### 224.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

### 225 Citrix Web Interface Configuration

#### 225.1 Copy across the Web Interface Files

The The required files (see prerequisites) need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

include.aspxf to /app_data/serverscripts

pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app_data/include.

Constants.java to /app_code/PagesJava/com/citrix/wi/pageutils

Radius_secret.txt to /Conf

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

#### 225.2 Edit the Radius_secret.txt

On the Citrix Web Interface server

Edit the radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server.

#### 225.3 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

#### The default settings are:

<add key="PINsafe_SSL" value="false" />
<add key="PINsafe_Server" value="192.168.2.254" />
<add key="PINsafe_Port" value="8080" />
<add key="PINsafe_Context" value="pinsafe" />
<add key="PINsafe_Secret" value="" />
<add key="PINsafe_AcceptSelfSigned" value="false" />
<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" /></add key="RADIUS_secret_PATH" value="/radius_secret_status_secret_Status_secret_Status_secret_Status_secret_Status_secret_Status_secret_Status_secret_Status_secret_Status_secret_Status_secret_Status_secret_Status_

<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

#### If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

<add key="PINsafe_SSL" value="true" />
<add key="PINsafe_Server" value="192.168.2.254" />
<add key="PINsafe_Port" value="8443" />
<add key="PINsafe_Context" value="proxy" />
<add key="PINsafe_Secret" value="" />
<add key="PINsafe_AcceptSelfSigned" value="True" />
<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" /></add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />
</add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" /></add key="RADIUS_SECRET_PATH" value_SECRET_PATH" value_SECRET_PATH" value_SECRET_PATH" value_SEC

### 225.4 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list.

⊡-General	Two-Factor Authentication		
Domain Restriction Explicit Authentication Type Two-Factor Authentication Password Settings	Two-factor setting: RADI RADIUS authentication is enabled.	US  Check the settings below:	)
	Address 10.7.142.128 10.7.142.129	Port 1812 1812	Move <u>Up</u> Move Do <u>w</u> n
	Add Edit ✓ Use the server list for load bal	Remo <u>v</u> e.	
	Bypass any failed server for:	1 🕂 Hours	•

Configure the PINsafe server as RADIUS server. If you have more than 1 PINsafe server, you may need to configure all of them in the preferred order. NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.

# 226 Additional Configuration Options

see Citrix Xen App 5.x additional login page options

# 227 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

## 228 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list. Remove the PINsafe RADIUS entries.

## 229 Troubleshooting

Check the PINsafe logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a Swivel virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

#### 229.1 Error Messages

#### INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the PINsafe NAS setting do not match.

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

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

# 230 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the PINsafe settings and files so the PINsafe integration may need to be applied again.

# 231 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

# 232 Citrix Web Interface 5.3 Integration

# 233 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.3 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

### **234 Prerequisites**

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.3 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
  login.js ? Customised login page client script.
  loginstyle.inc ? Customised login form style.
  loginMainForm.inc ? Customised login form.
  Constants.java ? Customised login logic constants.
  web.config.PINsafe ? Additional configuration entries for PINsafe integration.
  Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here

Note: The default Citrix Install path is: C:\Inetpub\wwwroot\Citrix\XenApp

PINsafe uses .NET so is not dependant on the OS being 32 bit or 64 bit.

# 235 Baseline

PINsafe 3.5 Citrix Web Interface build 5.3

## 236 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by RADIUS.

### 237 Swivel Configuration

### 237.1 Configuring the RADIUS server

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

### 237.2 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.

### 237.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

### 238 Citrix Web Interface Configuration

#### 238.1 Copy across the Web Interface Files

The required files (see prerequisites) need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

include.aspxf to /app_data/serverscripts

pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app_data/include.

Constants.java to /app_code/PagesJava/com/citrix/wi/pageutils

Radius_secret.txt to /Conf

Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.

#### 238.2 Edit the Radius_secret.txt

On the Citrix Web Interface server

Edit the radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server.

#### 238.3 Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file (not the <switches> section). Adjust the key values to reflect your PINsafe installation.

Note: The setting <add key="RADIUS_NAS_IDENTIFIER" value="" /> is present in the file and needs to be set to <add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />

<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="True" />

#### The settings for a software install of PINsafe are:

<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />

<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_AcceptSelfSigned" value="false" />

### 238.4 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list.

∃ General	Two-Factor Authentication		
Domain Restriction Explicit Authentication Type Two-Factor Authentication Password Settings Account Setf-Service	Two-factor setting: RADIUS RADIUS authentication is enabled. Check RADIUS server addresses (in order):	• k the settings below:	
	10.7.142.128 10.7.142.129	1812 1812 Move Up Move Down	
	Add Edit Rem ✓ Use the server list for load balancing Bypass any failed server for:	yoye	

Configure the PINSAFE server as RADIUS server. If you have more than one PINsafe server, you may need to configure all of them in the preferred order. NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.

# **239 Additional Configuration Options**

see Citrix Xen App 5.x additional login page options

## 240 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Login using Dual channel authentication

Welcome Log on to access your	applications.			
	User name:	graham		
	Password:			
	Domain:	ср		3
	PASSCODE:			?
			Get Code	
			Log On	

Login Using Single Channel Graphical Turing Image

Log on to access y	our applications.		
	User name:	graham	
	Password:	•••••	
	Domain:	ср	?
	PASSCODE:		?
	1 2 3	3 4 5 6 7 8 9	0
	2/1		12
	13 6 9	8/0/4/1/7/2	/ 5
	Get Code		

# 241 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list. Remove the PINsafe RADIUS entries.

## 242 Troubleshooting

Check the PINsafe logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a PINsafe virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

#### 242.1 Error Messages

#### INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the PINsafe NAS setting do not match.

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

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

# 243 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the PINsafe settings and files so the PINsafe integration may need to be applied again.

# 244 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

# 245 Citrix Web Interface 5.4 Integration

## 246 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.4 web interface/Xen App. If the Single Channel Image for authentication is to be used, a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

A statement from Citrix: All 7.x versions of XenApp and XenDesktop now support the use of Web Interface 5.4. Citrix has extended support of Web Interface for XenApp 7.5, XenDesktop 7.5, XenDesktop 7.1 and XenDesktop 7.0 to allow more time for planning and transition to StoreFront. Note, no new features will be added to Web Interface and its end-of-life remains August 2016.

### 247 Prerequisites

This installation guide assumes that a Presentation Server site has been configured with Explicit authentication enabled. The customised files provided are based on build 5.4 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation and need to be edited as required (see below):

- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
  login.js.add ? Customised login page client script.
  loginStyle.inc.add ? Customised login form style.
  loginMainForm.inc.add ? Customised login form.
  web.config.add ? Additional configuration entries for PINsafe integration.
  Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here.

An alternative solution, which includes buttons for TURing image and message request, can be found here. This solution includes two additional files: pinsafe_message.aspx and pinsafe_ping.aspx.

Note: The default Citrix Install path is: C:\Inetpub\wwwroot\Citrix\XenApp

PINsafe uses .NET so is not dependent on the OS being 32 bit or 64 bit.

NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.

NOTE: the files with the extension ".add" cannot simply be copied into the appropriate directories. They are text files containing notes as to how you should modify the corresponding files to implement PINsafe customisation. See the notes below for more details.

# 248 Baseline

PINsafe 3.7 Citrix Web Interface build 5.4

## 249 Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by RADIUS.

### **250 Swivel Configuration**

### 250.1 Configuring the RADIUS server

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

### 250.2 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.

### 250.2.1 Setting up PINsafe Dual Channel Transports

See Transport Configuration

### 251 Citrix Web Interface Configuration

### 251.1 Edit the radius_secret.txt

On the Citrix Web Interface server

Edit the conf/radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server. A copy of this file is included in the zip archive.

### 251.2 Edit the web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Note: the setting <add key="RADIUS_NAS_IDENTIFIER" value="" /> is present in the file and needs to be changed to

<add key="RADIUS_NAS_IDENTIFIER" value="citrix_wi" />

Note: It is recommended that you use the same value as the identifier in the NAS entry in the PINsafe admin console.

If the Web Interface server has multiple network interfaces, the value of RADIUS_NAS_IP_ADDRESS may need to be set to the IP address used by the NAS. This is the IP address of the Web Interface server, NOT the PINsafe server.

Make sure that the following entry is included, if it is not there already:

<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />

To allow access to the TURing image from the login page, locate the following line:

<add key="AUTH:UNPROTECTED_PAGES" ...

The value attribute on this entry is a list of URLs that can be accessed without authentication. Add the following to the end of this list (before the closing quote):

,/auth/pinsafe_image.aspx

If you are using the alternative integration, you will need to include the other files:

,/auth/pinsafe_image.aspx,/auth/pinsafe_message.aspx,/auth/pinsafe_ping.aspx

#### 251.3 Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list.

⊡ General Demois Restriction	I wo-Factor Authentication		
Domain Restriction Explicit Authentication Type Two-Factor Authentication Password Settings Account Self-Service	Two- <u>factor setting</u> : RADIUS authentication is enabled. Check <u>R</u> ADIUS server addresses (in order):	ck the settings below:	
	Address 10.7.142.128 10.7.142.129	Port Move Up 1812 1812 Move Down	
	Add     Edit     Ren       I     Use the server list for load balancing       Bypass any failed server for:	noye g 1 🛨 Hours 💌	

Configure the PINSAFE server as RADIUS server. If you have more than one PINsafe server, you may need to configure all of them in the preferred order. NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.
## **252 Additional Configuration Options**

The above modifications will allow authentication to the Web Interface using some of the PINsafe authentication mechanisms such as SMS, mobile Phone applet, and Taskbar. Additional configuration options including the single channel TURing image are listed below.

see also Citrix Web Interface 5.X additional login page options

### 252.1 Changing the OTC label

To change the label for the PINsafe one-time code field from the default of ?PASSCODE:?, locate the file C:\Program Files\Citrix\Web Interface\5.4.0\Languages\accessplatform_strings.properties. (If the language is not English, locate the appropriate file for the appropriate language, if it exists). Edit this file, and locate the line containing ?Passcode=PASSCODE:?. Replace the second word PASSCODE with OTC, or an appropriate text.

### 252.2 Configuring Single Channel: Modifying the Web Interface Files

The required files (see prerequisites) are of two types: those NOT ending in ".add" need to be copied to the following locations below the root of the Citrix web interface site. Those ending in ".add" contain instructions describing how to modify the corresponding file without the ".add" extension. Where an existing file is being replaced or modified, ensure you make a backup copy so that the integration can be removed at a later date. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory. The below files contained within the zip file should extract to the relevant locations.

The majority of the files included in the integration are modifications to existing files. This are stored with the same name as the file they are intended to modify, but with the additional extension of .add. Each file contains instructions as to how the original files should be added. More details are given below:

1. Copy pinsafe_image.aspx to /auth. This is a new file, not a modification to an existing one.

2. Edit login.js in /auth/clientscripts. Insert the contents of login.js.add at the start of this file, below the header, as indicated in the file itself.

3. Edit loginMainForm.inc in /app_data/include. Insert the contents of loginMainForm.inc.add as indicated in this file: locate a particular section of the file and insert a line.

4. Edit loginstyle.inc in /app_data/include. Insert the contents of loginstyle.inc.add at the bottom of this file, before the footer text, as indicated in the file.

5. Ensure file permissions are set correctly on the copied files, Authenticated users need read permissions.

### 252.3 Configuring Single Channel: Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

The web.config.add file contains additional keys that need to be copied into the <appSettings> section of the web.config file (not the <switches> section). Adjust the key values to reflect your PINsafe installation.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

If using a Swivel virtual or hardware appliance, then the following settings may need to be used.

<add key="PINsafe_SSL" value="true" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8443" />

<add key="PINsafe_Context" value="proxy" />

<add key="PINsafe_Secret" value="" />

<add key="PINsafe_AcceptSelfSigned" value="True" />

#### The settings for a software install of PINsafe are:

<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />

<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

<add key="PINsafe_Secret" value="" />

### 252.4 Challenge and Response Authentication with Count Down Timer

Citrix Web Interface can be configured to use Challenge and Response whereby a user enters a username and password, and if that is correct the user is sent an SMS message and will be prompted to enter an OTC. By default the OTC sent is valid for two minutes only, so a count down timer is provided to show how long the user has left.

For information on configuring the PINsafe RADIUS Challenge and response see Challenge and Response How to Guide.

The required files can be downloaded here: Challenge and Response with count down files

Extract the files ensuring their correct locations

challenge.inc is copied to app_data/include

challenge.js to auth/clientscripts

# 253 Testing

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Login using Dual channel authentication

Log on to access your a	pplications.			
	User name:	graham		1
	Password:			
	Domain:	ср	*	2
	PASSCODE:			3
			Get Code	
			Log On	

Login Using Single Channel Graphical Turing Image

User name:	graham	
Password:	•••••	
Domain:	cp 💌	?
PASSCODE:	****	?
1 2 3	3 4 5 6 7 8 9 (	0
4/0	10/0/1/1/2/2/1	
13/0 3	0/0/4/1/1/2/3	2

## 254 Uninstalling

Copy the backup files made at the start of installation back to their original locations.

On the Citrix Web Interface server:

Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select Configure Authentication methods > explicit.

Click Properties > Two-factor authentication, then select Radius from the drop down list. Remove the PINsafe RADIUS entries.

## **255 Troubleshooting**

Check the PINsafe logs for any error messages, or absence of session starts and RADIUS requests.

If following the installation steps the Citrix web interface fails to display properly edit web.config and set the customErrors mode to Off. This will enable the display of detailed error messages which may assist in troubleshooting.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

For a Swivel virtual or hardware appliance:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

If the virtual or hardware appliance is using a self signed certificate, you need to add the following entry to web.config:

<add key="PINsafe_AcceptSelfSigned" value="true" />

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

### 255.1 Error Messages

#### INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT

This indicates that the shared secret on the access device and the PINsafe NAS setting do not match.

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

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

## 256 Known Issues and Limitations

Upgrading the Citrix Web Interface will overwrite the PINsafe settings and files so the PINsafe integration may need to be applied again.

If you need to use userPrincipalName to authenticate to Swivel, you may find that the domain name is removed before sending the username to Swivel. To avoid this, make the following changes:

#### Locate and edit the file app_code\PagesJava\com\citrix\wi\pageutils\TwoFactorAuth.java

#### Find the following method:

```
public static String getUserName(UPNCredentials token, boolean fullyQualified) {
    if (fullyQualified) {
        return token.getShortDomain() + "\\" + token.getShortUserName();
    } else {
        return token.getShortUserName();
    }
}
```

#### Replace it with the following:

```
public static String getUserName(UPNCredentials token, boolean fullyQualified) {
  return token.getUserIdentity();
}
```

# **257 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

## 258 Citrix Web Interface 5.X additional login page options

### 258.1 Citrix Web Interface 5.x additional login page options

This outlines how to further customise the Citrix login page. This is a supplement to the Citrix Web Interface 5.x Integration guides.

### 258.2 Removing the Single Channel Button

To remove the *refresh image*, delete the following text:

### 258.3 Replacing the Single Channel Button with a Dual Channel Button

#### 258.3.1 Replacing TURing image with a Dual Channel (SMS) request

Edit the file pinsafe_image.aspx

#### find the following line:

```
url.AppendFormat("{0}:{1}/{2}/SCImage?username={3}", server, port, context, Request.QueryString["username"]);
```

#### Replace with:

url.AppendFormat("{0}:{1}/{2}/DCImage?username={3}", server, port, context, Request.QueryString["username"]);

#### 258.3.2 Compatibility

This has been tested on Citrix Web Interface 5.1

#### 258.3.3 Dual Channel Button modification

On the Swivel Administration console under Server/Dual Channel, ensure Allow message request by username: is set to Yes.

On the Citrix Web Interface Installation create a copy of auth/pinsafe_image.aspx, and call it pinsafe_message.aspx

You will also need to ensure that pinsafe_message.aspx is included in the list of unprotected pages.

In auth/clientscripts/login.js, make a copy of the function onTuringButtonClick(), calling it onMessageButtonClick (). Change image.src in this function to point to pinsafe_message.aspx.

Edit app_data/include/loginMainForm.inc. Locate the text '<div class="otcButtonPane". Copy from here up to the ending </div>, and paste it immediately after this div. Change "href=javascript:onTuringButtonClick" to "href=onMessageButtonClick".

Change the title and id of this div, as well as the id of the enclosed img and span elements. The new div element should be something like this:

```
<div class="otcButtonPane"><a
    href="javascript:onMessageButtonClick()" title="Click this button to retrieve a PinSafe message."
    onmouseover="changeOtcBtnColor(true);" onmouseout="changeOtcBtnColor(false);"
    onfocus="changeOtcBtnColor(true);" onblur="changeOtcBtnColor(false);"
    tabIndex="<%=Constants.TAB_INDEX_FORM%>"
    id="dcmessage"
    name="dcmessage"
    ><img id="msgButtonBg" src="../media/LoginButtonGlow.gif" alt=" /><span id="msgButtonWrapper">Get Message/a></div>
```

To make sure the new button looks right, you will also need to edit app_data/include/loginStyle.inc. Look for occurrences of #otcButtonWrapper and add ", #msgButtonWrapper". Also, for the entry #<%=Constants.ID_OTC_BTN%>, add ", #dcmessage".

To change the Refresh Image button modify the file under auth\clientscripts\login.js.add and search for the line Refresh Image and change to the required text, such as Request Code or Request SMS.

```
"<span class='rightDoor'>Refresh Image</span>" +"
```

#### 258.3.4 Dual Channel Testing

Test the button from the login page. Check the Swivel logs for the dual channel requests.

### 258.4 Single Channel Button with an automated Single Channel Image

The Citrix Web Interface 5.x integration has a button to generate the Single Channel Image. This can be modified to automatically show the Turing image without the need for pressing the button when the user enters into the required field.

### 258.4.1 Compatibility

This has been tested on Citrix Web Interface 5.1 using the Single Channel Turing Image

#### 258.4.2 Single Channel Button to automated Single Channel Image modification

Edit the loginMainForm.inc file on the Citrix server. Locate the username field - look for the following:

<input type='text' name='<%=Constants.ID_USER%>' ...

insert the following line after that one:

onblur='onTuringButtonClick()'

This causes the turing image JavaScript function to be called when the user leaves the username field.

#### 258.4.3 Automated Single Channel Image Testing

Test the image from the login page. Check the Swivel logs for the single channel image requests.

### 258.5 Turing, Dual channel and Display Index buttons

The Citrix Web Interface 5.x integration has a button to generate the Single Channel Image. This can be modified to add additional buttons of Show Turing Image, Send Dual Channel Security String and Display Index number. See also Multiple Security Strings How To Guide

#### 258.5.1 Compatibility

This has been tested on Citrix Web Interface 5.3

#### 258.5.2 Required Files

The following files are required and should be used for installation: [1]

#### 258.5.3 Installation Instructions

Follow the installation instructions for the relevant Citrix version.

#### 258.5.4 Testing

Verify that three buttons are displayed and that they show the expected results when selected.

The following screen shots show the different buttons in use

Benutzername:	graham	
Kennwort:	••••	
PASSCODE:		?
1 2 3	4 5 6 7 8 9	0
2/9/6/	0/3/8/4/17	5
Click t	his button to retrieve a PinSafe	code image.

Single Channel TURing Image request

Melden Sie sich an,	um auf Ihre Anwend	dungen zuzugrei	fen.	
	Benutzername:	graham		
	Kennwort:			
	PASSCODE:			?
		00		
	Get Image	Get String	Get Index	
			Anmelden	

Multiple Security String Message index number telling user which security string to use for authentication



Securiy String On Demand Confirmation message of sending the user a Security String

# 259 Cyberoam UTM SSL VPN

## **260 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.

### 260.1 Prerequisites

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

Cyberoam Firmware 10.x

PINsafe 3.x

### 260.2 Baseline

Cyberoam CR25i firmware 10.01.0 build 739

PINsafe 3.8

### 260.3 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.

# 261 Swivel Configuration

## 261.1 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.

Identifier:	Cyberoam	and the second second second
Hostname/IP:	172.16.1.1	CONTRACTOR
Secret:	000000000000000000000000000000000000000	the second s
EAP protocol:	None 🔻	formation and a second for the second seco
Group:	ANY 7	in Suchester 1
Authentication Mode:	All 🗢	
Vendor (Groups):	Watchguard 🗢	and mathematica
Change PIN warning:	No 🗵	e vesmeer j comganaen
Two Stage Auth:	No 🔽 Dalata	Beck

## 261.2 PINsafe Dual Channel Authentication

See Transport Configuration

## 262 Cyberoam CR25i Configuration

### 262.1 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:

#### 262.1.1 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.

### 262.1.2 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

Edit External Server		×	
Server Type	RADIUS Server	w	
Server Name *	PINs		Professional An
Server P*	172.16.1.9		
Authentication Port *	1820		1
Shared Secret *	3000300030		
Integration Type *	O Loose Integration		
	Tight Integration		
Group Name Attribute *	Fiter-kl		
Tas	20 Intection	Canosi	
			BUTTO BEAUGUARDE AND
			THE REPORT OF A CONTRACT OF A

### 262.2 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.

SSL VPN Au	thentication Methods			
	Same as VPN			The state of the s
	Same as Firewall			
	Ø Set Authentication Method for	SSL VPN		A A A A A A A A
	Authentication Server List	Selected Authentication Server		
	Q Search			
	Local	PINsafe_170		
	HEATHCOMM			12 A CONTRACTOR OF AND
	Lunzais_110			
	4	P		
		List order indicates Priority		
			Apaty	

### 262.3 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.

### 262.4 Additional Cyberoam Configuration Options

### 262.4.1 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

### 262.4.2 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.

eneral Settings		的建筑家族
Logo	Default Custom     Browse.     (Size: 700 X 80 Pixels)	
Window Title	Cyberoam SSL VPN Portal	
Login Page Message	<font style="fant-size:18px;font-family: tgbggg;"><b>Welcome to the Cybgroam SSL VPM Portal </b></font> font style="font-size:12px;font-family: tgbggg;">To authenticate, please type your password directly followed by PMgggg; OTC in the "Password:" field. <tp>Example: <b>mypassword5482</b><tp></tp></tp>	D
Home Page Message	<font style="font-size:18px;font-family:Arial,"><b>SSL, 신인 User Portal</b></font>	า เขาะสุขารระบาท เขาะสาย 
olor Scheme		
Background FFFFFF	Fant Color 0000	enisperiencessere
Table Header 65739E	Table Header Font Color FFFF	F
Table Cells EEEEF0	Table Cells Font Color 0000	مەرەپەرىيە بىلىغ ئىلى ئەرەپىرىكى ئەرەپىرىكى ئەرەپىرىكى ئەرەپىرىكى ئەرەپىرىكى ئەرەپىرىكى ئەرەپىرىكى ئەرەپىرىكى ئەرەپىرىكى ئەرەپىر
	Kon v Previewsky Resetto Datau 1	

### 262.5 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.

Cyberoam [•]	
Welcome to the Cyberoam SSL VPN Portal! To authenticate, please type your AD password directly followed by PINsafe OTC in the "Password:" field. Example: mypassword5482	
Usemame:	
Password:	

### 262.6 Troubleshooting

Check the PINsafe logs for RADIUS requests.

### 262.7 Known Issues and Limitations

Dual Channel authentication and Taskbar only

### 262.8 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

# 263 Deploy ACD using MS group policies

## **264 Introduction**

These are the instructions to use the windows group policies to "deploy" the AuthControl Desktop (Credential Provider).

## 265 Steps

1 - Install the Credential Provider on a single machine. Configure it as required, then use File, Export Settings from the configuration program to create a settings file named acd.xml. Alternatively, if you have a pre-configured build, there is no need for this step.

2 - Create a network share that can be accessed by all computers. Copy both the credential provider MSI and acd.xml (if required) to that folder.

3 - From the domain controller, in Server Manager, select the Tools menu, then "Group Policy Management".

4 - Select the domain node on the left-hand window. Right-click and choose "Create a GPO in this domain and link it here".

5 - Give the GPO a name, such as "AuthControl Credential Provider", and click OK.

6 - Under Group Policy Objects, find the GPO you just created, right-click on it and click Edit.

7 - Choose Computer Configuration, Policies, Software Settings, Software installation. Right-click and select New -> Package.

8 - From the file browser, enter the location of the MSI. It must be entered as a network share, i.e. \\Computer\Share\AuthControlCredentialProvider.msi. Leave deployment method as "Assigned".

9 - Choose User Configuration, Policies, Software Settings, Software installation and repeat the last 2 steps, except this time, the deployment method should be "Published".

10 - Close the editor and left-click on the GPO. Under Scope you should see the domain name in the Links section. Right-click on it and check "Enforced". Note that this will install the CP on every computer in the domain. It should be possible to restrict the policy to a single Organisational Unit, by applying the GPO link to that OU. You can only apply policies to domains or OUs, not ordinary containers. You can also restrict the policy by creating a group of computers and adding that group to Security Filtering.

9a) Choose User Configuration, Policies, Software Settings, Software installation. Right-click and select New -> Package.

9b) From the file browser, enter the location of the MSI. It must be entered as a network share, i.e. \Computer\Share\AuthControlCredentialProvider.msi. Set deployment method to "Published".

## 266 Notes

Our understanding is that steps 7 and 8 make the software available for network installation. This step installs the software automatically if it is not yet installed, the next time each user connects to the domain.

The notes on the final step suggest how you can restrict which computers have the WCP installed.

Check the link below for more details:

https://support.microsoft.com/en-gb/help/816102/how-to-use-group-policy-to-remotely-install-software-in-windows-server

## 267 Changing Settings

If you want to change the settings for computers that already have AuthControl Desktop installed, for example, to enable or disable test mode, currently the only way to do this is to change the registry settings directly.

All the settings are in the following registry key:

\\HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\AuthControl Desktop

You will need to know the names of the settings in the registry: please contact Swivel Secure support for specific requests. We will give an example below of enabling or disabling Test Mode, for which the setting name is "TestMode".

- 1. Open "Group Policy Management" from a Domain Controller.
- Right-click on the domain, or an OU if you only want to apply the policy to a subset
   Select "Create a GPO in this domain and link it here". Give the GPO a name.

- Select "Create a GPO in this domain and link it here". Give the GPO a name.
   Right-click on the GPO and select "Edit"
   Expand the tree for "Computer Configuration" -> "Preferences" -> "Windows Settings" -> "Registry"
   Right-click on "Registry" and select New -> Registry Item
   Make sure that action is "Update" and Hive is "HKEY_LOCAL_MACHINE"
   Enter Key Path as "SOFTWARE\Swivel Secure\AuthControl Desktop". Make sure you type this correctly, including the correct spacing
   Enter the Value name as "TestMode". To change a different value, enter the name as given by Swivel Secure
   Set the value type to REG_DWORD (this is for numeric or on/off settings for text settings use REG_SZ)
   Set the value data to 1 to enable TestMode, or 0 to disable it.

- 11. Set the value data to 1 to enable TestMode, or 0 to disable it.
- 12. Click OK

Note two points:

- The settings are only applied when a computer is restarted
- The settings are not applied immediately, so it is possible that the first login after restart will still use the old settings.

# 268 Ericom PowerTerm WebConnect

## **269 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.

# **270 Prerequisites**

Swivel 3.3 PowerTerm WebConnect

## 271 Baseline

Swivel 3.9

## 272 Architecture

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

## 273 Installation

### 273.1 Swivel Integration Configuration

### 273.1.1 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

RADIUS>Server	0
Please enter the details for t	he RADIUS server.
Server enabled:	Yes 💌
IP address:	0.0.0.0
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No 💌
Filter ID:	No 💌
Additional RADIUS logging:	Both
Enable debug:	Yes 💌
Radius Groups:	Yes 💌
Radius Group Keyword:	POLICY
	Apply Reset

### 273.1.2 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.

# RADIUS>NAS 🕑

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther via the RADIUS interface.

NAS:	Identifier:	Device Name
	Hostname/IP:	192.168.0.1
	Secret:	•••••
	EAP protocol:	None
	Group:	ANY
	Authentication Mode:	All
	Change PIN warning:	No 💌
		Apply Reset

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.

### 273.2 Ericom PowerTerm WebConnect Integration

### 273.2.1 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.

### 273.2.2 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?

Application Publishing Advanced Setti	ngs	
Cradantids Usemane Xu	Pessaveentt	
Use WebConnect User Credentials		
Use Dafault Domain		

## 273.3 Additional Installation Options

## 274 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.

NoverTerm Web	Connect Login	? X	) í
User Name:		2	
Pessword	Login	Cancel	

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.

- Natwork Password Authentication		
Reese enter your network password		
		And a second sec
	OK	
	Cancel	THE REPORT OF THE PARTY OF THE

The application will then open.

# 275 Uninstalling the Swivel Integration

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

# 276 Troubleshooting
# 277 Known Issues and Limitations

# 278 Additional Information

# 279 F5 APM Integration

## 280 F5 Big-IP Access Policy Manager (APM) Integration Notes

This article describes how to integrate the F5 Big-IP Access Policy Manager with Swivel. The article covers two aspects:

- the integration of the two servers so that the F5 uses Swivel as its RADIUS server
- the modification of the F5 login page to include the TURing image or other Swivel elements as required.

# **281 RADIUS Integration**

To use Swivel with F5 Big-IP you need to enable the Radius Server on Swivel. (On the RADIUS->Server page)

A NAS Entry then need to be created that includes the F5 server IP address/hostname and a shared secret.

The associated configuration then needs to be created on the F5 server.

This is done on the Access-Policy->AAA-Servers screen.

/ <b>©</b> I	BG-D® - P5.swiveldev.loc 🗴 🔪		
÷	→ C B https://f5console.s	wiveldev.local/xui/	
B W	eb Slice Gallery 🕌 Suggested Sites	()]] Imported From IE	
Host IP.Ac	rame <b>F5.swiveldev.local</b> Date: M ddrass: 192.168.68.199 Time: 4:	ar 13, 2013 – User - <b>admin</b> 36 FM (GMT) – Role: Administrator	
f.	ONLINE (ACTIVE) Standalone Provisioning Warning		
00	lain Helo Acout	Access Policy » AAA Servers	a llen Server
凸	Statistics		
m	iAnn	General Properties	
199	արին	Name	
	Wizards	Туре	RADIUS
PA	Local Traffic	Configuration	
		Mode	O Authentication O Accounting O Authentication & Accounting
	Access Policy	Server Connection	💿 Use Pool 🔘 Direct
	Access Profiles	Server Pool Name	
	AAA Servers >		Add
	ACLs		
	SSO Configurations	Server Addresses	
	SAML		
	Webtops >		The Deven Delate
	Secure Connectivity	Daaraa Daal Massiaa	
	Network Access	Server Pool Monitor	none 7
	Application Access	Authentication Service Port	1812
	Portal Access	Secret	
	Manage Sessions	Confirm Secret	
	Reports	MAS IP Address	
	Oustomization >	THE REAL FOR	
	Dashboard .=	MAS IPV6 Address	
	Dovico Mananomont	MAS Identifier	
	and management	Timeout	5 seconds
	Network	Retries	3
87	System	Samice Type	Default

Once this entry has been created it can be used when defining Access Profiles.

It is important to remember the name of the profile created as this will be required for the customisation.

### 281.1 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.

## 282 Logon page Customisation

Once you have configured your access policy, you need to modify the logon page. You can edit it from the management console as follows:

From the Main menu, select Access Policy, then Customization. From the View dropdown, select Advanced Customization. From the folder tree, select Customization Settings -> Access Profiles -> [Your access profile] -> Access Policy -> Logon Pages -> Logon Page -> logon.inc.

#### Search for the line

function OnLoad()

#### Insert the following immediately before it:

#### For TURing image:

```
// **** PINsafe Customisation Start ****
 // Change this to match the PINsafe image URL.
var imageUrl = "https://<your_swivel_server>:8443/proxy/SCImage?username=";
 function ShowTuring() {
     var usernameField = document.getElementById("input_1");
if (usernameField && usernameField.value && usernameField.value != "") {
          var img
if (img)
                           = document.getElementById("turing_img");
              img.style.display = "";
img.src = imageUrl + usernameField.value + "&random=" + Math.floor(Math.random()*10000);
 // **** PINsafe Customisation End ****
Or for PinPad:
  // **** PINsafe Customisation Start ****
 // Change this to match the PINsafe image URL.
var imageUrl = "https://<your_swivel_server>:8443/proxy/SCPinPad?username=";
 function ShowPinPad() {
  var usernameField = document.getElementById("input_1");
  if (usernameField & usernameField.value & usernameField.value != "") {
   var padno = Math.floor(Math.random() * 100000);
                   (var i=0; i<10; i++)
          for
              var ing = document.getElementById("pinpad" + i);
if (img) {
  var url = imageUrl + usernameField.value + "&padno=" + padno + ":" + i;
                   img.src = url;
              }
          }
     }
  }
 function InsertPinPad() {
      var footerCell = document.getElementById("credentials_table_footer");
      if (footerCell) {
          var footerRow = footerCell.parentNode;
var formTable = footerRow.parentNode;
         var formTable = footerCerl.parentNode;
var formTable = footerCerl.parentNode;
var pinpadRow = document.createElement("t");
pinpadCell = document.createElement("td");
pinpadCell.setAttribute("align, "center");
var pinpadTable = document.createElement("table");
pinpadTable.style.height = "225px";
pinpadTable.style.width = "150px";
var row, cell, img;
for (var r=1; r<=9; r+=3) {
  row = document.createElement("td");
  cell.setAttribute("align", "center");
  img = document.createElement("td");
  img = document.createElement("td");
  img .setAttribute("align", "center");
  img .setAttribute("align", "center");
  img.setAttribute("id", "pinpad" + c);
  img.setAttribute("id", "AddDigit(" + c + ")");
  cell.appendChild(cell);
  '''
                   row.appendChild(cell);
              pinpadTable.appendChild(row);
          row = document.createElement("tr");
          cell = document.createElement("td");
         cell = document.createsHement('td');
img = document.createsHement("img");
img.src = "images/refresh.png";
img.setAttribute("onclick", "ShowPinPad()");
```

cell.appendChild(img);

```
cell.appendChild(cell);
row.appendChild(cell);
cell = document.createElement("td");
cell.setAttribute("align", "center");
img = document.createElement("img");
img.src = "images/blank.png";
img.setAttribute("id", "pinpad0");
img.setAttribute("onclick", "AddDigit(0)");
cell.appendChild(img);
row_appendChild(cell);
 cell.appendchild(cell);
cell = document.createElement("td");
cell.setAttribute("align", "center");
img = document.createElement("img");
img.src = "images/clear.png";
img.setAttribute("onclick", "ClearOtc()");
```

```
cell.appendChild(img);
```

```
row.appendChild(cell);
      pinpadTable.appendChild(row);
pinpadCell.appendChild(pinpadTable);
pinpadRow.appendChild(pinpadCell);
      formTable.insertBefore(pinpadRow, footerRow);
}
// Check that the following field is correct. If PINsafe is the ONLY form of authentication,
// or is the first authentication, it will be "input_2".
// If it is the second authentication, it will be "input_3".
var otcFieldId = "input_2";
function AddDigit(digit) {
  var otcField = document.getElementById(otcFieldId);
  if (otcField) {
      otcField.value += digit;
   }
1
function ClearOtc() {
   var otcField = document.getElementById(otcFieldId);
   if
       (otcField) {
      otcField.value = "";
   }
l
// **** PINsafe Customisation End ****
```

#### A few lines below this are the following lines:

```
if( form == null ) {
    return;
}
```

#### Below this, insert the following for TURing:

```
// **** PINsafe Customisation Start ****
var footerCell = document.getElementById("credentials_table_footer");
if (footerCell) {
    var footerRow = footerCell.parentNode;
    var toringRow = document.createElement("tr");
    turingRow.setAttribute("id", "turing_row");
    var turingCell = document.createElement("td");
    turingCell.setAttribute("olspan", "2");
    var turingTell.setAttribute("align", "center");
    turingGell.setAttribute("id", "turing_row");
    var turingImg = document.createElement("img");
    turingTmg.setAttribute("id", "turing_ing");
    turingGell.appendChild(turingImg);
    var turingGell = document.createElement("br");
    turingGell.appendChild(turingImg);
    var turingBrk = document.createElement("br");
    turingBrk = document.createElement("input");
    turingBrk.setAttribute("value", "New Image");
    turingBrk.setAttribute("value", "New Image");
    turingRow.appendChild(turingBrw);
    turingRow.appendChild(turingRow, footerRow);
    }
    // Optional: to automatically show the TURing after entering the username, include the following lines.
    var usernameField = document.getElementById("input_1");
    if (usernameField = document.getElementById("input_1");
    // optional: to tautomatically show the TURing after entering the username, include the following lines.
    var usernameField.onblur = ShowTuring;
    // Optional: if the username is pre-populated, use the following line to display the TURing image immediately
    ShowTuring();
    // ***** PINsafe Customisation End ****
```

#### or this for Pinpad:

```
// **** PINsafe Customisation Start ****
InsertFinFad();
// The next section is optional - use this if you want to show the TURing automatically when the username changes.
var usernameField = document.getElementById("input_1");
if (usernameField) {
    usernameField.onblur = ShowPinPad;
    }
// **** PINsafe Customisation End ****
```

### 282.1 Removing the Automatic TURing image

#### Remove or comment out the following lines with // at the front

```
// Optional: to automatically show the TURing after entering the username, include the following lines.
var usernameField = document.getElementById("input_1");
if (usernameField) {
    usernameField.onblur = ShowTuring;
}
```

#### For Pinpad, the penultimate line above will be

```
usernameField.onblur = ShowPinPad;
```

The final step here is to set the image URL. There are a number of options:

- The simplest option is to use the Swivel Server directly. However, this requires that the Swivel Server is directly accessible from the internet, which is not a recommended solution, as it is a security risk. Also, you will need a commercial SSL certificate on the Swivel server to avoid problems with certificate errors. In this case, simply replace *<your_swivel_server>* above with the external URL of your Swivel Server.
- The second option is to create a virtual server on the F5 Big-IP to act as an anonymous proxy to the Swivel Server. This is suitable if the F5 is your only Swivel integration, as it requires that the F5 is set as the default gateway for your Swivel appliance. Details for this are not provided, as it should be clear from the F5 documentation how to do this. You might also want to create an iRule to restrict access only to the TURing image, as suggested below. In this case, you should replace <*your_swivel_server>* with the external URL of your F5. If you have set up the virtual server with a different service port, you might need to change this as well.

```
when HTTP_REQUEST {
    if { [HTTP::uri] starts_with "/pinsafe/SCImage?" } {
        pool PINsafe_8080
    } else { HTTP::respond 403 }
}
```

• The third option is suitable if you have other Swivel integrations. In this case, you can use the URL of the TURing image on the other integration to deliver the TURing image. For example, if you have an integration with Outlook Web Access, use the following:

var imageUrl = "https://<your_swivel_server>/owa/auth/SCImage.aspx?username=";

Here, replace <your_swivel_server> with the URL of your OWA server.

Another example: if you have a UAG integration, use the following:

var imageUrl = "https://<your_swivel_server>/InternalSite/images/customupdate/images.asp?username=";

NOTE: If you are using Pinpad, substitute SCPinPad for SCImage above.

# 283 Testing

Now when the F5 server is accessed via the **pinsafe** access policy the user should see a modified login page with the option to request a TURing image.

The user should enter their username and see a TURing image when the click the TURing button. At this point a Session Start message for the user should show in the PINsafe logs.

If no image shows, check that the URL is correct and ensure that there is no firewalls blocking the request.

Also check that Session Create by Username is enabled on the Swivel server.

The user should then enter their one-time code. The login.

If the log-in fails, check the Swivel log files to see if a RADIUS request was logged. If not then check the settings for the RADIUS on F5 and Swivel to ensure IP Addresses, port numbers and shared secrets all match. Also check that no firewalls are blocking the RADIUS requests.

If RADIUS attempts are being logged but authentication is failing, check that the session was started correctly and that there is no password associated with the account etc.

## 284 F5 Firepass Integration

### 284.1 Introduction

This document outlines the steps required to integrate the F5 Networks FirePass SSL VPN with the Swivel PINsafe authentication server.

FirePass VPN appliances are able to use external RADIUS servers for providing authentication. The PINsafe server provides RADIUS authentication, thus the FirePass VPN can be configured to use the PINsafe server for authentication via RADIUS.

PINsafe users can use either PINsafe?s Single Channel (TURing, PATtern) or Dual Channel (SMS, Swivlet applet) 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 FirePass VPN configured to use the matching PINsafe server for RADIUS authentication, no further integration is required.

However with Single Channel methods, the user must be presented with a TURing or PATTern image upon login (representing a single time-limited Security String), so they can extract their OTC. The Authentication configuration section below describes how to achieve the RADIUS configuration. Single Channel requires access to the PINsafe server by a Public IP address.

### 284.2 Prerequisites

### 284.2.1 Baseline

The FirePass VPN appliance tested was FirePass 600. (http://www.f5.com/products/FirePass/FP600.html)

The PINsafe server used was PINsafe v3.1. However, no changes have been made to PINsafe since then which would render the integration invalid.

The primary web browser used for testing was Internet Explorer 6.0.2900.2180.xpsp_sp2_gdr.050301-1519.

### 284.3 Architecture

The user connects to the FirePass VPN using a web browser, pointing to the appropriate login URL for the VPN in question.

The FirePass VPN is configured to use a PINsafe server for RADIUS authentication.

Users are stored and maintained in the PINsafe server.



Figure 1. The following diagram shows the configuration used and is typical. This example is used throughout this document:

### 284.4 Installation

### 284.4.1 PINsafe Configuration

Configuration of the PINsafe server for RADIUS authentication with the FirePass VPN consists of three steps:

- 1. Configure PINsafe RADIUS settings
- Set up the NAS (Network Access Server), which in this case is the FirePass VPN.
   Configure the PINsafe server to allow TURing/PATTern session creation with a username.

NOTE ? This document assumes that the PINsafe server has been configured to use a specific user repository and populated with users. Please refer to the PINsafe Administration Guide for detailed instructions.

### 1. Configuring PINsafe RADIUS settings

Configure the RADIUS settings using the RADIUS configuration page in the PINsafe Administration console. In our example (see diagram above) the RADIUS Mode is set to ?RADIUS Server? and the HOST IP (the PINsafe server) is set to 192.168.0.150.

Radius > Server 🕖		
Please enter the details for th	e <mark>PINsaf</mark> e RADIUS Server.	
Server Enabled:	Yes 🚩	· · · · · · · · · · · · · · · · · · ·
Enable Debug:	No ~	
Hostname:	pinsafeserver	
Host IP Address:	192. <mark>1</mark> 68.0.150	
Authorisation Port:	1812	
Accounting Port:	1813	
Maximum No. Session:	500	
Permit Empty Attributes:	No 🖌	
Additional RADIUS Logging:	Both 🕐	
Filter ID:	No 👻	
	Apply Reset	· · · · · · · · · · · · · · · · · · ·

Figure 2. PINsafe RADIUS configuration page.

#### 2. Setting up the NAS

Set up the NAS using the Network Access Servers page in the PINsafe Administration console. In our example (see Figure 3), the meaningful name ?FirePass VPN? has been assigned so it can be identified if you have more that one NAS configured. The IP address has been set to the IP of the VPN appliance, and the NAS secret assigned that will be used on both the PINsafe server and VPN RADIUS configuration.

<center> Figure 3. Extract from PINsafe NAS setup page

Radius	s>NAS 🔘		
Please e	enter the detai	Is for any RADIUS NAS.	S.A
MAS:	Identifier:	FirePass VPN	cincincincincincin
	IP Address:	192.168.0.100	
	Secret:	000000	
		Apply Reset	

#### 3. Configure the PINsafe server to allow TURing/PATTern session creation with a username.

The PINsafe server must be configured to allow a Single Channel session to be created by accessing a specific URL on the PINsafe server. The following URL would create a start a session and return the image for the user ?test?:

For a Swivel hardware or virtual appliance http://Swivel_IP:8443/proxy/SCImage?username=test

For a software only install see Software Only Installation

#### </center>

### 284.5 F5 Networks FirePass VPN Configuration

The RADIUS FirePass configuration is found under Users, Groups, Master Groups, Radius_Users, and then the Authentication tab. The Primary RADIUS server was set to the IP address of the PINsafe server followed by the authorization port (see Figure 5). The shared secret entered was the same secret entered in the PINsafe NAS entry (see Figure 3).

If you want to configure a secondary PINsafe RADIUS server for failover you would add the details of the server in the ?Secondary RADIUS server? section on this page. If you are utilizing the High Availability PINsafe solution, failover/redundancy is managed by that solution, thus you would only enter the Primary RADIUS server address.

Figure 4. Extract from FirePass RADIUS Authentication setup page

	RADUS A	uthendication	
		Convert authentication method»	n galantan kara da kar
	RADIUS settin	]]3	
Timeout:	5		
Retries:	5		101100-00-00-00-00-00-00-00-00-00-00-00-
Service Type (optional)	: Default 🛛 🗸		and the state of the second state of the secon
	Primary RADIUS s	31/131	
Server:	192.158.0.150		
Port:	1812		
Change Sharad Secret:			
Sharad Secret:			And a second sec
Confirm Shared Secret			
	Retrieve Single Sign Or Use a secondary RADII	n Password from RADIUS attribute US server	

### 284.6 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 PADIUS success or rejected message. RADIUS server is started and that the correct ports are being used.

### 284.7 Modifying the FirePass login page for PINsafe TURing image

The PINsafe sends Security Strings to users via SMS, Swivlet applet (Dual Channel) or through a TURing image (Single Channel) accessed by public IP address from the PINsafe server. The user extracts their One Time Code (OTC) from the Security String and enters it into the VPN sign-in. If the user has been assigned a PINsafe server static password, they must enter the password plus their OTC. For example, if the user?s PINsafe static password was ?foobar? and their OTC were 7452, they would enter ?foobar7452? at the login prompt.

If the PINsafe user were configured to use Dual Channel (SMS or applet), they should have a security string ready on their mobile device. No modification to the FirePass login page would be required. For Single Channel users, we need some way of presenting a TURing image on the FirePass VPN?s login page. This can be achieved through configuration of the FirePass login screen via WebDAV.

#### To enable WebDAV based customization

- Create an HTTP web service on the Device Management : Configuration : Network Configuration : Web Services screen.
   Select the Allow insecure access option on the Device Management : Security : User Access Security screen.
   Check Allow WebDAV sandbox customization on the Device Management : Customization screen and enter a WebDAV password in the text box that appears.

The WebDAV sandbox is accessed via HTTP at the URI /sandbox as the user webdav. So, for example, if the FirePass controller has been configured using the steps above with a HTTP web service at 192.168.0.99, you would use the URL http://192.168.0.99/sandbox/.

Any content can be placed in the sandbox directory. The FirePass controller uses specific files to override or supplement stock system behavior. To add the TURing image to the right of the logon prompt, the right.inc file was created and added to the sandbox, with the following content:

<script language="JavaScript">

</script>

<input name="btnTuring" type="button" value="OTC Image" class="submitbutton" onclick="ShowTuring()" />

<img id="imgTuring" style="visibility:hidden;" alt="Turing image" />

Edit the following line with the correct IP address

#### sUrl="http://192.168.0.150:8443/proxy/SCImage?UserName=";

For PINsafe 3.1.3a and later the following line needs to be edited:

sUrl="http://192.168.0.150:8443/proxy/SCImage?username=";

To upload the WebDAV pages browse to the sandbox with a web browser using http (not https) and enter the WebDAV username and password. Once loaded into the sandbox, the login page should contain a new button and the ability to display the TURing image.





### 284.8 Verifying Installation

Navigate to the F5 interface login page. The customisation is visible in the addition of a **One Time Code Image** button. Only when a correct PINsafe one time code is entered should the user be logged in. This can be done either by entering the OTC for a dual channel login, or selecting OTC Image and entering the OTC for a single channel login.

### 284.9 Troubleshooting

Check the PINsafe logs for any failure information.

### 284.10 Additional Information

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

# 285 F5 SAM Integration

## 286 F5 Secure Access Manager (SAM) Integration Notes

This article describes how to integrate the F5 Secure Access Manager with Swivel. The article covers two aspects:

- The integration of the two servers so that the F5 uses Swivel as its RADIUS server
- The modification of the F5 login page to include the TURing image or other Swivel elements as required.

# **287 RADIUS Integration**

To use Swivel with F5 SAM you need to enable the Radius Server on PINsafe. (On the RADIUS->Server page)

A NAS Entry then need to be created that includes the F5 server ip address/hostname and a shared secret.

The associated configuration then needs to be created on the F5 server.

This is done on the Access-Control->AAA-Servers screen.

Main	1	Help		Search		Access Control >>	AAA Serve	rs » S	wivel_Server	
	Overv	ew Traffi				Properties				
<u>lu</u>	Report	s, Perforn	nance,	Statistics	•	General Properties				
2	Local Virtual	Traffic Servers.	Profiles	s, iRules,		Name	5	Swivel_Se	rver	
U	SNATS	, SSL Cer	tificate	s		Туре	F	RADIUS		
	Acces	s Control	files			Configuration				
0		AAA Se	rvers		+ +	Host		10.100	.1.131	
		ACLS	Gatewa	ys	+	Service Port		1812		
0	Secur	Connec	tivity			Secret		•••••	••••	
3	Netwo	Pools, He k Access	source	Groups,	à.	Confirm Secret		•••••		_
_	Netwo	rk				NAS IP Address		10.100	.2.12	
	Filters, VLANs System	Spanning , ARP	g Tree,	Trunks,		Server Settings				
<b>†</b>	Licens	ing, Platfo	ives, P	gh 'referenci	as.	Timeout	ſ	5	seconds	
	SNMP,	Logs, Us	ers, Co	onsole	· ·	Retries	ſ	3	-	
						Service Type	I	Default	I	
						Update Delete	)			

Once this entry has been created it can be used when defining Access Profiles.

It is important to remember the name of the profile created as this will be required for the customisation.

### 287.1 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.

## 288 Log-in page Customisation

To modify the log-on page to include a TURing image you need secure-shell access (SSH) to the server.

Assuming that the Access Profile is called **pinsafe** the modifications are implemented by editing the file

/config/customization/advanced/logon/pinsafe_act_logon_page_ag/logon_en.inc

The steps are as follows.

1. Change directory to the required location

cd /config/customization/advanced/logon/**pinsafe_**act_logon_page_ag

2. Take a back-up of the existing file. Note that this example assumes that the Access Policy uses English. If another language is specified then you need to edit the corresponding file, eg log_fr.inc for French.

cp log_en.inc tmp_logon_en.inc

3. Edit the login file or copy a modified version of the file onto the server.

An example modified script is shown here. The required modifications are between the lines of asterisks. The setting of the sUrl variable needs to correspond to the PINsafe server being used.

4. To register the changes the following commands must be executed.

b customization group pinsafe_act_logon_page_ag action update b profile access pinsafe generation action increment

# 289 Testing

Now when the F5 server is accessed via the **pinsafe** access policy the user should see a modified login page with the option to request a TURing image.

The user should enter their username and see a TURing image when the clcik the TURing button. At this point a Session Start message for the user should show in the PINsafe logs.

If no image shows, check that the URL is correct and ensure that there is no firewalls blocking the request.

Also check that Session Create by Username is enabled on the PINsafe server.

The user should then enter their one-time code. The login.

If the log-in fails, check the Swivel log files to see if a RADIUS request was logged. If not then check the settings for the RADIUS on F5 and Swivel to ensure the IP Addresses, port numbers and shared secrets all match. Also check that no firewalls are blocking the RADIUS requests.

If RADIUS attempts are being logged but authentication is failing, check that the session was started correctly and that there is no password associated with the account etc.

290 Fortinet Fortigate Integration

# **291 Introduction**

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

## **292 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.

# 293 Baseline

Fortinet 3.x

Fortinet 4.x

Fortinet 6.x

Swivel 3.x

Swivel 4.x

## 294 Architecture

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

# **295 Swivel Configuration**

## 295.1 Configuring the RADIUS server

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

### 295.2 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.

## 296 Fortinet Fortigate Configuration

296.1 Fortinet FortigateVersion 3.x Integration guide

PINsafe'	SWIVEL
Fortigate SSL VPN 3.x With PINsafe Installa	ation Notes
Table of Contents Portgate SSL VIPN 3.x With PINasfe Installation Notes I. Introduction 2. Overview	
2.1. Prerequisites	
2.2. Baseline	
2.3. Architecture	
3.1. Configuring the PDNsafe server	
3.2. Configuring the Fortigate SSL VPN	
3.3. Integrating PINsafe into login screens	
3.4. Modifying the SSL login screen to integrate with the PINs	de Servert
3.5. Example SSL VPN login pages. Display Turing request botton and Turing image	
3.6. Turing Display Script	***************************************
3.7. On Demand Request for one time Security String	
3.8. On demand script	
6. Known haues and Limitations	
7. Additional Information	P
Fortigate SSL VPN 3.x With PDNsafe Installation Notes	Page 1 of 14
Number 24 Develop 02 9000	Undated: 26/01/2011

### 296.2 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.

System		
Router	Name	Swivel
Firewall	Primary Server Name/IP	192.168.1.2
UTM	Primary Server Secret	•••••
VPN	Secondary Server Name/IP	192.168.1.3
User	Secondary Server Secret	•••••
User User Authentication	Authentication Scheme	Use Default Authen O Specify Authenticat MS-CHAP-v2
Remote	NAS IP/Called Station ID	
<ul> <li>LDAP</li> <li>RADIUS</li> <li>TACACS+</li> <li>Directory Service</li> <li>Monitor</li> </ul>	Include in every User Group	Enable

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.

System		
Router	Name SSLVPN	
Firewall	Type   Firewall  Directory Service	
UTM	Allow SSL-VPN Access web-access	
VPN	Available Users	
User	- Local Users -	6
User User Authentication User Group User Group	swivel user	
E CORECTERATE LDAP RADIUS TACACS+	Remote authentication servers Add	
E 🛐 Directory Service	Remote Server	G
🗄 🗐 Monitor	Swivel	

## 296.3 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

FortiGate 100E	FW_GSW			
🚯 Dashboard	>	Edit RADIUS Server		
X Security Fabric	>	Name	Swivel_Pinsafe	
<ul> <li>Network</li> <li>System</li> <li>Policy &amp; Objects</li> <li>Security Profiles</li> <li>VPN</li> <li>User &amp; Device User Definition</li> </ul>	> > > > > > > > > > > > > > > > > > > >	Primary Server IP/Name Primary Server Secret Secondary Server IP/Name Secondary Server Secret Authentication Method NAS IP Include in every User Group	10.1.2.3  Default Specify	Test Connectivity Test Connectivity
Guest Management Device Inventory Custom Devices & Gro	oups			ОК
Single Sign-On LDAP Servers	~			Test RADIUS Connectivi
Authentication Setting FortiTokens	gs			Successful
🕍 Log & Report 🔇	>			

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.

FortiGate 100E	FW_GSW				
🚯 Dashboard	>	Edit User O	Group		
<ul> <li>Security Fabric</li> <li>FortiView</li> <li>Network</li> <li>System</li> <li>Policy &amp; Objects</li> <li>Security Profiles</li> <li>VPN</li> </ul>	> > > > > > > > > > > > > > > > > > > >	Name Type Members	swivel Firewall smith a +	××××	
🛔 User & Device	~	Remote G	roups		
User Definition		+ Add	🖋 Edit 📋 Delete		
User Groups	☆			Remote S	erver
Guest Management		Swive	el_Pinsafe		
Device Inventory Custom Devices & Gr	roups				ок
Single Sign-On LDAP Servers RADIUS Servers Authentication Settin	ngs				
FortiTokens					
Log & Report	>				
Monitor	>				

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

10000						
FortiGate 100E	FW_GSW					
🚯 Dashboard	>	Edit Policy				
🔆 Security Fabric	>					
🕍 FortiView	>	Name 🚯	swivel			
🕂 Network	>	Incoming Interface 🛆		<b>x</b> 100		
System	>	Outgoing Interface	T.			
Policy & Objects	~	Outgoing interface	m porti +	×		
IPv4 Policy	☆	Source	SSLVPN_TUNNEL_ADDR1	×		
Addresses			🖬 swivel	×		
Internet Service Datab	ase		+			
Services		Destination	10.1.2.0/29	×		
Schedules				×		
Virtual IPs				×		
IP Pools				×		
Security Profiles	>		+			
D VPN	>	Schedule	lo always	•		
🛔 User & Device	>	Service	ALL	×		
🔟 Log & Report	>	Action				
C Monitor	>	Action	ACCEPT O DENT IS LEAK			
		Firewall / Network Opt	ions			
		Security Profiles				
		SSL/SSH Inspection				
		Logging Options				
		Log Allowed Traffic C	Security Events All Sessions			
		Comments Clone of	Remote_SSL_Users .:: 25/1023			
		Enable this policy 🕥				
		A This policy ma • Remote	y be a duplicate of these existing poli _SSL_Users (13)	icies:		
0						

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					
B Dashboard	>	SSL-VPN Settings				
Security Fabric	>	Connection Settings	6 <b>()</b>			
FortiView	>	Listen on Interface(	s)	や RemoteAccess (SSLVPN)	×	
+ Network	>			T		
System	>	Listen on Port		10443		
Policy & Objects	>			Web mode access will be	listening at <u>ht</u>	ttps://x.x.x.x:104
Security Profiles	>		_			
	~	Redirect HTTP to SS	SL-VPN O			
IPsec Tunnels		Restrict Access		Allow access from any host	imit access to	specific hosts
IPsec Wizard		Idle Logout	•		_	
IPsec Tunnel Templa	tes	Inactive For		300	Seconds	
SSI-VPN Portals		Server Certificate		Fortinet_Factory	-	
SSL-VPN Settings	습			You are using a default bu	ilt-in certifica	ate, which will not b
SSL-VPN Personal Bo	ookmarks			your server's domain nam	e (your users	will see a warning)
SSL-VPN Realms				use.	e a certificate	e for your domain a
Luser & Device	>			Click here to learn more		
Log & Report	>					
Monitor	>	Require Client Certi	ificate 🔿			
		Tunnel Mode Client	Settings 0			
			octango o			10
		Address Range		Automatically assign address	25 Specify c	Sustom 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 Serve	rs O	)		
		Allow Endpoint Reg	istration (			
		Authentication/Por	tal Mapping	0		
		+ Create New	/ Edit	Delete		
			Users	/Groups	Realm	
		UNI			/	full-access
		swivel			/	full-access
		All Other Users/G	roups		1	web-access
Q						

### 296.4 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.

## 297 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

### 297.1 Forticlient

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

FortiClient SSLVPN		X		
			9	5 '9 ' 5 ' 5 ' 5 ' 5 ' 5 ' 5 ' 5 ' 5 ' 5
			MRIMINAL IN	5. (14.19 
		1		
Connection Name: Swivel		7		
Server Address: 192.168.1.91				
Usemame: graham			and and the second	
Password: assuments				
Dient Cartificale:		7		
- Comection-				
Status: Disconnected Bytes	Sent:	0		
Duration: 00:00:00 Byles	Received:	0		
Salings	Disconnect E	xit 🔤		

### 297.2 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

# 298 Testing

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

Example TURing login page

Please Login		
Name	USEY	
Password;		
	Login	
	1 2 3 4 5 6 7 8 9 0	
Get Image:	\$ 7 1 4 5 2 0 8 2 9	

### Example security string index login for Mobile or for SMS

Please Login		
Eane	user	marin an american
Passwowle		
	Login	
Mobile client index:	00	
		Constant Constant Announce of the state of t

# 299 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.

# **300 Known Issues and Limitations**

None

## **301 Additional Information**

PINsafe'	SWIVEL
Fortigate SSL VPN 4 With PINsafe Installat	ion Notes
Table of Contents Portgue SSL VPN 4 With PINsade Installation Notes Libroduction 2. Overview	
2.1. Prerequisites	
2.2. Baseline	
2.3. Architecture	
3.1. Configuring the PINsafe server	
3.2. Configuring the Fortigate SSL VPN	
3.3. Integrating PINsafe into login screens	
3.4. Modifying the SSL login screen to integrate with the PINs	ale Server
3.5. Example SSL VPN login pages. Display Turing request botton and Turing image	
3.6. Turing Display Script	
3.7. On Demand Request for one time Security String	
4. Verifying the Installation 5. Troubleshoring 6. Known Issues and Limitations 7. Additional Information	11 11 11
Fortigate SSL VPN 4 With PilNsafe Installation Notes	Page 1 of 1
Valuet: 2.2 Crosted: 02 2006	Oberation: 54-02-5013

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

# 302 HOB Remote Desktop VPN

## **303 Introduction**

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

## **304 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

## 305 Baseline

PINsafe 3.7 HOB RD VPN WebSecureProxy 2.2 0108

## **306 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.

## **307 Swivel Configuration**

### 307.1 Configuring the RADIUS server

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

### 307.2 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.

### 307.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

## 308 HOB RD VPN WebSecureProxy Integration

### 308.1 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.

🤣 HOB RD VPN WebSecureProxy [w	/sp\wsp.xml]		_ 🗆 🗙
<u>F</u> ile <u>H</u> elp			
wsp\wsp.xml	RADIUS Server		
WSP - O WSP(1) Connections - O SELECT	Name:	PINsafe	
Server Lists  SERVERLIST1  O Windows Terminal S  O Telnet 3270	Host IP Address:	192.168.1.100	
<ul> <li> <ul> <li></li></ul></li></ul>	Port:	1812	
Servers	Use network adapter:	Any	-
<ul> <li>Oser Group(1)</li> <li>Target Filters</li> </ul>	Timeout (sec):	15	
Add Remove	Shared Secret:	•••••	Show

### 308.2 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.

Incoming Connection	Outgoing Connection	SSL Au	thentication
Use authentication	common name	DIUS Servers	
User Group(1)			Chec <u>k</u> All Cl <u>e</u> ar All
RADIUS Servers			Chec <u>k</u> All Cl <u>e</u> ar All
Authorize user Cert	tificate		
	Incoming Connection Use authentication Check certificate's o User Groups User Group(1) RADIUS Servers RADIUS Servers EA_SERVER PINsafe Authorize user Certificate	Incoming Connection       Outgoing Connection         Use authentication       RA         □ Check certificate's common name       User Groups         ☑ User Groups       ☑         ☑ User Group(1)       ☑         RADIUS Servers       ☑         □ EA_SERVER       ☑         ☑ PINsafe       ☑         □ Authorize user Certificate	Incoming Connection Outgoing Connection SSL Au   Use authentication RADIUS Servers   Check certificate's common name   User Groups   Image: User Group(1)     RADIUS Servers   EA_SERVER   Image: PINsafe   Authorize user Certificate

### **308.3 Additional Installation Options**

#### 308.3.1 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.

#### 308.3.2 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 the mobile phone to change their PIN. If a PINsafe password is being used, they must use <password><OTC>.

HOB RD VPN Login	3
Please enter the specified challenge code into your token device. Then enter the displayed code into the field "Response:". Challenge in progress	
changepin	
Old OTC:	
••••	
New OTC:	
••••	
TURing Index Message	
1 2 3 4 5 6 7 8 9 0 8 2 0 9 4 7 6 5 1 3	
Login	

#### 308.3.3 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.

# 309 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.

HOB RD VPN Login	
Enter your Username and Password to login now.	
User Name:	
graham	an a secondar i terreta i terreta i
Password;	
0000	
TURing Index Message	
Login	

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

HOB RD VPN Login	â	
Enter your Username and Password to login now.		
User Name: graham		
Password:		
TJRing Index Nessage		
2374325732		
Login		

	and a second
	Martin Martin a martina
LINE OF MONIL AMIN	
ume um alu moâni	
	magy 20.2.2 - Organ day - Store
Enter your Username and Password to login now.	
0)N)	187 - per automatique per terre
User Mame;	10000000000000000000000000000000000000
graham	
	grantin gaining and
Password:	
0000	ALL WARDS IN THE ALL AND ALL A
TIDing Jacky Managan	An orall of the second
LAKIKI Maszalla	
0 0 0 1 2 1 2 0 0 0	
	the state of the second second
Las her and a total	X TO ADRESS OF THE PARTY OF THE
0 51 4 50 9 2 2 2	
	and the second second second second second second
Logia	
r o fin	the second s
	Sector And Party of

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.

HOB RD VPN Login	
Enter your Username and Password to login now.	WORK STATISTICS IN THE SECOND STATES
User Name:	and a second
Password:	<u></u>
DDDD Index Nessage	nand-the sector se
00	Staff Shares and the state of t
Login	

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

	tannarata.
uad ve alu eaîm	harrades etc. Arrest
Enter your Username and Password to login now.	
Authentication Error: WSP's query failed.	
User Name:	
Password:	
TURing Index Message	
Login	

# **310 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.

# **311 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.

# **312 Known Issues and Limitations**

# **313 Additional Information**

# 314 Juniper ChangePIN

## **315 Introduction**

This document outlines how to integrate the Swivel ChangePIN with Juniper. See also RADIUS ChangePIN and ChangePIN How to Guide

# **316 Prerequisites**

Swivel Server Juniper SSL VPN version 6 or 7 OS. Modified Changepin page for version 6 Modified Changepin page for version 7

## 317 Baseline

Juniper SA 2000 JunOS 6 or 7.

Swivel 3.8

## **318 Architecture**

A user authenticates against the Juniper server, which passes the RADIUS authentication to the Swivel server. If the user is required to Change their PIN the Swivel server responds with a RADIUS Challenge, and the user is redirected to a change PIN page.

## 319 Installation

Configure the Swivel and Juniper so that they are fully working together, see Juniper SA 6.x Integration or Juniper SA 7.x Integration or Juniper SA 8.x

### **319.1 Swivel Integration Configuration**

On the Swivel Administration Console select RADIUS then NAS and edit the required Juniper NAS entry Change PIN Warning to Yes, then apply the settings.

NAS:		
	Identifier:	Juniper
	Check Password with repository:	No 🔻
	Username attribute for repository:	
	Allow alternative usernames:	No 🔻
	Alternative username attributes:	
	Hostname/IP:	192.168.0.100
	Secret:	•••••
	Group:	ANY +
	EAP protocol:	None -
	Authentication Mode:	All 🗸
	Vendor (Groups):	None -
	Change PIN warning:	Yes 🕶
	Two Stage Auth:	No 👻

### **319.2 Juniper ChangePIN Integration**

Download the login page and add the modified ChangePIN page given above under prerequisites, rename and edit as appropriate, add to the zip file and upload to the Juniper server.

#### 319.2.1 Juniper ChangePIN page options

#### Edit the following options:

var OTC_OPTION = "image"; // button, image, disable

image When the user tabs down from the username field, the TURing will automatically show, used for Single Channel access

button The login page will present a TURing button. Click the button to display the TURing, used for Single or Dual Channel access

disable The TURing image will not be shown, used for Dual Channel access.

TURingImage: Is the URL used to generate a TURing image. This should point to the internal IP address of the appliance var TURingImage = "https://turing.swivelsecure.com/proxy/SCImage?username=";

#### 319.2.2 Juniper RADIUS Custom rules

On the Juniper Administration console select the Swivel RADIUS server and create a Custom RADIUS rule with the following settings:

Name: ChangePIN Response Packet Type: Access Challenge Attribute Criteria: RADIUS Attribute Reply-Message (18) Attribute Criteria: Operand Matches the expression

#### Value: changepin

Action: use the appropriately modified page; Show Next Token page or show New Pin Page

Name	Response Packet Type	Attribute criteria
<u>ChangePIN</u>	Access Challenge	(Reply-Message matches the expression "change

### **319.3 Additional Installation Options**

#### 319.3.1 Combining Swivel and RSA RADIUS changePIN

Where Swivel is acting as a proxy RADIUS server for RSA authentication, Swivel can proxy the RADIUS request.

Configure the Swivel RADIUS proxy so that it will authenticate RSA users, see RADIUS Proxy How to guide.

On the Juniper edit the Swivel RADIUS authentication setting to add an additional custom rule with the following settings:

Name: RSAChangePIN

Response Packet Type: Access Challenge

Attribute Criteria: RADIUS Attribute Reply-Message (18)

Attribute Criteria: Operand does not match the expression

Value: changepin

Action: show Generic Login page

Apply the settings

Auth Servers > Cohort > Edit Custom Radius Rule			
Name: RSAChangepin			
If received Radius Response Packet			
Response Packet Type: Access Ch	allenge 👻		
Attribute criteria:			
Radius Attribute	Operand	Value	
Reply-Message (18) 🔹	matches the expression 🔹		Add
Reply-Message	does not match the expression	changepin	×
Then take action			
Show New Pin page			
Show Next Token page			
show Generic Login page			
Show user login page with error	or message		
<ul> <li>show Reply-Message attri</li> </ul>	bute from the Radius server to th	e user	
Sand Access Pequest with add	itional attributes		
De dive Attribute	Value		
Kadius Attribute	value		
User-Name (1)		Add	

Note: The Juniper displays the Generic login page as show Defender page

Name	Response Packet Type	Attribute criteria
ChangePIN	Access Challenge	(Reply-Message matches the expression "change
RSAChangepin	Access Challenge	(Reply-Message does not match the expression "

## 320 Verifying the Installation

Login as a Swivel user.

Set the user to be required to change their PIN, the user should be redirected to the ChangePIN page. The user will be required to enter their old OTC, and a new OTC based on what they want their PIN to be. This OTC could be from the TURing, SMS message or mobile app. Remember to never enter the Swivel PIN.

Where RSA authentication is being used, require the user to change their PIN, and they should be redirected to a RSA Change PIN page. The the first time a user accesses the system with a new token the user will be required to enter a new PIN. If the user wanted a PIN of 1234 the would enter 1234 in the box.

JUNIPEC	
Welcome to the	
Instant V	irtual Extranet
Challenge / Respo	nse
Challenge: Enter a r	new PIN having from 4 to 8 alphanumeric characters:
Enter the challenge stri	ng above into your token, and then enter the one-time response in the field below
Response:	
C. Barris	(Annu)
Sign in	Gancel

The RSA server then send a challenge asking for the PIN to be re-entered to confirm the user has not miss-typed it. The user would again enter 1234.

JUNIPEC	
Welcome to the	
Instant Virte	ual Extranet
Challenge / Response	
Challenge: Please re-ente	r new PIN:
Enter the challenge string abo	ve into your token, and then enter the one-time response in the field below
Response:	
Sign In Canc	

Once the user has successfully changed their PIN the RSA server asks them to login again with their new PIN plus token code. The user would enter 1234XXXXX where XXXXXX is the code displayed on the token.



If the RSA server sees the token go out of sync it will ask the user to enter their next token code. The user would now enter XXXXXX where XXXXXX is the next code displayed on the token after the code the user used to authenticate. They do not type their PIN at this stage.

Welcome to the	
Instant Vir	tual Extranet
Challenge / Response	
Challenge: Wait for tok	en to change, then enter the new tokencode:
Enter the challenge string a	bove into your token, and then enter the one-time response in the field below.
Response:	

# 321 Uninstalling the Swivel Integration

Remove the modified login pages and RADIUS customisation.
# 322 Troubleshooting

Check the Swivel logs for authentication, proxy and ChangePIN requests.

# 323 Known Issues and Limitations

Where Swivel and RSA change PIN is being used and the user is a Swivel and a RSA user, and dual channel authentication is being used, then the Change PIN will fail for RSA users. for single channel users not using dual channel authentication, the proxy server can be used to detect the presence of a single channel session being started.

# 324 Additional Information

# 325 Juniper OneTouch

## 326 Overview

This document is intended to supplement the the OneTouch Mobile guide and the OneTouch Voice guide for using the Swivel Juniper OneTouch Demo application.

## **327 Prerequisites**

Swivel 3.10.4

Juniper 7.x or 8.x

Nexmo Account (or other Telephony provider) for OneTouch Voice telephone-based solution

Latest version of the Swivel Appliance Proxy available from Downloads

Swivel OneTouch Application demo available from Downloads

Juniper Custom login pages OneStage.zip or TwoStages.zip

## 328 Baseline

(The version tested with) Swivel 3.10.4

Juniper 7.x

# 329 Architecture

See OneTouch Voice and OneTouch Mobile

## 330 Installation

#### 330.1 One Touch Demo Application Installation

Install the Swivel OneTouch Demo Application

#### 330.2 Swivel Integration Configuration

Configure the Swivel server and users as detailed in this guide OneTouch Voice or OneTouch Mobile.

#### 330.3 Juniper One Touch Integration

#### 330.4 Modifying the Custom login Pages

Modify the Juniper login pages either for OneStage or TwoStage authentication.

#### 330.4.1 For Single Stage authentication

Open the OneTouchOneStage.zip file Modify the LoginPage.thtml file edit the 2 URLs to access to your OneTouch demo app: e.g.: http://localhost:8081/onetouchdemo/onetouch?returnurl= Save the changes and create a zip. NOTE: the zip has to contain just the files and not the onetouch folder or itself a subfolder.

#### 330.4.2 For Two Stage Authentication

Open the OneTouch2Stages.zip file

Modify the Defender.thtml file

edit the URLs to access to your OneTouch demo app:

e.g.: http://localhost:8081/onetouchdemo/onetouch?returnurl=

Save the changes and create a zip. NOTE: the zip has to contain just the files and not the onetouch folder or itself a subfolder.

#### 330.5 Uploading the Custom Sign in pages

As with the Swivel Juniper integration, the custom pages need to be uploaded and assigned to a signing-in policy and realm.

Ensure all the modified files are included with the zip file to upload to the Swivel server. On the Juniper select Signing In/Sign-in Pages then click on Upload Custom Pages.

	r
Central Manager	
Central Manager System Status Configuration Configuration Network Clustering Log/Monitoring Authentication Signing In Endpoint Security Auth. Servers Auth. Servers Admin Realms Admin Roles Users	Signing In         Sign-in Policies         Sign-in Policies         New Page         Upload Custom Pages         Delete         Sign-In Page         Meeting Sign-In Page         Standard
User Realms >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	

Enter a Name for the Custom page, then use Browse to find the location of the Templates file. Then click on the Upload Custom Pages, observe any errors that may occur.

# 

Central Manager	
System Status Configuration Network Clustering Log/Monitoring Authentication	Signing In > Upload Custom Sign-In Pages Custom sign-in pages allow you to provide customized templates for various pages that appear during the sign-in process. Refer to the documentation for information about creating valid templates.
Signing In → Endpoint Security →	Sign-In Pages
Auth. Servers - Administrators	Name: PINsafe
Admin Realms → Admin Roles → ■ Users	Page Type: <ul> <li>Access</li> <li>Meeting</li> </ul>
User Realms >> User Roles >> Resource Profiles >	Templates File: C:\Documents and Setting Browse Zip file containing the custom templates and assets.
Resource Policies >	Upload
Maintenance System Import/Export Push Config Archiving Troubleshooting	skip validation checks during upload

The new signing in page should be listed.

# 

Central Manager		
- System		
Status >	Signing In	
Configuration +		
Network +	Sign-in Policies Sign-in Pages	
Clustering +		
Log/Monitoring +		
- Authentication	New Page Upload Custom Pages Delete	
Signing In 🔶 🕨		
Endpoint Security +	Sign-In Page	Туре
Auth. Servers		
- Administrators	PINsate	Cust
Admin Realms 🔸	Default Sign-In Page	Stan
Admin Roles 🔸	Meeting Sign-In Page	Stan
- Users		
User Realms →		
User Roles >>		
Resource Profiles +		
Resource Policies >		
- Maintenance		
System >		
Import/Export +		
Push Config		
Archiving >		
Troubleshooting +		

### 330.6 RADIUS Authentication Server Configuration

On the Juniper Server select Authentication Servers then select RADIUS Server from the drop down menu, and click on New Server.

Central Manager			
<ul> <li>System</li> <li>Status</li> <li>Configuration</li> <li>Network</li> <li>Clustering</li> <li>Log/Monitoring</li> <li>Clustering</li> <li>Log/Monitoring</li> <li>Authentication</li> <li>Signing In</li> <li>Authentication</li> <li>Signing In</li> <li>Endpoint Security</li> <li>Auth. Servers</li> <li>Admin Realms</li> <li>Admin Roles</li> <li>User Realms</li> <li>User Roles</li> <li>Resource Profiles</li> <li>Resource Policies</li> <li>Resource Policies</li> <li>Maintenance</li> <li>System</li> <li>Import/Export</li> <li>Push Config</li> <li>Archiving</li> </ul>	Authentication Server New: (Select server type) (Select server type) NE Authentication LDAP Server ANIS Server ACE Server ACE Server Active Directory / Windows Anonymous Server SiteMinder Server SiteMinder Server SAML Server	Vers	ete Type IVE Authenticatio IVE Authenticatio
Archiving → Troubleshooting →			

The following information is required:

Name: A descriptive name for the RADIUS server

**RADIUS Server:** The Swivel server IP/Hostname (Use the Swivel server real IP address not the VIP, multiple servers can be defined as Primary and secondary servers).

Authentication Port: the port used to carry authentication information, by default 1812

Shared Secret: The shared secret that has been entered on the Swivel server

Accounting Port: the port used to carry accounting information, by default 1813

NAS-IP Address: the Juniper interface used for communication, usually left empty

Users authenticate using tokens or one-time passwords Ensure this box is ticked

Backup server, Enter the details of any additional Swivel servers which can be used for authentication.

- Curtom			
	Auth Servers >		
Status >	PINsafe		
Naturation P			
Clustering	Sattings Lieore		
Log/Monitoring	Securitys Users		
- Authentication			
Signing In →	Name:	PINsafe	Label to reference this server.
Endpoint Security +	Padius Convert	92 60 104 105	Name of ID address
Auth. Servers	Raulus Server.	02.05.154.155	Name of IP address
- Administrators	Authentication Port:	1812	
Admin Realms →	Shared Secret:		
Admin Roles →	Accounting Ports	1813	Dert used for Padius assounting, if applicable
- Users	Accounting Port.	1013	Port used for Kadius accounting, ir applicable
User Roles	NAS-IP-Address:		IP address
Resource Profiles >			
Resource Policies >	Timoout	30	
- Maintenance	Timeouc.	seconds	
System >	Retries:	0	
Import/Export >			
Push Config	V Users authenticat	e using tokens or one	-time passwords
Archiving +	Note: If you select th	his IVE will send the user	's authentication method as "token" if you use SAM
Troubleshooting >	and this credential w	ill not be used in automat	tic SSO to backend applications.
	Backup server		
	Radius Server:		Name or IP address
	Authentication Port:		
	Shared Secret:		
	Accounting Bort		Part used for Padius accounting if applicable
	Accounting Port.		Porcused for Radius accounting, if applicable
	Padius assounting		
	Radius accounting		
	NAS-Identifier:		Name of IVE as known to Radius s

For Two Stage Authentication Go to the auth, select the server used for one touch and add a new challenge rule. The value has to be the same as configured on Defender.thtml and radius_challenges.txt on the Swivel core.

Example Rule:

Name: Challenge One Touch

Response Packet Type: Access Challenge

RADIUS Attribute: Reply-Message

Operand: matches the expression

Value: One Touch

ame: Challenge One Touch			
f received Radius Response Packet			
esponse Packet Type: Access C	hallenge 👻		
ttribute criteria:			
Radius Attribute	Operand	Value	
Reply-Message (18)	<ul> <li>matches the expression</li> </ul>	•	Add
Reply-Message	matches the expression	One Touch	×
an take action			
show New Pin page			
<ul> <li>show New Pin page</li> <li>show Next Token page</li> </ul>			
<ul> <li>show New Pin page</li> <li>show Next Token page</li> <li>show Generic Login page</li> </ul>			
<ul> <li>show New Pin page</li> <li>show Next Token page</li> <li>show Generic Login page</li> <li>show user login page with er</li> </ul>	ror message		
<ul> <li>show New Pin page</li> <li>show Next Token page</li> <li>show Generic Login page</li> <li>show user login page with er</li> <li>show Reply-Message att</li> </ul>	ror message tribute from the Radius server to	o the user	
<ul> <li>show New Pin page</li> <li>show Next Token page</li> <li>show Generic Login page</li> <li>show user login page with er</li> <li>show Reply-Message at</li> <li>send Access Request with access Re</li></ul>	ror message tribute from the Radius server to Iditional attributes	o the user	
<ul> <li>show New Pin page</li> <li>show Next Token page</li> <li>show Generic Login page</li> <li>show user login page with er</li> <li>show Reply-Message att</li> <li>send Access Request with ac Radius Attribute</li> </ul>	ror message tribute from the Radius server to Iditional attributes Value	o the user	

#### 330.6.1 Authentication Realm Configuration

Authentication realms determine which method of authentication will be used. On the Juniper select User Realms, and either create a new Realm with the New button or or modify an existing realm by clicking on it.

Junipe	e <b>r</b> °
Central Manager	
System Status Configuration Network Clustering Clustering Clustering Authentication Signing In Endpoint Security Auth. Servers Auth. Servers Admin Realms Admin Roles Users	User Authentication Realms   New   Duplicate   Authentication Realm   Users   Authentication realms specify what server to use for authentication, how policies are assigned to users.
User Realms > User Roles > Resource Profiles > Resource Policies > Maintenance System > Import/Export > Push Config Archiving > Troubleshooting >	

330.7 Additional Installation Options

# 331 Verifying the Installation

# 332 Uninstalling the Swivel Integration

# 333 Troubleshooting

# 334 Known Issues and Limitations

# 335 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.

# 336 Juniper SA 5.x Integration

#### 336.1 Overview

PINsafe can be integrated with the SA series of SSL VPN products, with the SA 2000 and higher products also allowing additional login page functionality.

Juniper SA 5.x Basic Integration Guide

Juniper SA 5.x files for modified login page

Juniper SA 5.x Enhanced Integration Guide

## 337 Juniper SA 6.x Integration

#### 337.1 Overview

PINsafe can be integrated with the SA series of SSL VPN products, with the SA 2000 and higher products also allowing additional login page functionality.

Juniper SA 6.x Integration Guide

#### 337.2 Troubleshooting

INFO RADIUS: <69> Access-Request(1) LEN=147 192.168.1.1:13145 Access-Request by ADMIN\graham Failed: AccessRejectException: AGENT_ERROR_NO_USER_DATA

INFO 192.168.1.1 Juniper:Login failed for user: ADMIN\graham, error: No data for the user was found.

Authentication has failed as the User Ream has been configured with <USER> instead of <USERNAME>

# 338 Juniper SA 7.x Integration

### 339 Overview

Swivel can be integrated with the SA series of SSL VPN products, with the SA 2000 and higher products also allowing additional login page functionality. Creating additional login pages allow different authentication methods and test pages to be created with different functionality. 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.

The SA 700 can be configured in a similar manner using RADIUS authentication except for the TURing image and other login page modifications.

For 6.x integration guide see Juniper SA 6.x Integration

For 8.x integration guide see Juniper SA 8.x Integration

It is also possible to configure Two Stage authentication whereby the user enters a username and AD Password and if correct the user can be sent a security string or OTC for Authentication. This can be combined with the Juniper Two Stage authentication to allow the AD Single Sign On (SSO) features. See Juniper Two Stage Challenge and Response.

## **340 Prerequisites**

Juniper 7.x

Swivel 3.x

Modified login pages can be downloaded from here: PINsafe modified pages also requires sample pages from Juniper appliance.

It is possible to access Juniper SSL VPN from mobile devices such as iPhone, Blackberry, Windows Mobile and Andriod devices.

To support this, additional pages needs to be modified to support Swivel.

Mobile login pages can be downloaded from here: Swivel Mobile login pages, and should be included if the Single channel images are required on mobile devices.

Where the Virtual DNS is to be used, a DNS entry that uses the same IP address of the external VPN is required. For example turing.swivelsecure.com would need to point to the same IP address as vpn.swivelsecure.com. A valid certificate is required on the Swivel server.

# 341 Baseline

Juniper 7.2 Swivel 3.7

# 342 Architecture

A user receives their security string by their transport and enters the authentication information into the login page. The Juniper makes a RADIUS request against the Swivel server to verify the OTC. Usually the Juniper page also verifies the AD password is correct by verifying it against the AD server, in addition to the OTC.

### 343 Installation

#### 343.1 Swivel Configuration

#### 343.1.1 Configuring the RADIUS server

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

#### 343.1.2 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.

#### 343.2 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

#### 343.3 Juniper Integration

#### 343.3.1 RADIUS Authentication Server Configuration

On the Juniper Server select Authentication Servers then select RADIUS Server from the drop down menu, and click on New Server.

Central Manager - System			
Status  Configuration Network Clustering Clu	Authentication Serve New: (Select server type) (Select server type) NE Authentication LDAP Server ACE Server Stadius Server Active Directory / Windows NT Anonymous Server SiteMinder Server Certificate Server SAML Server	Vers	ete Type IVE Authenticatio IVE Authenticatio

The following information is required:

Name: A descriptive name for the RADIUS server

**RADIUS Server:** The Swivel server IP/Hostname (Use the Swivel server real IP address not the VIP, multiple servers can be defined as Primary and secondary servers).

Authentication Port: the port used to carry authentication information, by default 1812

Shared Secret: The shared secret that has been entered on the Swivel server

Accounting Port: the port used to carry accounting information, by default 1813

NAS-IP Address: the Juniper interface used for communication, usually left empty

Users authenticate using tokens or one-time passwords Ensure this box is ticked

Backup server, Enter the details of any additional Swivel servers which can be used for authentication.

– System			
Status +	Auth Servers >		
Configuration +	PINsafe		
Network +			
Clustering >	Settings Users		
Log/Monitoring →			
- Authentication			
Signing In 🔶 🔸	Name:	PINsafe	Label to reference this server.
Endpoint Security >	Radius Server:	82.69.194.195	Name or IP address
Auth. Servers		1010	
<ul> <li>Administrators</li> </ul>	Authentication Port:	1812	
Admin Realms →	Shared Secret:		
Admin Roles →		4040	
- Users	Accounting Port:	1813	Port used for Radius accounting, if applicable
User Realms →	NAS-IP-Address:		IP address
User Roles >			
Resource Profiles +		20	
- Maintenance	limeout:	30 seconds	
Sustan	Retries:	0	
Import/Export			
Push Config			time an environde
Archiving +	Voters authenticat	te using tokens or one	- time passwords
Troubleshooting +	and this credential w	ill not be used in automati	ic SSO to backend applications.
	Backup server		
	Padius Convort		Name of ID address
	Radius Server.		Name of the address
	Authentication Port:		
	Shared Secret:		
	Accounting Port:		Port used for Radius accounting, if applicable
	Radius accounting		
	NAS-Identifier:		Name of IVE as known to Radius

#### 343.3.2 Authentication Realm Configuration

Authentication realms determine which method of authentication will be used. On the Juniper select User Realms, and either create a new Realm with the New button or or modify an existing realm by clicking on it.

# Juniper*

Central Manager	
- System	
Status > Configuration > Network > Clustering >	User Authentication Realms         New       Duplicate
Log/Monitoring →	
- Authentication	Authentication Realm
Signing In Endpoint Security Auth. Servers	Users
- Administrators	
Admin Realms → Admin Roles →	Authentication realms specify what server to use for authentication, how policies are assigned to users,
- Users	
User Realms  User Roles  Resource Profiles  Resource Policies	
Maintenance	
System > Import/Export > Push Config Archiving > Troubleshooting >	

#### 343.3.3 Swivel as the Primary Authentication Server

Swivel can be configured as the only authentication method, the first or more usually configured as the secondary authentication server. By changing the Authentication device order on the Juniper, Swivel can be configured as the first authentication server, but you may lose some functionality of SSO to sign you into AD applications and services. The login page would also need to be modified to display the correct text.

To configure Swivel as the server select the Swivel server as the first listed Authentication Server.

#### 💽 Juniper° **Central Manager** System New Authentication Realm Status Configuration Network Clustering PINsafe Realm Label to reference Name: Log/Monitoring - Authentication Description: PINsafe OTC ~ Signing In Authentication Realm Endpoint Security + Auth. Servers Administrators When editing, start on the Role Mapping page Admin Realms Admin Roles Servers User Realms Specify the servers to use for authentication and authorization. To create or manage servers, see the User Roles Resource Profiles > Resource Policies ► Authentication: PINsafe Specify the server Maintenance Directory/Attribute: Same as above 💙 Specify the server System Import/Export Accounting: None Specify the server Push Config Archiving Additional authentication server Troubleshooting > Dynamic policy evaluation Save changes?

#### 343.3.4 Swivel as the Secondary Authentication Server

Swivel can be configured as the only authentication method, or more usually configured as the secondary authentication server.

To configure Swivel as the server as a secondary authentication server cluck on the box Additional authentication server

Save Changes

General Authentication Polic	cy Role Mapping	
Name:	PINsafe 2 stage authentic	Label to re
Description:	PINsafe 2 stage	
	When editing, start on the Role M	Mapping page
Servers		
Specify the servers to use for authe	ntication and authorization. To create or manage servers, s	see the <u>Servers</u> page.
Authentication:	AD-TEST-SERVER	Specify the
Directory/Attribute:	Same as above 💌	Specify the
Accounting:	None	Specify the
Additional authenticatio	n server	
You can specify an additional authe are specified by the sign-in page), o	ntication server for single sign-on (SSO) purposes. The add or they can be pre-defined below, in which case the user wil	ditional credentials can be spec I not be prompted for the crede
Authentication #2:	pinsafe-demo 💌	
Username is:	C specified by user on sign-in page	9
	predefined as: <a href="https://www.estimation.org">USERNAME&gt;</a>	
Password is:	<ul> <li>specified by user on sign-in page</li> </ul>	
	O predefined as: PASSWORD>	
	☑ End session if authentication aga	ainst this server fails

**NOTE:** when <USERNAME> is used then just the Username is sent to the Juniper, without a Domain prefix/suffix. When <USER> is used then the Domain Name may be added in the authentication request to the Swivel instance in the form domain\username.

USERNAME

### Additional authentication server

You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specified user on the sign-in page (the labels for these inputs are specified by the sign-in page), or they can be pre-defined below, which case the user will not be prompted for the credential.

Authentication #2:	SwivelSecure -
Username is:	specified by user on sign-in page
	o predefined as:
Password is:	specified by user on sign-in page
	o predefined as: <password></password>
	End session if authentication against this server fails

#### USER

Additional authentication	ion server
You can specify an additional auth the user on the sign-in page (the which case the user will not be pro	nentication server for single sign-on (SSO) purposes. The additional credentials can be speci labels for these inputs are specified by the sign-in page), or they can be pre-defined below, ompted for the credential.
Authentication #2:	SwivelSecure -
Username is:	specified by user on sign-in page
	o predefined as: <user></user>
Password is:	specified by user on sign-in page
	o predefined as: <password></password>
	End session if authentication against this server fails

Central Manager				
- System				
Status >	User Authentication Realms			
Configuration +				
Network >	New Duplicate Delete			
Log/Monitoring				
- Authentication	Authentication Realm			
Signing In +	PINsafe Realm			
Endpoint Security >				
- Administrators				
Admin Realms				
Admin Roles	Authentication realms specify what server to use for authentication, how policies are assigned to users.			
- Users				
User Realms →				
User Roles >>				
Resource Profiles >				
Resource Policies >				
- Maintenance				
System >				
Import/Export >				
Archiving				

#### 343.3.5 Juniper Sign-In Policy

The Policy associates a login URL to a login page and an authentication realm which will verify a users credentials. Swivel authentication can be applied to an existing authentication page or to a new possibly customised login page (see login page customisation).

To associate Swivel authentication to a signing in page, associate the realm with the required login page. On the Juniper select Signing-In/Sign-in Policies, then New URL.

# 

Cent	ra	Man	ager

central Hanager					
🗏 System					
Status )	Signing In				
Configuration )					
Network )	Sign-in Policies Sign-in Pages				
Clustering )					
Log/Monitoring		A DIS YOS			
Authentication	Restrict access to administrators only				
Signing In	Only administrator URLs will be accessible. Note that IVE Administrators can attempt to sign in eve				
Auth Servers					
Administrators	Display multiple user sessions warning notification				
Administrators	Check this option to notify users if	they are already logged in with another active se	ssion. If the u		
Admin Realms	terminated.				
- Users					
lines Beelen	New ORL Delete Enab				
User Roles					
Resource Profiles )					
Resource Policies )	Administrator URLs	Sign-In Page	,		
- Maintenance	*/admin/	Default Sign-In Page			
System )	A 10 10 10 10 10 10 10 10 10 10 10 10 10				
Import/Export	·				
Push Config					
Archiving					
Troubleshooting )	User URLs	Sign-In Page			
	*/	Default Sign-In Page	1		
	Meeting URLs	Sign-In Page			
	/meeting/	Meeting Sign-In Page			

Enter a name for the URL, and select a signing-in page (see details below for custom pages). Ensure Swivel is selected as an authentication realm.
# 

Central Manager	
System Status Configuration Network Clustering Log/Monitoring Authentication	Save Changes
Signing In > Endpoint Security > Auth. Servers Auth. Servers Administrators Admin Realms > Admin Roles > User Realms > User Realms > User Roles > Resource Profiles >	User type: Ousers Ondeministrators Oneeting Sign-in URL: */pinsafe Description: PINsafe sign in Policy Sign-in page: PINsafe To create or manage pages, see <u>Sign-In pages</u> . Meeting URL: */meeting/ V
Resource Policies > Maintenance System > Import/Export > Push Config Archiving > Troubleshooting >	Authentication realm         Specify how to select an authentication realm when signing in.         • User types the realm name         The user must type the name of one of the available authentication realms.         • User picks from a list of authentication realms         The user must choose one of the following selected authentication realms when they sign in. If sign-in page will not display the list). To create or manage realms, see the User Authentication         Available realms:       Selected realms:         Users       Add ->         PINsafe Realm       Move Up         Move Down

When complete the new Swivel policy should be listed.

# 

## Central Manager

- System				
Status >	Signing In			
Configuration >				
Clustering +	Sign-in Policies	Sign-in Pages		
Log/Monitoring +				
- Authentication	Restrict acces	s to administrators (	only	
Signing In → Endpoint Security →	Only administrate	or URLs will be accessibl	e. Note that IVE Administrators can attem	pt to sign in eve
Auth. Servers	Display multiple	e user sessions warr	ning notification	
- Administrators	Check this option	to notify users if they a	are already logged in with another active	session. If the u
Admin Roles >	terminated.			
- Users	New URL	elete Enable	Disable 主 🖡	
User Realms →				
User Roles >				
Resource Profiles +	Administrator U	JRLs	Sign-In Page	A
- Maintenance	*/admin/		Default Sign-In Page	A
System ▶				
Import/Export >				
Archiving >				
Troubleshooting >	User URLs		Sign-In Page	A
	<u>*/</u>		Default Sign-In Page	L
	*/pinsafe/		PINsafe	A
	Meeting URLs		Sign-In Page	A
	/meeting/		Meeting Sign-In Page	

## 344 Additional Installation Options

Swivel can provide additional authentication options including:

#### Challenge and Response

Single Channel Authentication Images

Dual Channel Image for Confirmed Messages

Security String Index Image for Multiple security strings

For ChangePIN integration see Juniper ChangePIN

Where an image is used it is requested by the client from the Swivel server, this can be done in a number of ways:

- Swivel on a public IP address
- Swivel behind a Network Address Translation/Port Address Translation
- Swivel behind a Proxy server
- Swivel behind a Juniper Virtual DNS Proxy

### 344.1 Creating a Virtual DNS Entry

If using the single channel authentication such as TURing, or SMS confirmed Images, or SMS on demand buttons, an external DNS entry is required that points to the same IP address as the Juniper SSL VPN.

Example:

Juniper SSL VPN vpn.mycompany.com IP 1.1.1.1 Turing Image turing.mycompany.com IP 1.1.1.1

Swivel Example:

Juniper SSL VPN vpn1.swivelsecure.com IP 1.1.1.1 Turing Image turing.swivelsecure.com IP 1.1.1.1

#### 344.1.1 Creating a role for Virtual hostname

Create a role for the Virtual hostname. Then under User Roles/<role name>/Web/Bookmarks, the role does not need any web bookmarks, but under the Options, advanced settings set *Allow browsing untrusted SSL sites, and remove the option* to *Warn users about the certificate problems*.

- System	
Status >	Roles >
Configuration >	Pinsafe
Network >	
Clustering >	General Web Files SAM Telnet/SSH Terminal Services Virtual Desktops
IF-MAP Federation →	
Log/Monitoring →	Bookmarks   Options
Authentication	
Signing In →	User can type URLs in the IVE browse bar
Endpoint Security >	Users can browse to sites by typing URLs on their bookmarks page. If disabled, users can s
Auth. Servers	
- Administrators	User can add bookmarks
Admin Realms	Users can add personal bookmarks
Admin Roles >	
Users	Mask hostnames while browsing
Licer Realms	Conceals the actual server name in URLs while the user is browsing for protocols rewritten by
User Roles	
Resource Profiles >	<ul> <li>View advanced options</li> </ul>
Resource Policies >	
Junos Pulse	If Java applets are enabled, they will normally be modified to allow secure network connection
- Maintenance	
Sustam	Allow Elach contant
Import/Export	If this option is enabled, Flash content will be modified to allow secure network connections.
Push Config	
Archiving >	Persistent cookies
Troubleshooting >	User preferences and application settings are sometimes stored in persistent cookies. To m
	Unrewritten pages open in new window
	When users access pages that are not rewritten (see the <u>Selective Rewriting</u> policy page), yo
(	Allow browsing untrusted SSL websites Allow users to access web servers with problem certificates, or with certificates not issued by
	Warn uppers about the cortificate problems
	Allow users to bypass warnings on a server-by-server basis
	Rewrite file:// URLs
	file:// URLs get rewritten so files can be downloaded using Windows file browsing.
	Rewrite links in PDF files Links in PDF files
	Links in PDF mes get rewritten so that they can be settlely accessed through the gateway.
	HTTP Connection Timeout
	HTTP Connection Timeout: 240 Seconds 30 to 1800 seconds. This determine
	Save changes?
	Sava Changes

#### 344.1.2 Creating an ACL for the Virtual hostname role

An ACL must be created on the Juniper SA to allow access to the Swivel server. For further information see [1]

A new policy and role may be required for this. Select Resource Policies/Web Access Policies/<Policy Name>/General, under Resources enter the Swivel internal address:

Example https://pinsafe.swivel.local:8443/proxy/*

For Roles select Policy Applies to selected roles, add the required role to the selected roles.

For Actions select Allow Access.

Junos Pulse Secure Ac	cess Service on ive2		
🗄 System			
Status +	Web Access Policies	>	
Configuration +	Pinsafe		
Network +			
Clustering +	General Detail	ed Rules	
IF-MAP Federation >			
Log/Monitoring >			
- Authentication	* Name:	Pinsafe	
Signing In >	Description:		
Endpoint Security >			
Auth. Servers			
- Administrators			+
Admin Realms 🔹 🕨			
Admin Roles >>	Resources		
- Users			
User Realms →		Specify the resources for which this polic	y applies, one per line. In order for yo
User Roles 🔶 🕨	* Posourcos		Examples
Resource Profiles +	Resources.	https://pinsafe.	http://*.domain.com/p
Resource Policies +		ctrl.local:8443/proxy*	https://www.domain.com
Junos Pulse >			_ 10.10.10.10/24:8000-9
- Maintenance			
System >			
Import/Export +	Koles		
Push Config →		Policy applies to ALL roles	
Archiving +			
Troubleshooting >		Policy applies to SELECTED rol	les
		Policy applies to all roles OTHE	ER THAN those selected below
		Available roles:	
		Birds & Bees	
			(≡)
			<b>T</b>
	Action		
		Allow access	
		Deny access	
		O Use Detailed Rules (see <u>Detail</u>	ed Rules page)
	Save changes?		
		Save Changes Save as Con	/
		Care changes	·
Done			

L

#### 344.1.3 Creating the Virtual Hostname

To create a Virtual DNS entry, on the Juniper SA select the Authentication/Signing In/Sign-In Policies and then select New Page. Select the Authorization Only Access radio button for User type. Complete the following information:

Virtual Hostname: enter the DNS name that will point to the Swivel virtual or hardware appliance for the TURing image.

Example: turing.swivelsecure.com/

Backend URL: enter the protocol, IP address and port of the Swivel virtual or hardware appliance

Example for a Swivel virtual or hardware appliance: http://192.168.0.35:8443/*

For a software only install see Software Only Installation

Authorization Server: select No Authorization

Role Option: Select a Role

Save the Changes

<u>signing In</u> > juniper.swivelsed	cure.com/	
Save Changes		
User type:	C Users C Administrators C Aut	horization Only Access
Virtual Hostname:	juniper.swivelsecure.com/	Clients connect to a virtual hostname on the
Backend URL:	http://192.168.0.215:8443/*	Required: Protocol, hostname and port of the Server paths are not supported.
Description:	Turing Proxy	
Authorization Server:	[No Authorization]	
Role Option:	AnonyRole  Not all role options will apply. See admin guide	
Save changes?		
Save Changes		



#### 344.1.4 Verifying the Virtual DNS Entry

Swivel virtual or hardware appliance

From within the network verify the Swivel server is working using the below to generate a TURing image

http://<PINsafe appliance URL>:8443/proxy/SCImage?username=test

Then verify the external access using

https://<turing.mycompany.com>/proxy/SCImage?username=test

Software Install

For a software only install see Software Only Installation

Then verify the external access using

https://<turing.mycompany.com>/pinsafe/SCImage?username=test

## 344.2 Login Page Modifications for Single Channel Authentication and SMS On Demand

The sample pages provided by Juniper on the current version to be integrated, should always be used, as these are the supplied compatible pages and contain the latest updates and security features. To obtain these, login to the Juniper and select Signing-In, Sign-in pages, then click on Upload Custom Pages.

	r°	
Central Manager		
– System		
Status > Configuration > Network > Clustering > Log/Monitoring > Authentication Signing In > Endpoint Security >	Signing In Sign-in Policies Sign-in Pages New Page Upload Custom Pages Delete Sign-In Page	Tvr
Auth. Servers	Default Circ In Deep	
Administrators	Default Sign-In Page	Sta
Admin Realms →	Meeting Sign-In Page	Sta
Admin Roles >		
- Users		
User Realms →		
User Roles →		
Resource Profiles ►		
Resource Policies >		
- Maintenance		
System >		
Import/Export >		
Archiving		
Troubleshooting >		

Click on the **Sample** and download the latest sample pages. This is a zip file, and any additional files or changes will need to be added back to the zip file with the original contents, to be uploaded again.

Junipe	r°
Central Manager	
- System	
Status > Configuration >	Upload Custom Sign-In Pages
Clustering Log/Monitoring Authentication	Custom sign-in pages allow you to provide customized templates for various pages that appear during the sign-in process. Refer to the documentation for information about creating valid templates.
Signing In → Endpoint Security → Auth. Servers	Sign-In Pages Name:
Administrators Admin Realms Admin Roles	Label to reference the custom sign-in pages. Page Type: <ul> <li>Access</li> <li>Meeting</li> </ul>
i≕ Users User Realms → User Roles → Resource Profiles →	Templates File: Browse Zip file containing the custom templates and assets.
Resource Policies >	Upload
- Maintenance	
System  Import/Export Push Config Archiving Troubleshooting	Skip validation checks during upload

Using the sample login pages we can add the Swivel modified pages (see prerequisites), and change them to suit the integration requirements.

The configuration section within LoginPage.thtml should be edited to suit your environment as the below modifications.

#### 344.2.1 Modifying the Login Page

OTC_OPTION Controls how the TURing image will be displayed to the user

Option	Description	Single channel Option	Dual Channel Option
image	When the user tabs down from the username field, the TURing will automatically show	Y	N
button	The login page will present a TURing button. Click the button to display the TURing	Y	Y
disable	No TURing image	Y	Y

#### OTC_RANDOM Displays a button on screen to refresh the TURing image

Option	Description	Single channel Option	Dual Channel Option
true	Button will be displayed	Y	Y
false	No button	Y	Y

#### TURingImage URL for generating a TURing image

Option	Description	Single channel Option	Dual Channel Option
URL (see below)	Change the TURingImage value to reflect the IP address of the Swivel appliance	Y	Y

The URL may be one of the following:

#### Using Virtual DNS

#### Swivel appliance

https://virtual_hostname/proxy/SCImage?username=";

#### Software install

http://virtual_hostname/pinsafe/SCImage?username=";

• For a NAT or Public IP address

#### Swivel appliance

https://hostname:8443/proxy/SCImage?username=";

Software install

http://hostname:8080/pinsafe/SCImage?username=";

#### 344.2.2 Modifying the Welcome Message

To customise login page welcome message, you must edit the LoginPage.thtml (and LoginPage-stdaln.thtml if using Network Connect):

Search and remove the following:

<% welcome FILTER verbatim %>

This references the first line of the Welcome message. E.g. change this to "Welcome to the"

Search and remove the following:

<% portal FILTER verbatim %>

This references the second line of the Welcome message. E.g. change this to "Swivel Secure Login Page"

#### 344.2.3 Modifying the login for SMS Only requests

Swivel supports SMS on Demand, SMS in advance and SMS using Two Stage authentication. Where SMS on demand only, is used, the login page may be modified so that instead of generating a TURing image a SMS is sent to the user. Locate the following line:

https://virtual_hostname/proxy/SCImage?username=";

and modify the SCImage?username=" to DCMessage?username=;

Example:

#### Using Virtual DNS

Swivel appliance

https://virtual_hostname/proxy/DCMessage?username=";

Software install

http://virtual_hostname/pinsafe/DCMessage?username=";

• For a NAT or Public IP address

#### Swivel appliance

https://hostname:8443/proxy/DCMessage?username=";

For a software only install see Software Only Installation

#### 344.2.4 Modifying the login button text

The login page button and link to Get Another Image may be modified.

To modify the login button text locate the text value='Turing' and replace the Turing with the required text.

To modify the Get another image? URL, locate the two instances of Get another image? and change the text as required.

#### 344.2.5 Modifying the login for PINpad

The custom page for Pinpad, is available from here.

Follow the same instructions as above, but note the following:

- The zip file contains 3 additional images that need to go into the imgs folder of the Juniper custom login.
- OTC_OPTION needs to be set to "pinpad", which it already is in the attached file.

• You need to set the value for *PinpadImage*, rather than *TURingImage* to match your own Swivel instance.

#### Example

var PinpadImage = "https://hostname:8443/pinsafe/SCImage?username=";

#### to

var PinpadImage = "https://hostname:8443/pinsafe/SCPinPad?username=";

#### 344.2.6 Modifying the Login pages for Mobile Devices

Download the mobile modified pages that can be uploaded with any other modified pages to add Swivel authentication to the login.

Modify the file PageHeader-mobile-webkit.thtml, find the below line and change the link for the Swivel appliance as the standard login page above. var TURingImage = "https://pinsafe.company.com/proxy/SCImage?username=";

Instant Virtual Ex	ktranet 📑 🗟 🕸 EN
Instant Virtua	l Extranet
Please sign in to be	gin your secure session.
username	test
password	•••••
One-Time Coo	te ••••
Turing	
1 2 3 4	5 6 7 8 9 0
	ELYEAS
Get another in	nage?
	Sign In

#### 344.2.7 Juniper Network Connect login page modification

The Juniper Network Connect can be started directly, and to customise the login page for Swivel authentication copy the login.thtml page to LoginPage-stdaln.thtml

A Network Conn	ect - Sign In		
<u>T</u> ools			
Sign-in Page:	https://juniper.swivelsecure.com	▼ Go	
Swi	VEL [®] on Solutions		*
We	lcome to the Swive	Secure VPN	
userna passwo	ord	Please sign in to begin your secure session.	
One-T Code	ime		
	Sign In		
			*

Juniper Network Connect with TURing

Network Connect - S	Sign In			X
Tools				
Sign-in Page: http	s://juniper.swivelsecure.com	➡ Go		
Authentication So Welco username password One-Time Code	Sign In L 2 3 4 5 U B O E P Get another image?	vivel Secure	Please sign in to begin your secure session.	E
				_

#### 344.2.8 Uploading the Modified Page

Ensure all the modified files are included with the zip file to upload to the Swivel server. On the Juniper select Signing In/Sign-in Pages then click on Upload Custom Pages.

	r
Central Manager	
Central Manager System Status Configuration Configuration Network Clustering Log/Monitoring Authentication Signing In Endpoint Security Auth. Servers Auth. Servers Admin Realms Admin Roles Users	Signing In         Sign-in Policies         Sign-in Policies         New Page         Upload Custom Pages         Delete         Sign-In Page         Meeting Sign-In Page         Standard
User Realms >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	

Enter a Name for the Custom page, then use Browse to find the location of the Templates file. Then click on the Upload Custom Pages, observe any errors that may occur.

# 

Central Manager	
System Status Configuration Network Clustering Log/Monitoring Authentication	Signing In > Upload Custom Sign-In Pages Custom sign-in pages allow you to provide customized templates for various pages that appear during the sign-in process. Refer to the documentation for information about creating valid templates.
Signing In → Endpoint Security →	Sign-In Pages
Auth. Servers - Administrators	Name: PINsafe Label to reference the custom sign-in pages.
Admin Realms → Admin Roles → Users	Page Type: <ul> <li>Access</li> <li>Meeting</li> </ul>
User Realms User Roles Resource Profiles	Templates File: C:\Documents and Setting Browse Zip file containing the custom templates and assets.
Resource Policies >	Upload
Maintenance System Import/Export Push Config Archiving Troubleshooting	skip validation checks during upload

The new signing in page should be listed.

# 

Cen	tral	Ma	nao	er

Central Manager		
- System		
Status >	Signing In	
Configuration >		
Network +	Sign-in Policies Sign-in Pages	
Clustering +		
Log/Monitoring	New Page Upload Custom Pages Delate	
Authentication	Unew Page Delete	
Signing In		
Endpoint Security +	Sign-In Page	Туре
Administrators	PINsafe	Cust
Auministrators	Default Sign-In Page	Stan
Admin Realms >		Starr
Admin Roles >	Meeting Sign-In Page	Stan
- Users		
User Realms →		
User Roles >>		
Resource Profiles +		
Resource Policies >		
- Maintenance		
System >		
Import/Export >		
Push Config		
Archiving +		
Troubleshooting +		

## 345 Verifying the Installation

Navigate to the login page and verify that the page is as expected. Test a login using an OTC and verify the user can login with a correct OTC an fails with an incorrect OTC.

**Dual Channel Authentication** 

SWIVEL® Authentication Solutions	
Welcome to the	e Swivel Secure VPN
username password One-Time Code	Please sign in to begin your secure session.
Sign In	

Single Channel Authentication



## 346 Uninstalling the Swivel Integration

To remove Swivel, remove the customised page, Swivel realm, and Swivel Policy.

## 347 Troubleshooting

Check the Swivel logs. If the Single Channel image is used then a 'session start' should be see for the username. RADIUS authentication requests should be seen for successful or failed login attempts.

Check the Juniper logs, look for user authentication requests.

If the TURing image is not visible, right click on the red cross and view the details of the image URL.

Copy and paste this URL into a separate web browser, observe any certificate errors.

Welcome to the	
Swivel Secure VPN	Access Page
username bob	Please sign in to begin your secure session.
password	
Sign In	
Turing	
×	

#### **Internal Certificate Authorities**

If an internal certificate authority is used, then the Single Channel image may not be accessible externally unless the client has installed the certificate as a trusted root certificate. Using a valid public certificate will remove this requirement.

#### domain\username is used instead of username

On the Juniper when USER is used then the domain name may be added in the authentication request to the Swivel instance in the form domain/username. When USERNAME is used then just the username is sent to the Juniper.

## 348 Known Issues and Limitations

"ExceededConcurrent.thtml" is not found in zip file.

Ensure that the file is present.

Make sure that the files are not located in a sub-directory within the zip folder

Select All of the files within the folder and then send to a zip folder

#### 348.1 iPhone, iPad iOS automatic TURing image generation issue

The Onblur method in Javascript does not work in iOS, so a TURing button would need to be created to request the image after the username has been entered.

<a class="wide confirm buttonTxt" href="#" onclick="var frm = document.getElementById('frmLogin'); if (onFormSubmit()) { frm.submit(); }">Si

A modified login page is available here: iPad modified login page

#### 348.2 Junos Pulse usability issue

Junos Pulse for SSL VPN: How to resolve usability issue (very small fonts and field size) with the VPN login screen on iPhone running iOS 7

#### 348.3 Authentication fails after upgrading Swivel

In Swivel 3.8, the domain name was automatically removed for RADIUS authentication. However, this prevents authentication in cases where the domain\ prefix is required.

Assuming PINsafe is not the primary authentication, this can be worked around by changing the value passed to Swivel by the Juniper as <USERNAME>, rather than <USER>. This is in the Juniper settings for secondary authentication: "Username is predefined as".

## 349 Additional Information

Custom sign-in pages for Pinpad can be found here.

## 350 Juniper SA 8.x Integration

## 351 Overview

Swivel can be integrated with the SA series of SSL VPN products, with the SA 2000 and higher products also allowing additional login page functionality. Creating additional login pages allow different authentication methods and test pages to be created with different functionality. 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.

The SA 700 can be configured in a similar manner using RADIUS authentication except for the TURing image and other login page modifications.

For 6.x integration guide see Juniper SA 6.x Integration

For 7.x integration guide see Juniper SA 7.x Integration

It is also possible to configure Two Stage authentication whereby the user enters a username and AD Password and if correct the user can be sent a security string or OTC for Authentication. This can be combined with the Juniper Two Stage authentication to allow the AD Single Sign On (SSO) features. See Juniper Two Stage Challenge and Response.

## **352 Prerequisites**

Juniper 8.x

Swivel 3.x

Modified login pages can be downloaded below. Note that you don't need the included image files unless you are using Pinpad.

It is possible to access Juniper SSL VPN from all mobile devices, however additional pages need to be modified to support Swivel integration.

Mobile login pages can be downloaded below, and should be included if the Single channel images are required on mobile devices. NOTE: These have not been tested on version 8.

Where the Virtual DNS is to be used, a DNS entry that uses the same IP address of the external VPN is required. For example turing.swivelsecure.com would need to point to the same IP address as vpn.swivelsecure.com. Since the Juniper will be supporting at least two different host names, the SSL certificate on the Juniper must either be a wildcard certificate, or must include SANs (Subject Alternative Names) for all host names used.

## 353 File Downloads

PINsafe modified pages

Swivel Mobile login pages

Modified pages for both PC and tablets. These files have been tested internally only, and do not currently work with PINpad on tablets. The main advantage is that you only need edit one file - swivel-header.thtml - to set the image URL for all devices.

## 354 Baseline

Juniper 8 Swivel 3.9.7

## **355 Architecture**

A user receives their security string by their transport and enters the authentication information into the login page. The Juniper makes a RADIUS request against the Swivel server to verify the OTC. Usually the Juniper page also verifies the AD password is correct by verifying it against the AD server, in addition to the OTC.

## 356 Installation

### 356.1 Swivel Configuration

#### 356.1.1 Configuring the RADIUS server

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

#### 356.1.2 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.

#### 356.2 Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

#### 356.3 Juniper Integration

#### 356.3.1 RADIUS Authentication Server Configuration

On the Juniper Server select Authentication Servers then select RADIUS Server from the drop down menu, and click on New Server.

Central Manager		
<ul> <li>System</li> <li>Status</li> <li>Configuration</li> <li>Network</li> <li>Clustering</li> <li>Log/Monitoring</li> <li>Clustering</li> <li>Log/Monitoring</li> <li>Authentication</li> <li>Signing In</li> <li>Endpoint Security</li> <li>Auth. Servers</li> <li>Admin Security</li> <li>Admin Realms</li> <li>Admin Roles</li> <li>User Realms</li> <li>User Roles</li> <li>Resource Profiles</li> <li>Resource Profiles</li> <li>Resource Policies</li> <li>Maintenance</li> <li>System</li> <li>Import/Export</li> <li>Push Config</li> <li>Archiving</li> <li>Troubleshooting</li> </ul>	Authentication Servers New: (Select server type)  New Server Delete (Select server type) NE Authentication LDAP Server ANIS Server ACE Server StedMinder Server SiteMinder Server SAML Server	Type IVE Authenticatio IVE Authenticatio

The following information is required:

Name: A descriptive name for the RADIUS server

**RADIUS Server:** The Swivel server IP/Hostname (Use the Swivel server real IP address not the VIP, multiple servers can be defined as Primary and secondary servers).

Authentication Port: the port used to carry authentication information, by default 1812

Shared Secret: The shared secret that has been entered on the Swivel server

Accounting Port: the port used to carry accounting information, by default 1813

NAS-IP Address: the Juniper interface used for communication, usually left empty

Users authenticate using tokens or one-time passwords Ensure this box is ticked

Backup server, Enter the details of any additional Swivel servers which can be used for authentication.

- System			
Status >	Auth Servers >		
Configuration >	PINsafe		
Network 🕨			
Clustering >	Settings Users		
Log/Monitoring →			
- Authentication		DUL 2	
Signing In >	Name:	PINsate	Label to reference this server.
Endpoint Security >	Radius Server:	82.69.194.195	Name or IP address
Auth. Servers	Authentication Daute	1010	
- Administrators	Authentication Port:	1012	
Admin Realms →	Shared Secret:		
- Users	Accounting Port:	1813	Port used for Radius accounting, if applicable
User Realms →	NAC-ID-Address		TD address
User Roles →	NAS-IP-Address.		IP dutiess
Resource Profiles >			
Resource Policies >	Timeout:	30 seconds	
- Maintenance	Patrios:	0	
System >	Neures.	•	
Import/Export >			
Push Config	Users authenticate using tokens or one-time passwords		
	Note: If you select this, IVE will send the user's authentication method as "token" if you use SAM		
	and this credential will not be used in automatic SSO to backend applications.		
	Packup convor		
	backup server		
	Radius Server:		Name or IP address
	Authentication Port:		
	Shared Secret:		
	Accounting Port:		Port used for Radius accounting, if applicable
	Radius accounting		
	NAS-Identifier:		Name of IVE as known to Radius

#### 356.3.2 Authentication Realm Configuration

Authentication realms determine which method of authentication will be used. On the Juniper select User Realms, and either create a new Realm with the New button or or modify an existing realm by clicking on it.

## Juniper*

Central Manager	
- System	
Status > Configuration > Network > Clustering >	User Authentication Realms         New       Duplicate
Log/Monitoring >	
- Authentication	Authentication Realm
Signing In Endpoint Security Auth. Servers	Users
- Administrators	
Admin Realms → Admin Roles →	Authentication realms specify what server to use for authentication, how policies are assigned to users,
- Users	
User Realms  User Roles  Resource Profiles  Resource Policies	
Maintenance	
System > Import/Export > Push Config Archiving > Troubleshooting >	

#### 356.3.3 Swivel as the Primary Authentication Server

Swivel can be configured as the only authentication method, the first or more usually configured as the secondary authentication server. By changing the Authentication device order on the Juniper, Swivel can be configured as the first authentication server, but you may lose some functionality of SSO to sign you into AD applications and services. The login page would also need to be modified to display the correct text.

To configure Swivel as the server select the Swivel server as the first listed Authentication Server.

#### 💽 Juniper° **Central Manager** System New Authentication Realm Status Configuration Network Clustering PINsafe Realm Label to reference Name: Log/Monitoring - Authentication Description: PINsafe OTC ~ Signing In Authentication Realm Endpoint Security + Auth. Servers Administrators When editing, start on the Role Mapping page Admin Realms Admin Roles Servers User Realms Specify the servers to use for authentication and authorization. To create or manage servers, see the User Roles Resource Profiles > Resource Policies ► Authentication: PINsafe Specify the server Maintenance Directory/Attribute: Same as above 💙 Specify the server System Import/Export Accounting: None Specify the server Push Config Archiving Additional authentication server Troubleshooting > Dynamic policy evaluation Save changes?

#### 356.3.4 Swivel as the Secondary Authentication Server

Swivel can be configured as the only authentication method, or more usually configured as the secondary authentication server.

To configure Swivel as the server as a secondary authentication server cluck on the box Additional authentication server

Save Changes

General Authentication Polic	cy Role Mapping	
Name:	PINsafe 2 stage authentic	Label to re
Description:	PINsafe 2 stage	
	When editing, start on the Role M	Mapping page
Servers		
Specify the servers to use for authe	ntication and authorization. To create or manage servers, s	see the <u>Servers</u> page.
Authentication:	AD-TEST-SERVER	Specify the
Directory/Attribute:	Same as above 💌	Specify the
Accounting:	None	Specify the
Additional authenticatio	n server	
You can specify an additional authe are specified by the sign-in page), o	ntication server for single sign-on (SSO) purposes. The add or they can be pre-defined below, in which case the user wil	ditional credentials can be spec I not be prompted for the crede
Authentication #2:	pinsafe-demo 💌	
Username is:	C specified by user on sign-in page	9
	predefined as: <a href="https://www.estimation.org">USERNAME&gt;</a>	
Password is:	<ul> <li>specified by user on sign-in page</li> </ul>	
	O predefined as: PASSWORD>	
	☑ End session if authentication aga	ainst this server fails

Note when USERNAME is used then just the username is sent to the Juniper. When USER is used then the domain name may be added in the authentication request to the Swivel instance in the form domain/username.

USERNAME

#### Additional authentication server

You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specified user on the sign-in page (the labels for these inputs are specified by the sign-in page), or they can be pre-defined below, which case the user will not be prompted for the credential.

Authentication #2:	SwivelSecure -
Username is:	specified by user on sign-in page
	predefined as: <username></username>
Password is:	specified by user on sign-in page
	o predefined as: <password></password>
	End session if authentication against this server fails

#### USER

Additional authentication server				
You can specify an additional auth the user on the sign-in page (the which case the user will not be pro	nentication server for single sign-on (SSO) purposes. The additional credentials can be speci labels for these inputs are specified by the sign-in page), or they can be pre-defined below, mpted for the credential.			
Authentication #2:	SwivelSecure -			
Username is:	specified by user on sign-in page			
	o predefined as: <user></user>			
Password is:	specified by user on sign-in page			
	o predefined as: <password></password>			
	End session if authentication against this server fails			

Central Manager		
- System		
Status >	User Authentication Realms	
Configuration +		
Network +	New Duplicate Delete	
Log/Monitoring		
- Authentication		
Signing In Endpoint Security >	PINsafe Realm	
- Administrators		
Admin Roalms		
Admin Roles	Authentication realms specify what server to use for authentication, how policies are assigned to users.	
- Users		
User Realms →		
User Roles →		
Resource Profiles >		
Resource Policies >		
- Maintenance		
System >		
Import/Export >		
Push Config		
Troubleshooting		

#### 356.3.5 Juniper Sign-In Policy

The Policy associates a login URL to a login page and an authentication realm which will verify a users credentials. Swivel authentication can be applied to an existing authentication page or to a new possibly customised login page (see login page customisation).

To associate Swivel authentication to a signing in page, associate the realm with the required login page. On the Juniper select Signing-In/Sign-in Policies, then New URL.

# 

Control	Man	30	<b>0</b> F
CEILLIAI			

Central Manager			
- System			
Status >	Signing In		
Configuration >			
Network >	Sign-in Policies Sign-in Pages		
Clustering +			
Log/Monitoring >			
Authentication	Restrict access to administrators only		
Signing In	Only administrator URLs will be accessible. Note that IVE Administrators can attempt to sign in eve		
Auth Servers			
- Administrators	Display multiple user sessions	warning notification	
	Check this option to notify users if t	hey are already logged in with another active s	ession. If the u
Admin Realms >	terminated.		
- Ilsors			
Ileas Bealers	Linew ORL Delete Enable		
User Roles >			
Resource Profiles >			
Resource Policies >	Administrator URLs	Sign-In Page	,
- Maintenance	*/admin/	Default Sign-In Page	1
System >			
Import/Export +			
Push Config			
Archiving >			
Troubleshooting >	User URLs	Sign-In Page	,
	<u>**/</u>	Default Sign-In Page	<u>l</u>
		Cian In Daga	
		Sign-In Page	,
	/meeting/	Meeting Sign-In Page	

Enter a name for the URL, and select a signing-in page (see details below for custom pages). Ensure Swivel is selected as an authentication realm.

## 

Central Manager	
System Status Configuration Network Clustering Log/Monitoring Authentication	Save Changes
Signing In > Endpoint Security > Auth. Servers Administrators Admin Realms > Admin Roles > User Realms > User Realms > Resource Profiles >	User type: ① Users ② Administrators ③ Meeting Sign-in URL: */pinsafe Description: PINsafe sign in Policy Sign-in page: PINsafe To create or manage pages, see <u>Sign-In pages</u> . Meeting URL: */meeting/ ♥
Resource Policies > Maintenance System > Import/Export > Push Config Archiving > Troubleshooting >	Authentication realm         Specify how to select an authentication realm when signing in.         • User types the realm name         The user must type the name of one of the available authentication realms.         • User picks from a list of authentication realms         The user must choose one of the following selected authentication realms when they sign in. If sign-in page will not display the list). To create or manage realms, see the User Authentication         Available realms:       Selected realms:         Users       Add ->         PINsafe Realm       Move Up         Move Down

When complete the new Swivel policy should be listed.
# 

# Central Manager

- System				
Status >	Signing In			
Configuration >				
Clustering +	Sign-in Policies	Sign-in Pages		
Log/Monitoring +				
- Authentication	Restrict access to administrators only			
Signing In → Endpoint Security →	Only administrate	or URLs will be accessibl	e. Note that IVE Administrators can attem	pt to sign in eve
Auth. Servers	Display multiple	e user sessions warr	ning notification	
- Administrators	Check this option	to notify users if they a	are already logged in with another active	session. If the u
Admin Roles >	terminated.			
- Users	New URL	elete Enable	Disable 主 🖡	
User Realms →				
User Roles >				
Resource Profiles +	Administrator U	JRLs	Sign-In Page	A
- Maintenance	*/admin/		Default Sign-In Page	A
System ▶				
Import/Export >				
Archiving >				
Troubleshooting >	User URLs		Sign-In Page	A
	<u>*/</u>		Default Sign-In Page	L
	*/pinsafe/		PINsafe	A
	Meeting URLs		Sign-In Page	A
	/meeting/		Meeting Sign-In Page	

# **357 Additional Installation Options**

Swivel can provide additional authentication options including:

#### Challenge and Response

Single Channel Authentication Images

Dual Channel Image for Confirmed Messages

Security String Index Image for Multiple security strings

For ChangePIN integration see Juniper ChangePIN

Where an image is used it is requested by the client from the Swivel server, this can be done in a number of ways:

- Swivel on a public IP address
- Swivel behind a Network Address Translation/Port Address Translation
- Swivel behind a Proxy server
- Swivel behind a Juniper Virtual DNS Proxy

# 357.1 Creating a Virtual DNS Entry

If using the single channel authentication such as TURing, or SMS confirmed Images, or SMS on demand buttons, an external DNS entry is required that points to the same IP address as the Juniper SSL VPN.

Example:

Juniper SSL VPN vpn.mycompany.com IP 1.1.1.1 Turing Image turing.mycompany.com IP 1.1.1.1

Swivel Example:

Juniper SSL VPN vpn1.swivelsecure.com IP 1.1.1.1 Turing Image turing.swivelsecure.com IP 1.1.1.1

#### 357.1.1 Creating a role for Virtual hostname

Create a role for the Virtual hostname. Then under User Roles/<role name>/Web/Bookmarks, the role does not need any web bookmarks, but under the Options, advanced settings set *Allow browsing untrusted SSL sites, and remove the option* to *Warn users about the certificate problems*.

- System	
Status +	Roles >
Configuration >	Pinsafe
Network >	
Clustering +	General Web Files SAM Telnet/SSH Terminal Services Virtual Desktops
IF-MAP Federation ►	
Log/Monitoring >	Bookmarks Options
- Authentication	
Sianina In →	User can type URLs in the IVE browse bar
Endpoint Security >	Users can browse to sites by typing URLs on their bookmarks page. If disabled, users can s
Auth. Servers	
- Administrators	User can add bookmarks
Admin Realms	Users can add personal bookmarks
Admin Roles	
Hears	Mask hostnames while browsing
:_: USERS	Conceals the actual server name in URLs while the user is browsing for protocols rewritten by
User Realms →	
User Roles >	<ul> <li>View advanced options</li> </ul>
Resource Profiles >	
Resource Policies >	V Allow Java applets
Junos Pulse >	If Java applets are enabled, they will normally be modified to allow secure network connection
- Maintenance	
System +	Allow Flash content
Import/Export >	If this option is enabled, Flash content will be modified to allow secure network connections.
Push Config >	
Archiving >	Persistent cookies
Troubleshooting >	User preferences and application settings are sometimes stored in persistent cookies. To m
	Unrewritten pages open in new window
	With users access pages that are not rewritten (see the <u>selective tewriting</u> pointy page), yo
	Allow browsing untrusted CCI websites
/	Allow users to access web servers with problem certificates, or with certificates not issued by
	Warn users about the certificate problems
	Allow users to bypass warnings on a server-by-server basis
	file:// URLs get rewritten so files can be downloaded using Windows file browsing.
	Rowrite links in DDE files
	Links in PDF files get rewritten so that they can be securely accessed through the gateway.
	HTTP Connection Timeout
	HTTP Connection Timeout: 240 Seconds 30 to 1800 seconds. This determine
	Save changes?
	ouve changes.
	Save Changes

## 357.1.2 Creating an ACL for the Virtual hostname role

An ACL must be created on the Juniper SA to allow access to the Swivel server. For further information see [1]

A new policy and role may be required for this. Select Resource Policies/Web Access Policies/<Policy Name>/General, under Resources enter the Swivel internal address:

Example https://pinsafe.swivel.local:8443/proxy/*

For Roles select Policy Applies to selected roles, add the required role to the selected roles.

For Actions select Allow Access.

System         Status         Configuration         Network         IF-MAP Federation         Log/Monitoring         - Authentication         Signing In         - Authentication         Signing In         - Authentication         - Authentication         - Administration         - Administration         - Administration         - Administration         - Administration         - Resources         - Users         - User Ralms         - Administration         - Resource Profiles	Junos Pulse Secure A	ccess Service on ive2		
Status       Web Access Policies >         Configuration       Pinsafe         Clustering       Ceneral Detailed Rules         IT-MAP Federation       Pinsafe         Signing In       Description:         - Authentcation       * Name:         Description:	🖃 System			
Configuration       Pinsafe         Network       General Detailed Rules         Log/Monitoring       * Name:         Description:       * Name:         Endpoint Security       Administrators         Administrators       Resources         Administrators       Resources         Administrators       Resources         Administrators       Resources         Specify the resources for which this policy applies, one per line. In order for you that this policy applies, one per line. In order for you that this policy applies, one per line. In order for you that this policy applies to supplies to all policy applies to SLECTED roles         System       Policy applies to all po	Status >	Web Access Policies	>	
Network       General       Detailed Rules         Clustering       * Name:       Pinsafe         Signing In       Description:       *         * Auth-streves       Administrators         Administrators       Resources         * Resources       *         * Resource Profiles       *         * Resource Profiles       *         * Resource Profiles       *         System       *         * Name:       Policy applies to ALL roles         * Archoving       *         * Resource Profiles       *         System       *         * Roles       *         * Resource Profiles       *         * Name:       Policy applies to ALL roles         * Archiving       *         * Roles       *         * Policy applies to all roles OTHER THAN those selected below         Available roles:       *         Birds & Bees       *         *       *         Action       *         Action       *         *       *         Deny access       Deny access         Deny access       Outry access         Deny access       Save changes </td <td>Configuration &gt;</td> <td>Pinsafe</td> <td></td> <td></td>	Configuration >	Pinsafe		
Clustering       General Detailed Rules         IF-MAP Faderation Log/Monitoring       * Name:       Pinsafe         Signing In       Description:       *         Administrators       Administrators       *         Administrators       *       Resources         User Realms       *       Resources         *       Resource Profiles       *         Resource Profiles       *       Resources         *       Name:       Delailed Rules         *       Resource Profiles       *         Resource Profiles       *       Resources         *       Name:       Delailed Rules         *       Resource Profiles       *         Resource Profiles       *       Resources:         *       Name:       Delailed Rules         System       *       Policy applies to ALL roles         *       Policy applies to SELECTED roles       *         *       Policy applies to all roles OTHER THAN those selected below         Available roles:       Birds & Bees       *         Birds & Bees       *       *         *       Attion       *         *       Auxilable roles:       *         De	Network >			
IJF-AAP Federation   Log/Monitoring       * Name: Pinsafe         Signing In       Description:         * Auth.servers       Description:         * Administrators       Resources         * Administrators       Resources         * Obser       Specify the resources for which this policy applies, one per line. In order for you         * Resource Profiles       *         * Resource Profiles       *         * Resource Profiles       *         * Maintenance       *         * Maintenance       *         * Resource Profiles       *         * Junos Pulse       *         * Resource Profiles       *         * Maintenance       *         * Reles       *         * Policy applies to ALL roles         * Policy applies to all roles OTHER THAN those selected below         Available roles:         Birds & Bees         *         *       Action         *       Allow access         > Deny access       >         > Use Detailed Rules (see Detailed Rules page)         Save changes?       Save Changes         Save Changes       Save as Copy	Clustering +	General Detail	ed Rules	
Log/Monitoring     Authoritication     ** Name:     Pinsafe     Description:     ** Constraints     Administrators     Administrator     Administ	IF-MAP Federation >			
Name: Pinsafe      Description:     Authentication     * Name: Pinsafe      Description:     * Admin Relams     Admin Relams     Admin Relams     Admin Relams     Admin Relams     Admin Relams     * Resources      Bises     User Relams     * Resources:     Specify the resources for which this policy applies, one per line. In order for you     Trestource Profiles     * Resource Profiles     * Resources:     Trips://pinsafe.     Ctrl.local:8443/proxy*     Policy applies to ALL roles     Policy applies to ALL roles     Policy applies to SELECTED roles     Policy applies to SELECTED roles     Policy applies to all roles OTHER THAN those selected below     Available roles:     Birds & Bees     F     Ctrl         Save changes?     Save Changes Save as Copy  Done	Log/Monitoring >			
Signing In       Pescription:         Endpoint Security       Description:         Admin Realms       Resources         Admin Realms       Resources         User Realms       Specify the resources for which this policy applies, one per line. In order for you user Roles         Besource Profiles       Resources:         https://pinsafe. ctrl.local:8443/proxy*       Examples: http://scont 10.10.10/25.255.25         Junos Pulse       Policy applies to ALL roles         System       O Policy applies to SELECTED roles         Policy applies to all roles OTHER THAN those selected below         Available roles:       Birds & Bees         Birds & Bees       E         Save changes?       Save changes         Save Changes       Save as Copy	- Authentication	* Name:	Pinsafe	
Endpoint Security       Admin Roles         Admin Roles       Resources         User Realms       Resources         User Realms       Resources:         Proport Security       * Resources for which this policy applies, one per line. In order for you there readers for which this policy applies, one per line. In order for you there readers for the resource Policies *         Resource Policies       * Resources:         Intps://pinsafe.ctll.local:8443/proxy*       * Proportion:         System       *         Troubleshooting       *         Reles       *         Policy applies to ALL roles       *         Policy applies to SELECTED roles       *         Policy applies to all roles OTHER THAN those selected below         Available roles:       *         Birds & Bees       *         @       Allow access         Deny access       *         Use Detailed Rules (see Detailed Rules page)         Save changes?       Save Changes         Done       *	Signing In >>	Description		
Auth. Servers Administrators  Fresources  Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources Fresources	Endpoint Security >	Description.		*
Administratore     Adminis Realms     Associated Profiles     Resources Profiles     Resources Profiles     Adminis Realms     Action     Action     Action     Action     Action     Action     Action     Save changes     Save Changes     Save as Copy Done	Auth. Servers			
Admin Roles  Admin Roles  User Realms User Realms User Realms User Relations User Realms User Roles  Resources  Resource Profiles  Resources:  Resources:  Resources:  Resources:  Roles  Roles Roles  Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles Roles	- Administrators			-
Admin Rollins Admin Rollins - Users User Realms Resource Profiles Resource Profiles - Maintenance System Import/Export Push Config Archiving Troubleshooting Action Action Action Done	Admin Realms			
Closes         Resources           User Realms         *           User Realms         *           User Roles         *           Resource Policies         *           Junos Pulse         *           *         Resource Policies           Junos Pulse         *           *         Relation           *         Policy applies to ALL roles           *         Policy applies to all roles OTHER THAN those selected below           Available roles:         *           Birds & Bees         *           *         Use Detailed Rules (see Detailed Rules page)           Save changes?         Save Changes           Save Changes         Save as Copy	Admin Roles			
User Realms       Specify the resources for which this policy applies, one per line. In order for your sector Profiles         * Resource Profiles       * Resource Profiles         Junos Pulse       * Resource Profiles         * Maintenance       * Reles         Resource Profiles       * Reles         Resource Profiles       * Resources:         Maintenance       * Policy applies to ALL roles         System       • Policy applies to SELECTED roles         Push Config       • Policy applies to all roles OTHER THAN those selected below         Available roles:       # Artion         • Allow access       • Deny access         • Use Detailed Rules (see Detailed Rules page)       Save changes?         Done       Save Changes       Save as Copy	- lisers	Resources		
User Relations       * Resource Profiles         Resource Profiles          Resource Profiles          Junos Pulses          Paintenance          System          Import/Export          Push Config          Archiving          Troubleshooting          Policy applies to ALL roles         Policy applies to SELECTED roles         Policy applies to all roles OTHER THAN those selected below         Available roles:         Birds & Bees         Birds & Bees         Birds & Bees         Save changes?         Save Changes       Save as Copy	- Use Backson		Specify the resources for which this polic	y applies, one per line. In order for you
User Roles       * Resource Poilies         Resource Poilies       https://pinsafe. ctrl.local:8443/proxy*         Junos Pulse       *         Maintenance       *         System       *         Import/Export       *         Pub Config       *         Archiving       *         Troubleshooting       *         Policy applies to ALL roles       *         Archiving       *         Policy applies to SELECTED roles       *         Policy applies to all roles OTHER THAN those selected below         Available roles:       *         Birds & Bees       *         *       *         Action       *         Action       *         Save changes?       Save as Copy         Done       *	User Realms >			
Resource Policies >         Junos Pulse >>         Maintenance         System         Import/Export >         Push Config >         Archiving >         Troubleshooting >         Policy applies to ALL roles         O Policy applies to SELECTED roles         O Policy applies to all roles OTHER THAN those selected below         Available roles:         Birds & Bees         Extin         Action         Action         Action         Save changes?         Save Changes       Save as Copy	Oser Koles	* Resources:	https://pinsafe.	Examples: http://*domain.com/or
Note Pulse       10.10.10.10/25.25.25         Junos Pulse       10.10.10.10/24:8000-9         Waintenance       Policy applies to ALL roles         System       Policy applies to SELECTED roles         Policy applies to all roles OTHER THAN those selected below         Available roles:         Birds & Bees         Example         Action         Action         Allow access         Deny access         Use Detailed Rules (see Detailed Rules page)         Save changes?         Done	Resource Profiles P		ctrl.local:8443/proxy*	https://www.domain.com
Maintenance         System         Import/Export         Publ Config         Archiving         Troubleshooting         Policy applies to ALL roles         Archiving         Policy applies to SELECTED roles         Policy applies to all roles OTHER THAN those selected below         Available roles:         Birds & Bees         Birds & Bees         One	Junos Dulsa			10.10.10/255.255.25
System       Roles         Import/Export <ul> <li>Policy applies to ALL roles</li> <li>Policy applies to SELECTED roles</li> <li>Policy applies to all roles OTHER THAN those selected below</li> <li>Available roles:</li> <li>Birds &amp; Bees</li> <li>Action</li> </ul> Action           Action <ul> <li>Allow access</li> <li>Deny access</li> <li>Use Detailed Rules (see Detailed Rules page)</li> </ul> Save changes         Save as Copy	- Maintenance			- 10.10.10/24:8000-9
System       Roles         Import/Export       Policy applies to ALL roles         Archiving <ul> <li>Policy applies to SELECTED roles</li> <li>Policy applies to all roles OTHER THAN those selected below</li> <li>Available roles:</li> <li>Birds &amp; Bees</li> <li>Action</li> </ul> Action <ul> <li>Allow access</li> <li>Deny access</li> <li>Use Detailed Rules (see Detailed Rules page)</li> </ul> Save changes       Save as Copy				
Push Config         Archiving         Troubleshooting         Policy applies to ALL roles         Policy applies to SELECTED roles         Policy applies to all roles OTHER THAN those selected below         Available roles:         Birds & Bees         Image: Action         Action         Allow access         Deny access         Use Detailed Rules (see Detailed Rules page)         Save Changes       Save as Copy         Done	System >	Roles		
Archiving Archiving Troubleshooting Policy applies to ALL roles Policy applies to SELECTED roles Policy applies to all roles OTHER THAN those selected below Available roles: Birds & Bees Action Action Action Action Action Action Save changes? Done Done	Import/Export >			
Action     Action     Action     Action     Save changes?  Done	Archiving		Policy applies to ALL roles	
Policy applies to all roles OTHER THAN those selected below     Available roles:     Birds & Bees     Action     Action     Allow access     Deny access     Deny access     Use Detailed Rules (see <u>Detailed Rules</u> page)     Save changes     Save Changes     Save as Copy Done	Troubleshooting		Policy applies to SELECTED ro	les
Available roles: Birds & Bees Action Action Action Action Action Action Action Action Action Action Action Birds & Bees Deny access Deny access Use Detailed Rules (see <u>Detailed Rules</u> page) Save changes Save changes Save as Copy Done	inconcisionality .		Delicy applies to all relat OTH	CD THAN these selected below
Available roles: Birds & Bees Action Action Action Action Action Output access Deny access Deny access Use Detailed Rules (see <u>Detailed Rules</u> page) Save changes? Save changes Save as Copy Done			Policy applies to all roles OTH	ER THAN those selected below
Available roles: Birds & Bees Action Action Action Action Allow access Deny access Use Detailed Rules (see <u>Detailed Rules</u> page) Save changes? Save Changes Save as Copy Done			Available releas	
Action  Action  Action  Action  Allow access  Deny access  Use Detailed Rules (see Detailed Rules page)  Save changes?  Save changes Save as Copy  Done			Available foles:	
Action  Action  Action  Action  Allow access  Deny access  Use Detailed Rules (see <u>Detailed Rules page</u> )  Save changes?  Save Changes Save as Copy  Done			Birds & Bees	<u>^</u>
Action  Action  Action  Action  Allow access  Deny access  Duse Detailed Rules (see Detailed Rules page)  Save changes?  Save Changes Save as Copy  Done				(=) C
Action  Action  Action  Action  Action  Action  Action  Save changes?  Deny access  Use Detailed Rules (see Detailed Rules page)  Save changes  Save changes  Save Changes Save as Copy  Done				
Action   Action   Action   Action				
Action	-			
Action				
<ul> <li>Allow access</li> <li>Deny access</li> <li>Use Detailed Rules (see <u>Detailed Rules</u> page)</li> </ul> Save changes?       Save Changes     Save as Copy   Done		Action		
Deny access Deny access Use Detailed Rules (see <u>Detailed Rules</u> page) Save changes Save Changes Save as Copy Done				
© Deny access © Use Detailed Rules (see <u>Detailed Rules</u> page) Save changes? Save Changes Save as Copy Done			Allow access	
© Use Detailed Rules (see <u>Detailed Rules</u> page) Save changes? Save Changes Save as Copy Done			Deny access	
Save changes? Save Changes Save as Copy Done			O Use Detailed Rules (see Detail	ed Rules page)
Save changes? Save Changes Save as Copy Done				
Done		Cause shares a		
Save Changes Save as Copy Done		bave changes?		
Done			Save Changes Save as Con	V
Done				<u> </u>
Done				
	Done			

### 357.1.3 Creating the Virtual Hostname

To create a Virtual DNS entry, on the Juniper SA select the Authentication/Signing In/Sign-In Policies and then select New URL. Select the Authorization Only Access radio button for User type. Complete the following information:

Virtual Hostname: enter the DNS name that will point to the Swivel virtual or hardware appliance for the TURing image.

Example: turing.swivelsecure.com/

Backend URL: enter the protocol, IP address and port of the Swivel virtual or hardware appliance

Example for a Swivel virtual or hardware appliance: http://192.168.0.35:8443/*

For a software only install see Software Only Installation

Authorization Server: select No Authorization

Role Option: Select a Role

Save the Changes

<u>signing In</u> > juniper.swivelsed	cure.com/	
Save Changes		
User type:	🔍 Users 🔍 Administrators 🖉 Auth	norization Only Access
Virtual Hostname:	juniper.swivelsecure.com/	Clients connect to a virtual hostname on the
Backend URL:	http://192.168.0.215:8443/*	Required: Protocol, hostname and port of the Server paths are not supported.
Description:	Turing Proxy	
Authorization Server:	[No Authorization]	
Role Option:	AnonyRole Not all role options will apply. See admin guide.	
Save changes?		
Save Changes		



### 357.1.4 Verifying the Virtual DNS Entry

Swivel virtual or hardware appliance

From within the network verify the Swivel server is working using the below to generate a TURing image

http://<PINsafe appliance URL>:8443/proxy/SCImage?username=test

Then verify the external access using

#### Software Install

For a software only install see Software Only Installation

Then verify the external access using

https://<turing.mycompany.com>/pinsafe/SCImage?username=test

# 357.2 Login Page Modifications for Single Channel Authentication and SMS On Demand

The sample pages provided by Juniper on the current version to be integrated, should always be used, as these are the supplied compatible pages and contain the latest updates and security features. To obtain these, login to the Juniper and select Signing-In, Sign-in pages, then click on Upload Custom Pages.



Click on the **Sample** and download the latest sample pages. This is a zip file, and any additional files or changes will need to be added back to the zip file with the original contents, to be uploaded again.

~			
		ner	
7			
<u>n</u> 2	NETWORKS	and the second second	

Central Manager	
- System	
Status >	Signing In >
Configuration +	Upload Custom Sign-In Pages
Network >	
Clustering >	Custom sign-in pages allow you to provide customized templates for various pages that
Log/Monitoring →	appear during the sign-in process. Refer to the documentation for information about
<ul> <li>Authentication</li> </ul>	creating valid templates.
Signing In Endpoint Security >	Sign-In Pages
Auth. Servers	Name:
- Administrators	Label to reference the custom sign-in pages
Admin Realms >	Laber to reference the costoff sign-in pages.
Admin Roles >	Page Type: Access O Meeting
- Users	Page Type. O Access O Meeting
User Realms →	Templates File:
User Roles >	Zip file containing the custom templates and assets.
Resource Profiles +	
Resource Policies >	Upload
- Maintenance	
System >	skip validation checks during upload
Import/Export >	
Push Config	
Archiving +	Upload Custom Pages
Troubleshooting >	

Using the sample login pages we can add the Swivel modified pages (see prerequisites), and change them to suit the integration requirements.

The configuration section within LoginPage.thtml should be edited to suit your environment as the below modifications.

If you are using the combined PC and tablet version, you should make these changes to swivel-header.thtml.

### 357.2.1 Modifying the Login Page

OTC_OPTION Controls how the TURing image will be displayed to the user

Option	Description	Single channel Option	Dual Channel Option
image	When the user tabs down from the username field, the TURing will automatically show	Y	N
button	The login page will present a TURing button. Click the button to display the TURing	Y	Y
disable	No TURing image	Y	Y

#### OTC_RANDOM Displays a button on screen to refresh the TURing image

Option	Description	Single channel Option	Dual Channel Option
true	Button will be displayed	Y	Y
false	No button	Y	Y

#### TURingImage URL for generating a TURing image

Option	Description	Single channel Option	Dual Channel Option
URL (see below)	Change the TURingImage value to reflect the IP address of the Swivel appliance	Y	Y

The URL may be one of the following:

#### Using Virtual DNS

#### Swivel appliance

https://virtual_hostname/proxy/SCImage?username=";

#### Software install

http://virtual_hostname/pinsafe/SCImage?username=";

• For a NAT or Public IP address

#### Swivel appliance

https://hostname:8443/proxy/SCImage?username=";

For a software only install see Software Only Installation

#### 357.2.2 Modifying the Welcome Message

To customise login page welcome message, you must edit the LoginPage.thtml (and LoginPage-stdaln.thtml if using Network Connect):

Search and remove the following:

<% welcome FILTER verbatim %>

This references the first line of the Welcome message. E.g. change this to "Welcome to the"

Search and remove the following:

<% portal FILTER verbatim %>

This references the second line of the Welcome message. E.g. change this to "Swivel Secure Login Page"

#### 357.2.3 Modifying the login for SMS Only requests

Swivel supports SMS on Demand, SMS in advance and SMS using Two Stage authentication. Where SMS on demand only, is used, the login page may be modified so that instead of generating a TURing image a SMS is sent to the user. Locate the following line:

https://virtual_hostname/proxy/SCImage?username=";

and modify the SCImage?username=" to DCMessage?username=;

Example:

Using Virtual DNS

Swivel appliance

https://virtual_hostname/proxy/DCMessage?username=";

Software install

http://virtual_hostname/pinsafe/DCMessage?username=";

• For a NAT or Public IP address

Swivel appliance

https://hostname:8443/proxy/DCMessage?username=";

For a software only install see Software Only Installation

#### 357.2.4 Modifying the login button text

The login page button and link to Get Another Image may be modified.

To modify the login button text locate the text value='Turing' and replace the Turing with the required text.

To modify the Get another image? URL, locate the two instances of Get another image? and change the text as required.

#### 357.2.5 Modifying the login for PINpad

Customising for Pinpad can be done using the same custom pages as above. Follow the same instructions as above, except the following:

- The zip file contains 3 additional images that need to go into the *imgs* folder of the Juniper custom login.
- OTC_OPTION needs to be set to "pinpad".
- You need to set the value for PinpadImage, rather than TURingImage to match your own Swivel instance.

Example

to

#### var PinpadImage = "https://hostname:8443/pinsafe/SCPinPad?username=";

#### 357.2.6 Modifying the Login pages for Mobile Devices

The prerequisites section contains the mobile modified pages that can be uploaded with any other modified pages to ad wivel authentication to the login. Modify the file PageHeader-mobile-webkit.thtml, find the below line and change the link for the Swivel appliance as the standard login page above. var TURingImage = "https://pinsafe.company.com/proxy/SCImage?username=";

Instant Virtual E	xtranet 📑 🗧 🗟 ː 🕅
Instant Virtua	I Extranet
Please sign in to be	gin your secure session.
username	test
password	•••••
One-Time Co	de
Turing	
	5 6 7 8 9 0 E/L Y E A 5
	Sign In

#### 357.2.7 Juniper Network Connect login page modification

The Juniper Network Connect can be started directly, and to customise the login page for Swivel authentication copy the login.thtml page to LoginPage-stdaln.thtml

🐥 Network Conn	ect - Sign In			- <b>X</b>
Tools				
Sign-in Page:	https://juniper/swivelsecu	e.com	Go	
Swi	VEL [®] on Solutions			*
We	lcome to t	he Swive	el Secure VPN	
userna passw	me ord		Please sign in to begin your secure session.	
One-T Code	ime			
	Sign In			
				-

Juniper Network Connect with TURing

Iools         Signin Page:       https://juniper.swivelsecure.com         Image:       https://juniper.swivelsecure.com         Image:       Image:         Authentication Solutions         Image:       Image:         Image:       Image: <th>A Network Connect - 3</th> <th>Sign In</th> <th></th> <th></th> <th>X</th>	A Network Connect - 3	Sign In			X
Sign-in Page: https://juniper.swivelsecure.com     Second Solutions     Welcome to the Swivel Secure VPN     username   graham   password   One-Time     Sign In     1 2 3 4 5 6 7 8 9 0   Weight Secure 3	Tools				
Authentication Solutions          Welcome to the Swivel Secure VPN         username       graham         password       Please sign in to begin your secure session.         One-Time       One-Time         Sign In       1 2 3 4 5 6 7 8 9 0         W B O E P O TO J O F         Get another image?	Sign-in Page: http	os://juniper.swivelsecure.com	▼ Go		
	Authentication Se Welco username password One-Time Code	Sign In Sign In Get another image?	vivel Secur 6 7 8 9 0 D M J D H	e VPN Please sign in to begin your secure session.	E

### 357.2.8 Uploading the Modified Page

Ensure all the modified files are included with the zip file to upload to the Swivel server. On the Juniper select Signing In/Sign-in Pages then click on Upload Custom Pages.

	er°	
Central Manager		
System Status	Signing In	
Configuration   Network   Clustering   Log/Monitoring	Sign-in Policies Sign-in Pages	
Signing In   Endpoint Security	Sign-In Page	тур
Auth. Servers Administrators Admin Realms	Default Sign-In Page Meeting Sign-In Page	Sta Sta
Admin Roles → Ξ Users		
User Realms > User Roles > Resource Profiles > Resource Policies >		
Maintenance System → Import/Export → Push Confin		
Archiving > Troubleshooting >		

Enter a Name for the Custom page, then use Browse to find the location of the Templates file. Then click on the Upload Custom Pages, observe any errors that may occur.

# 

Central Manager	
System Status Configuration Network Clustering Log/Monitoring Authentication	Signing In > Upload Custom Sign-In Pages Custom sign-in pages allow you to provide customized templates for various pages that appear during the sign-in process. Refer to the documentation for information about creating valid templates.
Signing In → Endpoint Security →	Sign-In Pages
Auth. Servers - Administrators	Name: PINsafe Label to reference the custom sign-in pages.
Admin Realms → Admin Roles → Users	Page Type: <ul> <li>Access</li> <li>Meeting</li> </ul>
User Realms User Roles Resource Profiles	Templates File: C:\Documents and Setting Browse Zip file containing the custom templates and assets.
Resource Policies >	Upload
Maintenance System Import/Export Push Config Archiving Troubleshooting	skip validation checks during upload

The new signing in page should be listed.

# 

Cen	tral	Ma	nao	er

Central Manager		
- System		
Status >	Signing In	
Configuration >		
Network +	Sign-in Policies Sign-in Pages	
Clustering +		
Log/Monitoring	New Page Upload Custom Pages Delate	
Authentication	Unew Page Delete	
Signing In		
Endpoint Security +	Sign-In Page	Туре
Administrators	PINsafe	Cust
Auministrators	Default Sign-In Page	Stan
Admin Realms >		Starr
Admin Roles >	Meeting Sign-In Page	Stan
- Users		
User Realms →		
User Roles >>		
Resource Profiles +		
Resource Policies >		
- Maintenance		
System >		
Import/Export >		
Push Config		
Archiving +		
Troubleshooting +		

# 358 Verifying the Installation

Navigate to the login page and verify that the page is as expected. Test a login using an OTC and verify the user can login with a correct OTC an fails with an incorrect OTC.

**Dual Channel Authentication** 

SWIVEL® Authentication Solutions	
Welcome to th	e Swivel Secure VPN
username	Please sign in to begin your secure session.
password	
One-Time Code	
Sign In	

Single Channel Authentication



# 359 Uninstalling the Swivel Integration

To remove Swivel, remove the customised page, Swivel realm, and Swivel Policy.

# 360 Troubleshooting

Check the Swivel logs. If the Single Channel image is used then a 'session start' should be see for the username. RADIUS authentication requests should be seen for successful or failed login attempts.

Check the Juniper logs, look for user authentication requests.

If the TURing image is not visible, right click on the red cross and view the details of the image URL.

Copy and paste this URL into a separate web browser, observe any certificate errors.

Welcome to the	
Swivel Secure VPN	Access Page
username bob password	Please sign in to begin your secure session.
Sign In	
Turing	
×	

#### **Internal Certificate Authorities**

If an internal certificate authority is used, then the Single Channel image may not be accessible externally unless the client has installed the certificate as a trusted root certificate. Using a valid public certificate will remove this requirement.

#### domain\username is used instead of username

On the Juniper when USER is used then the domain name may be added in the authentication request to the Swivel instance in the form domain/username. When USERNAME is used then just the username is sent to the Juniper.

# 361 Known Issues and Limitations

"ExceededConcurrent.thtml" is not found in zip file.

Ensure that the file is present.

Make sure that the files are not located in a sub-directory within the zip folder

Select All of the files within the folder and then send to a zip folder

## 361.1 iPhone, iPad iOS automatic TURing image generation issue

The Onblur method in Javascript does not work in iOS, so a TURing button would need to be created to request the image after the username has been entered.

<a class="wide confirm buttonTxt" href="#" onclick="var frm = document.getElementById('frmLogin'); if (onFormSubmit()) { frm.submit(); }">Si

A modified login page is available here: iPad modified login page

## 361.2 Authentication fails after upgrading Swivel

In Swivel 3.8, the domain name was automatically removed for RADIUS authentication. However, this prevents authentication in cases where the domain\ prefix is required.

Assuming PINsafe is not the primary authentication, this can be worked around by changing the value passed to Swivel by the Juniper as <USERNAME>, rather than <USER>. This is in the Juniper settings for secondary authentication: "Username is predefined as".

# **362 Additional Information**

Custom sign-in pages for Pinpad can be found here.

# 363 Juniper Two Stage Challenge and Response

## 363.1 Juniper Two Stage and Challenge and Response Authentication

## 363.2 Introduction

Juniper supports the use of a challenge and response whereby a password is used prior to entering a One Time Code. In addition the Challenge and Response mechanism allows an SMS to be sent upon successful entry of a password.

## 363.3 Prerequisites

PINsafe 3.7

Juniper 6.x

Dual Channel authentication

Two stage authentication requires the use of either a PINsafe password, or that Check password with repository is enabled.

## 363.4 Baseline

PINsafe 3.7

Juniper 6.4

## 363.5 Architecture

Juniper using RADIUS authentication to the PINsafe server, with security strings sent to the user using an SMS gateway.

## 363.6 Installation

Configure the PINsafe server and Juniper appliance for Dual Channel Authentication. Ensure either the user has a PINsafe password, or that Check password with repository is enabled.

# 363.7 Adding Two Stage Authentication

See also: Two Stage Authentication How to Guide

On the PINsafe Administration Console server select RADIUS/NAS and the Access device which two stage authentication is required. Set the Two stage Auth to Yes and Apply.

RAD	IUS>NAS 🕘		
Please e authent	enter the details for an ication services of the	y RADIUS network access se PINsafe server via the RADI	rvers. A NAS is permitted to access the US interface.
NAS:	Identifier:	VPN	
	Hostname/IP:	1.1.1.1	
	Secret:	•••••	
	EAP protocol:	None	
	Group:	ANY	
	Authentication Mode:	All	
	Change PIN warning:	No 💌	
	Vendor (Groups):	None	
	Two Stage Auth:	Yes 💌	Delete

On the Juniper Administration Console, browse to the Authentication/Auth Servers menu, and select the PINsafe RADIUS authentication server. Under Custom RADIUS Rules click on the New RADIUS Rule button.

Timeout	t:	30 seconds			
Retries:		0			
Vse Note and	rs authentica e: If you select t this credential v	te using tokens or one- this, the device will send the will not be used in automati	time passwords a user's authentication me c SSO to backend applicat	ethod as "token" if you use SAML, tions.	
Backup S	Server (required	l only if Backup server exis	ts)		
Radius S	Server:		Name or IP address		
Authent	tication Port:				
Shared	Secret:				
Accoun	ting Port:		Port used for Radius acc	counting, if applicable	
Radius ad	ccounting				
User-Na	ame:	<user>(<realm>)</realm></user>	<pre>(<role login="" name<br="" s="" sep='&lt;/pre&gt;&lt;/th&gt;&lt;th&gt;Template for reporting user&lt;/th&gt;&lt;th&gt;ide&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;The template can cont&lt;br&gt;a list of all variables.&lt;/th&gt;&lt;th&gt;ain textual characters as v&lt;/th&gt;&lt;th&gt;well as variables for substitution. Variables sho&lt;/th&gt;&lt;th&gt;bub&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;Interim&lt;br&gt;T Use&lt;/th&gt;&lt;th&gt;Update Inter&lt;br&gt;NC assigned&lt;/th&gt;&lt;th&gt;Examples:&lt;br&gt;&lt;USER&gt; The of&lt;br&gt;&lt;REALM&gt; The of&lt;br&gt;&lt;ROLE SEP=","&gt; The of&lt;br&gt;&lt;ROLE&gt; The of&lt;br&gt;&lt;ROLE&gt; The of&lt;br&gt;val: minutes&lt;br&gt;IP Address for FRAMED&lt;/th&gt;&lt;th&gt;user'>user's sign-in realm ist of ","-separated roles first role amongst multiple - IP-ADDRESS attribut</role></pre>	assigned to the user a roles assigned to the user Time interval to send an int (min: 15 minutes, max: 14- ce value in Radius Accounting	eri 40
Custom F	Radius Rules				
Delete		New Radius Rule			
	Name	Response Packet Ty	pe	Attribute criteria	
	PIN	Access Challenge			
Sav	e Changes	Reset			

Enter a name for the Rule and ensure Response Packet Type is set to Access Challenge.

Under Attribute Criteria ensure RADIUS Attribute is set to Reply Message (18), with the Operand matches the expression, leave the value setting blank. Ensure that the radio button for ?Show Generic Login Page? is selected.

Click on Save Changes.

Auth Servers > PINsafe > Edit Custom Radius Rule	•		
Name: PIN			
If received Radius Response Packet			
Response Packet Type: Access Ch	allenge 🔽		
Attribute criteria:			
Radius Attribute	Operand	Value	
Reply-Message (18)	matches the expression		Add
Then take action			
C show New Pin page			
Show Next Token page			
• show Generic Login page			
C show user login page with error	or message		
c 🔤			
C show <b>Reply-Message</b> attr user	ibute from the Radius server to	the	
• send Access Request with add	litional attributes		
Radius Attribute	Value		
User-Name (1)	•	Add	
Save Changes ?			

# 363.8 Adding Challenge and response Authentication

See also: Challenge and Response How to Guide

For PINsafe 3.7 and later, on the PINsafe Administration Console server select RADIUS/NAS and ensure the Two Stage Auth is set to Yes, then click on Apply.

RAD	IUS>NAS 🥘			
Please e authent	enter the details for an tication services of the	y RADIUS network a PINsafe server via	access serve the RADIUS	ers. A NAS is permitted to access the interface.
NAS:	Identifier:	VPN		
	Hostname/IP:	1.1.1.1		
	Secret:	•••••	•••••	
	EAP protocol:	None 💌		
	Group:	ANY	•	
	Authentication Mode:	All		
	Change PIN warning:	No 💌		
	Vendor (Groups):	None		
	Two Stage Auth:	Yes 💌		Delete

For PINsafe 3.6 and earlier, on the PINsafe Administration Console server select RADIUS/Server and ensure the Use Challenge/Response is set to Yes, then click on Apply.

RADIUS>Server	8
Please enter the details for t	he RADIUS server.
Server enabled:	Yes 💌
IP address:	
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No 💌
Additional RADIUS logging:	Both
Enable debug:	Yes 💌
Radius Groups:	No 💌
Radius Group Keyword:	
Use Challenge/Response:	Yes 💌
	Apply Reset

On the PINsafe Administration Console server select Server/Dual Channel. For delivery of a new security string upon entering a correct password, ensure On-Demand Authentication is set to Yes, then click on Apply.

# Server>Dual Channel @

Please select whether dual channel security string messages are delivered preemptively or on demand at t point of authentication.

On-demand authentication:	Yes 💌
Allow message request by username:	Yes 💌
Confirmation image on message request:	Yes 💌
On-demand delivery:	No 💌
Multiple authentications per String:	Yes 💌
Apply	Reset

# 363.9 Combining Juniper and PINsafe Two Stage Authentication

Using the Juniper AD authentication is useful for single Sign On (SSO) features, so it may be of use to combine the Juniper Two Stage login with that of the PINsafe Two Stage authentication in order to send the user a security string or OTC when the AD password is entered. To configure this:

Enable Two Stage Authentication on the Juniper

Enable two Stage Authentication on the PINsafe Administration Console

Enable Check Password with Repository on the PINsafe Administration Console, See Check Password With Repository

On the Juniper select the User Realm relating to the required Authentication Realm and change the set Password is: to the value Predefined as <PASSWORD>

When an authentication is made, the AD password is used for the Juniper and the PINsafe Two Stage Authentication so it does not need to be entered twice.

## 363.10 Verifying the Installation

Check the PINsafe logs

Check the Juniper logs

# 363.11 Troubleshooting

View the users security string to ensure the correct security string is being used.

Ensure authentication is working with standard authentication.

## 363.12 Known Issues and Limitations

PINsafe 3.7 Beta required the use of Multiple Authentications per string to be enabled for dual/single channel located on the PINsafe Administration console under Server/Single Channel or Server/Dual Channel.

# 363.13 Additional Information

Juniper can also be configured for Constrained Delegation where a PINsafe One Time Code is entered and this signs the user into their AD applications without the use of an AD password in the login process. See the following documentation: http://www.juniper.net/techpubs/software/ive/6.x/6.4/

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

# 364 Microsoft Direct Access Integration

# **365 Introduction**

Microsoft Direct Access allows a VPN connection to be brought up when a user requires access to an organisations internal resources. PINsafe can authenticate a user accessing those internal resources using Dual channel authentication such as SMS, Mobile Phone Client and the Taskbar utility Taskbar How to Guide and Token.

# **366 Prerequisites**

Microsoft Direct Access fully configured

Microsoft CA server for OTP authentication

PINsafe 3.x

# 367 Baseline

Microsoft UAG SP1 with Direct access configured

PINsafe 3.8

# 368 Architecture

When a Direct Access connection is made, a pop up appears for the user prompting them to enter their One Time Code. This is then checked by the UAG against PINsafe using RADIUS authentication.

# 369 Installation

# 369.1 PINsafe Configuration

## 369.1.1 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 appliances, the PINsafe VIP should not be used as the server IP address, see VIP on PINsafe Appliances

RADIUS>Server 😕		
Please enter the details for the RADIUS server.		
Server enabled:	Yes 💌	
IP address:	0.0.0.0	
Authentication port:	1812	
Accounting port:	1813	
Maximum no. sessions:	50	
Permit empty attributes:	No 💌	
Filter ID:	No 💌	
Additional RADIUS logging:	Both 💌	
Enable debug:	Yes	
Radius Groups:	Yes 💌	
Radius Group Keyword:	POLICY	
	Apply Reset	

#### 369.1.2 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.

# RADIUS>NAS 🥑

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther via the RADIUS interface.

NAS:	Identifier:	Device Name
	Hostname/IP:	192.168.0.1
	Secret:	•••••
	EAP protocol:	None
	Group:	ANY
	Authentication Mode:	All
	Change PIN warning:	No 💌
		Apply Reset

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.

#### 369.1.3 Enabling Session creation with username

PINsafe can be configured to use the Taskbar to present a TURing image to users when prompted for authentication by Direct Access. See Taskbar How to Guide

To allow Single Channel authentication on PINsafe follow the below steps.

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:

Appliance

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

For a software only install see Software Only Installation

## 369.2 Microsoft Direct Access Integration

Ensure that the Microsoft Direct Access is fully working and tested before startigng the PINsafe integration.

#### 369.2.1 Enable Two Factor Authentication

On the Forefront UAG Direct Access configuration page select under Step 2 Optional Settings the link for Two-Factor Authentication



Click on Require two-factor authentication
UAG DirectAccess Server	Configuration
Two-Factor Au	Ithentication Configuration
Client Authentication	You can require clients to use two-factor authentication. Select the method used by UAG DirectAcc for two-factor authentication.
	Require two-factor authentication
	C Clients will log on using a PKI smart card
	C Clients will authenticate using a one-time password (OTP)
Learn more	< <u>B</u> ack <u>N</u> ext > <u>F</u> inis

Click on Clients will authenticate using a one-time password (OTP)

a UAG DirectAccess Server	Configuration	
<b>Two-Factor Au</b> Client Authentication OTP Authentication	Ithentication Configuration           You can require clients to use two-factor authentication. Select the method used by UAG DirectAd for two-factor authentication.	
OTP CA Servers	Require two-factor authentication	
on on templates	C Clients will log on using a PKI smart card	
	Clients will authenticate using a one-time password (OTP)	
Learn more	< <u>B</u> ack <u>N</u> ext > <u>F</u> in	

## 369.2.2 Configure OTP Authentication Server

On the OTP Authentication tab click Add

Carl UAG DirectAccess Server C	onfiguration
Two-Factor Au Client Authentication OTP Authentication OTP CA Servers OTP CA Templates	thentication Configuration         DirectAccess client authentication is configured to use OTP. Select the OTP authentication server.         OTP authentication server:         Image: Configuration of the OTP authentication server of the OTP authentication server.         Image: Configuration of the OTP authentication server of the OTP authentication server of the OTP authentication servers can be edited and deleted in the Authentication and Authorization Servers dialog box, available in the Admin menu.
	Require OTP user names to match Active Directory user names With this setting enabled, users log on in UPN format (username@domain).
Learn more	< <u>B</u> ack <u>N</u> ext > <u>F</u> ini

Select Server Type RADIUS and enter the following information:

- Server Name: A descriptive name for the RADIUS server
  Port: RADIUS port used by the Swivel server, usually 1812
  IP address/host: The Swivel RADIUS server
  Alternate IP/host: A secondary Swivel RADIUS server
  Alternate port: The port used by the secondary Swivel server, usually 1812
  Secret Key: A shared secret entered on the Swivel servers.

d Authentication S	erver	
Server type:	S RADIUS	•
Server name:	RADIUS	
IP address/host:	192.168.1.100	
Port:	1812	
Alternate IP/host:	192.168.1.101	
Alternate port:	1813	
Secret key:	••••	
	OK	Cancel

Ensure that the new Swivel server is selected. Optionally select *Require OTP user names to match Active Directory user names with this setting enabled, users log on in UPN format (username@domain).* then the user name will be automatically populated at the direct access login.

NG DirectAccess Server C	onfiguration		
Two-Factor Au	thentication Configuration		
Client Authentication OTP Authentication	DirectAccess client authentication is configured t	to use OTP. Select the	OTP authentication serv
OTP CA Servers	OTP authentication server:		·
	The OTP authentication servers can be edi Authorization Servers dialog box, available Require OTP user names to match Active Dire With this setting enabled, users log on in UPI	ted and deleted in the e in the Admin menu. ectory user names N format (username@	e Authentication and
Learn more		< <u>B</u> ack	Next >

## 369.2.3 CA Server Configuration

Under OTP CA Servers click on Add and select the OTP CA Server.

Client Authentication OTP Authentication	UAG DirectAccess uses certificates for OTP authentication. Select the CA servers that will issue certit specify how CA templates are configured and deployed.
OTP CA Servers OTP CA Templates	Specify the OTP <u>C</u> A servers. Add them in the order they should be queried during OTP authentication
	Common parent CA to which the OTP CA servers chain:
	Select how CA templates are deployed:  Use a UAG DirectAccess script to configure CA templates and automatic renewal  Use existing CA templates located on the CA servers, and configure automatic renewal manu  When you create the script on the next page of the wizard, you can apply it immediately, script and apply it at a later time. When you apply the script, all existing CA templates are the CA servers

This example is configured to use existing CA templates.

E.

Client Authentication OTP Authentication	UAG DirectAccess uses certificates for OTP authentication. Select the CA servers that will issue certif specify how CA templates are configured and deployed.
OTP CA Servers OTP CA Templates	SVVCERT
	Common parent CA to which the OTP CA servers chain:
	SVVCERT
	Select how CA templates are deployed: Use a UAG DirectAccess script to configure CA templates and automatic renewal Use existing CA templates located on the CA servers, and configure automatic renewal manual
	If you use existing CA templates, configure them manually on the CA servers, and select th page of the wizard.

Select the required templates

Client Authentication	Select the CA template used for issuing certificates for OTP client authentication and identifying the UAG DirectAccess server to OTP clients. Specify a certificate renewal policy.			
OTP CA Servers	OTP certificate template for client authentication:			
OTP CA Templates	OTPUser			
	OTP certificate template for workstation authentication:			
	OTPWorkstation			
	Enable certificate renewal. Maximum renewal period (days):			
	When you select this option, you have to configure the selected templates on the CA ser OTP authentication. They will not be configured automatically by UAG DirectAccess.			
	Click to verify that the CA servers can be used for OTP authentication: Valida			
	Certificate OTPUser cannot be enrolled. Ensure that each UAG DirectAccess server has Er			

Validate the CA templates

💐 UAG DirectAccess Server (	Configuration	
Two-Factor Au	thentication Configuration	
Client Authentication OTP Authentication OTP CA Servers	Select the CA template used for issuing certificates for OTP client authentication and identifying the UAG DirectAccess server to OTP clients. Specify a certificate renewal policy. OTP certificate template for client authentication:	
OTP CA Templates	OTPUser 💌	
	OTP certificate template for workstation authentication:	
	OTPWorkstation	
	Enable certificate renewal. Maximum renewal period (days): 7	
	When you select this option, you have to configure the selected templates on the CA ser OTP authentication. They will not be configured automatically by UAG DirectAccess.	
	Click to verify that the CA servers can be used for OTP authentication: Valida	
	Validation successful. CA servers are configured correctly.	
Learn more	< <u>B</u> ack <u>N</u> ext > <u>F</u> ini	

369.3 Additional Installation Options

# 370 Verifying the Installation

Access with the Direct Access client entering username, AD password and One Time Code. If the option to *Require OTP user names to match Active Directory user names* then the user name will be automatically populated.

Check the UAG and PINsafe logs for authentication messages.

# 371 Uninstalling the PINsafe Integration

# 372 Troubleshooting

# **373 Known Issues and Limitations**

## **374 Additional Information**

Microsoft DirectAccess

## **375 Microsoft IAG Integration**

## 375.1 Introduction

This document covers the integration of PINsafe with the Microsoft Intelligent Application Gateway.

## **375.2 Prerequisites**

PINsafe 3.x

Microsoft IAG

The IAG integration guide can be found here: IAG SP1 Integration Guide and here SP2 Integration Guide

- 375.3 Baseline
- **375.4 Architecture**
- 375.5 Installation
- 375.5.1 PINsafe Integration Configuration
- 375.5.2 Access Device or Application Integration
- 375.5.3 Additional Installation Options
- 375.6 Verifying the Installation
- 375.7 Uninstalling the PINsafe Integration

## 375.8 Troubleshooting

- **375.9 Known Issues and Limitations**
- 375.10 Additional Information

## **376 Microsoft IAG Multiple Authentication**

### 376.1 PINsafe and IAG/UAG Integration using multiple repositories

This article explains how to use PINsafe with Microsoft IAG/UAG so that different applications are available to users depending on how they authenticated.

These notes are based on IAG Version 3.7 and PINsafe Version 3.6

This article shows the approach required to add this functionality to a standard IAG/UAG and PINsafe integration. Standard integration notes are available from the Microsoft IAG Integration guide and should also be referred to.

### 376.2 Approach

The approach is to create two different repositories on the IAG. One repository will use Agent-XML for authentication the other will use RADIUS.

One repository will be associated with single channel authentication, the other with dual channel authentication.

The login page will determine which repository the user is authenticating based on whether the user has requested a single channel (TURing) image or not.

The IAG will be configured to allow access to specific applications based on the repository a user has authenticated to.\

On the PINsafe server the NAS or Agent associated with the IAG Dual channel repository will be set to accept dual channel authentication only.

#### **376.3 Implementation**

The names used for repositories etc are just examples, but sometimes names are important, eg the repository of type "other" needs to have the same name as the associated .inc file and needs to reflected in the checkradio() function in PinsafeLogin.asp

#### 376.3.1 PINsafe Configuration

In this example radius will be used for dual channel authentications only so on the PINsafe server

Enable RADIUS server

Create a NAS entry for the IAG

Set ip address and shared secret as required

Set mode to dual channel only for the NAS

Create an Agent entry for the IAG

Set ip address and shared secret as required

#### 376.3.2 IAG Repository Configuration

Copy images.asp to von\IntnernalSite\Images\CustomUpdate

Ensure that it is the version that can also handle index images and ensure that the IP addresses etc match the PINsafe server

```
if request.querystring("index") <> "" then
    Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
    objWinHttp.Open "GET", "http://127.0.0.1:8080/pinsafe/DCIndexImage?username="&request.querystring("username"), false
else
    Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
    objWinHttp.Open "GET", "http://127.0.0.1:8080/pinsafe/SCImage?username="&request.querystring("username"), false
end if
```

Create a new Repository called pinsafe of type other.

Copy the pinsafe.inc file to von\InternalSite\inc\CustomUpdate

Edit pinsafe.inc so that the secret (m_secret), ip address and port matches that of the PINsafe server

```
function checkswivelpwd (userName, password)
LIGHT_TRACE "checkswivelpwd entered for " & userName
LIGHT_TRACE "SWIVEL - lets check if the password is right"
Dim strHTML
m_secret = "secret"
Dim objWinHttp
m_request = "<?xml version=""1.0"" ?><SASRequest><Version>1.0</Version><Action>login</Action><Username>" & username & "</Username><OTC>" & pa
& m_secret & "</Secret></SASRequest>"
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
objWinHttp.Open "GET", "http://<ipaddress>:8080/pinsafe/AgentXML?xml=" & m_request, false
```

Create a new Repository called pinsaferadius or type RADIUS.

Enter the details of the PINsafe RADIUS server on the config screen.

#### 376.3.3 Trunk Configuration

For the trunk you are using eg portal, ensure that both pinsafe and pinsaferadius repositories are associatd with the page

Also ensure that the option User Selects from A List of Servers is set

Set the login pages to be PINsafeLogin.jsp

Application Access Portal	ispection 🖉 🔎 Global URL Settings
😵 General 🛛 🔉 Authentication	Session 🥥 Application Cus
Authenticate User on Session Login	Logoff Scheme
Select Authentication Servers:	/internalSite/LogoffMsg asp
i pinsaferadius Add	
ill pinsafe Remove	Logoff Message: /InternalSite/LogoffMsg.asp
	Wait 30 Sec. After Logoff UBL to Terminate Session
	Pass the Logoff to the Application Server
User Selects From a List of Servers	Send Logoff Response to Browser
Show Server Names	
C User Must Provide Credentials for Each Selected Server	
🔽 Use the Same User Name	
C Use Integrated Windows authentication	
🔽 Enable NTLM protocol	
🔽 Enable Kerberos protocol	
Enable Users to Add Credentials On-the-Fly	
Enable Users to Change Their Passwords	
Notify User 7 Days Prior to Expiration	
Enable Users to Manage Their Credentials	
Enable Users to Select Language	
Skip client compliance checks when accessing a SharePoint site outside of a session	
Login Page: PinsafeLogin.asp	
On-the-Fly Login Page: PinsafeLogin.asp	
Permitted Authentication Attempts: 3	
Block Period: 0 Minutes	

Now copy the PINsafeLogin.jsp to von\InternalSite

Edit the PINsafeLogin.jsp to ensure that the repository names match those that you are using and that the dual channel and single channel authentication are matched to the correct repository.

```
function checkradio()
{
  var radiovalue = eval(document.form1.swivel[1].checked);
  var r = document.getElementById("repository");
  if (radiovalue == true)
  {
    //alert("turing");
    //TURing selected, therefore refresh TURing image
    updateotp();
    //repository for TURing is pinsafe
    r.value = "pinsafe"
    } else{
    //alert("sms");
    updateindex(); //if we are using multi-sms update index will display required index
    r.value = "pinsaferadius"
    //repository for TURing is pinsaferadius
    }
}
```

#### 376.3.4 Application Authorization

With different repositories aligned to different authentication methods, it is possible then to make some applications only accessible when a user has authenticated using the dual channel method.

To do this restrict access to applications to the pinsaferadius group on the Trunk->Applications-.Authorization tab

Application Properties (Enhanced Generic Client App (hosts dis 🗙			
😳 Client Settings 🔇 Portal Link 😫 Authorization			
All Users Are Authorized			
Users/Groups	Allow	View	Deny
pinsaferadius:Authenticated Users	1	8	
Save A <u>s</u> Local Group	<u>A</u> dd		<u>R</u> emove
Help	0	ĸ	Cancel

## 376.4 User Experience

The user is presented with the option of authenticating via SMS or TURing.

To authenticate the user enters their username and then clicks on the authentication method they wish to use. If they select TURing and TURing image is displayed.

Web site		
Please pro	vide the following:	
	SMS O	Turing
User Name:	test	
Password:		
Language:	English (default)	
1 2	3 4 5 6 7 8 9	0
21	8 4 9 6 3 5 0	- 
		1

If they select SMS (and multi-SMS is being used) the index of the security string that they need to use is displayed.

Web site	TUDE	
Please pro	wide the following:	Turing C
User Name:	test	
Password:		
Language:	English (default)	
00		

(If they have no valid SMS strings, -1 is shown)

When they make their selection the login page automatically associates them with the correct repository.

After authentication they will only have access to applications appropriate to their method of authentication.

# 377 Microsoft IAG SMS login video

## 377.1 Microsoft IAG SMS login Video

PINsafe_IAG_SMS_login.swf

# 378 Microsoft IAG Turing login video

## 378.1 Microsoft IAG TURing login Video

PINsafe_IAG_Turing_login.swf?

## 379 Microsoft ISA 2006 Cluster Integration

## 379.1 ISA 2006 Cluster Integration

#### 379.2 Overview

In an ISA cluster, the Swivel filter needs to be registered with the cluster on the storage server and on each member of the cluster.

If all the ISA Servers are installed on 32-bit operating systems, then you can use version 1.2 of the PINsafe ISA filter, which manages filter registration as part of the login process. You must install on the configuration storage server first, and then on each member server. See the standard ISA filter integration guide (link below) for further instructions.

If you are running ISA Server on a 64-bit operating system, the reference above will not work. Instead, you will have to use the older 64-bit version together with installation scripts.

Refer to the ISA 2006 integration guide for additional steps, for both versions of the filter. Microsoft_ISA_2006_Integration

### 379.3 Prerequisites

These are required in addition to the ISA 2006 Integration prerequisites

- RegisterFilter.vbs
- RegisterFilterMember.vbs

These files can be downloaded from here: File:PINsafe_ISA_2006_Cluster_Registration.zip

### 379.4 ISA 2006 Cluster Installation Steps

#### 379.4.1 Install the PINsafe filter

Run the setup.exe file on each of the ISA servers ignoring errors relating to registration of the PINsafeISAFIIter

#### 379.4.2 Ensure the PINsafe Filter is on each ISA server

Ensure that the PINsafeISAFilter.dll is installed on C:\Program Files\Microsoft ISA Server on all ISA servers.

#### 379.4.3 ISA Cluster Storage Server Filter Registration

On the configuration storage server copy RegisterFilter.vbs to C:\Program Files\Microsoft ISA Server and run it.

You may have to run it from the command prompt, specifying the fully-qualified name of the configuration storage server, if that is not the server you are running it from.

#### 379.4.4 ISA Cluster Member Filter Registration

Copy RegisterFilterMember.vbs to C:\Program Files\Microsoft ISA Server on each member server, and run. Once you have done this, check that it appears in the list of web filters for the server.

when manually registering a web filter .dll, from the command prompt you need to be in the SAME directory as the .DLL, otherwise you will get an error:

Error: The Web Filter referenced by Server xxxxx does not exist The error occurred on object ?xxxxx? of class ?Server? in the scope of array ?Learning-ISA?

#### 379.4.5 Configure the ISA Filter

Configure the ISA filter using the configuration tool provided. Each ISA server in the cluster will need to be configured. To start is select Start/Programs/PINsafe ISA Filter/Configuration.

# 380 Microsoft ISA 2006 Integration

381 Microsoft Internet Security and Acceleration Server (ISA) Integration Notes

## **382 Introduction**

This document outlines the necessary steps to integrate Swivel authentication into either Outlook Web Access (OWA) 2003 or Sharepoint Forms-based Authentication (FBA) provided with Microsoft ISA Server 2006. Additionally the login page can be further customised, for further information see: Microsoft ISA 2006 web page customisation How to Guide. If the ISA server is part of a cluster then the filter needs to be installed on each cluster, the 32 bit installer handles cluster registration, for further information and manual registration see Microsoft ISA 2006 Cluster Integration

Note that with the release of version 1.2 of the Swivel ISA filter, filter registration is part of the configuration process. See below for more information. This also means that the same installer can be used for Enterprise and Standard ISA Server. Unfortunately, version 1.2 supports 32-bit operating systems only. However, there is a 64-bit version for Microsoft Forefront Threat Management Gateway. The documentation for this is now available from a separate page here.

## **383 Prerequisites**

This installation guide assumes that publication of the relevant service has already been configured in ISA Server, following the relevant instructions. In addition a working Swivel server version 3.1 or later is required.

If the option to check a user is a Swivel user and issue a OTC field is to be used, this requires Swivel 3.4 or later.

The Swivel Configuration utility requires .Net version 2 or higher. This is not supplied above and must be downloaded and installed if you do not already have it.

The ISA server and its configuration should be fully backed up prior to the Swivel integration.

Allow around 1 hour downtime per ISA server for the integration, and the integration will require a restart of the ISA Firewall Services.

### 383.1 ISA 2006 Filter

The installer can be downloaded from here.

### 383.2 TMG Filter

The TMG version can be found here. NOTE: this is version 1.4.0 of the TMG filter, released 23/8/12, which includes a number of enhancements over previous versions. See the included documentation.

## 384 Baseline

Swivel 3.4 or later (3.6 or later preferred)

Microsoft ISA Server 2006 or Microsoft Forefront TMG

Web-based server, typically Microsoft IIS-based, to be protected, such as OWA or SharePoint.

## **385 Architecture**

The ISA server makes authentication requests against the Swivel server by XML or RADIUS. Some of the additional features are only available in the XML authentication. For security reasons Sharepoint authentication should be configured using RADIUS. The Swivel installation creates a separate custom login.

The default install path for the standard OWA login page is:

C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\Exchange\HTML

The standard install path for PINsafe OWA authentication page is:

C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINsafeOWA\HTML

## **386 Swivel Configuration**

## 386.1 Configure a Swivel Agent For XML Authentication

- 1. On the Swivel Management Console select Server/Agent
- 2. Enter a name for the Agent
- 3. Enter the ISA internal IP address
- 4. Enter the shared secret

Г

5. Click on Apply to save changes

Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	•••••	
	Group:	ANY	
	Authentication Modes:	ALL	Delete
	Name:	IIS	
	Name: Hostname/IP:	IIS 192.168.1.1	
	Name: Hostname/IP: Shared secret:	IIS 192.168.1.1	
	Name: Hostname/IP: Shared secret: Group:	IIS 192.168.1.1	

## 386.2 Configure Single Channel Access

- 1. On the Swivel Management Console select Server/Single Channel
- 2. Ensure ?Allow session request by username? is set to YES

Server>Single Channel 🥘	
Please specify how single channel security str	ings are delivered.
Image file:	turing.xml 💌
Rotate letters:	No 💌
Allow session request by username:	Yes
Only use one font per image:	Yes 💌
Jiggle characters within slot:	No 💌
Add blank trailer frame to animated images:	Yes 💌
Text Alpha Value:	80
Number of complete display cycles per image	e: 10
Inter-frame delay (1/100s):	40
Image Rendering:	Static 💌
Multiple AUthentications per String:	No 💌
Generate animated images:	No 💌
Random glyph order when animating:	No 💌
No. Characters Visible:	1
	Apply Reset

## 386.3 Configure a RADIUS NAS entry for Sharepoint authentication

NOTE: this is only required if you wish to use RADIUS authentication with Swivel. This is recommended for SharePoint integration and optional for other solutions.

- 1. Ensure the RADIUS server is running on Swivel
- 2. On the Swivel Management Console select RADIUS NAS
- 3. Enter a name for the NAS
- 4. Enter the ISA internal IP address
- 5. Enter the shared secret
- 6. Click on Apply to save changes

## 387 ISA Installation

The following steps should be carried out on the ISA server. No configuration changes need to be performed on the Exchange server or Sharepoint server. For Additional Sharepoint configuration see the Special Considerations for Sharepoint below.

#### 387.1 Publish OWA or Sharepoint

Publish Outlook Web Access, Sharepoint or your website as described in the ISA Server documentation, if you have not already done so. Ensure that they are working as expected.

#### 387.1.1 Configure ISA firewall rules

Create an access rule permitting HTTP access from the ISA Server to the correct port (commonly 8080) on the Swivel server. To do this, you will need to create a new protocol for outbound TCP on the appropriate port.

#### 387.1.2 Install the ISA server software

NOTE: if you are installing in an Enterprise environment, you should always install on the Configuration Storage server first, and then on each array member. Be aware that the firewall service on member servers will stop when they try to synchronise with the configuration storage server, if that has the Swivel filter installed and the member does not. Once the filter is installed on the member server, you will be able to restart the firewall service.

Run PINsafeISAFilter.exe to install the filter DLL. You will be prompted for the location in which to install the filter configuration, and also for the location of Microsoft ISA Server, usually C:\Program Files\Microsoft ISA Server.

PIX:aie15A filter Installation		X Start Contraction
Select destination directory		rg with splitter in the solution
PIAkafe ISA Filter wil be installed to the directory shown below.		
- Davina lina Directron		
USERCIAL USERCY To installate a different disactions, allow there are a second with the data between the beauty		
for a cestination cirectory. (*16saie GA Piter' is outpractedly at	dad.)	
	1	per oran housed
Cliprogram FfesipiNsafe ISA Albar	Втомеени	present for Source to be been
- Microsoft 196, Server		
Barra mathematical Atoma 9, 753, Sanaris Installad		
Neves 216 TA Miles Mile 200 CM Seves Preventer	-	2
CilProgram Files/Ricrosoft ISA Server	8 <u>r</u> cwse	Sin a conservation and a second
<back max<="" td=""><td>C Gancel</td><td></td></back>	C Gancel	

Note that the installation process will include installation of Microsoft Visual C++ 2010 runtime libraries, if they are not already installed.

### 387.2 Register the ISA Filter

When installation is complete, you have the option to run the configuration program. Assuming you elect to do so, you will first be prompted to register the filter with Swivel. You have a choice of registration types:

[[Image: Register_Filter.PNG ]]

Select the right option for your requirements. The last option is required if you are installing on the Configuration Storage server and the same server is also a member of the ISA server array.

#### 387.2.1 Configure the ISA server

Configure the ISA filter using the configuration tool provided. This will optionally run immediately after installation. To start subsequently, select Start/Programs/PINsafe ISA Filter/Configuration.

PINsafe configuration tab:

Pinsele ISA Pinsele Authe	Filer Configuration 📃 🗆 🛛	
Server:	pinsafa.swivel.dev.local	
Patr	8080	
Cortex:	pinsafe	
	<u>≥</u> 35L	
	🗌 Alow Sal-Signed	
Secret:		
Pouro	Dard Dava	Anima wana 2 1
	1233 0.058	

Server: is the name or IP address of the Swivel server (Hint: Use hostname to avoid problems with SSL certificates)

Port: is the port on which Tomcat is running. PINsafe virtual or hardware appliances require the use of XML authentication on port 8080 and the 8443 proxy port should not be used when integrating with ISA. (Hint: Use port 8080)

**Context**: is the name of the Swivel web application, usually ?pinsafe?. Note when using a Swivel virtual or hardware appliance where the proxy port is available, the path pinsafe using port 8080 should still be used, the ISA proxy provides security.

SSL: will, if checked, send requests to the Swivel server using https, rather than http.

Allow self-signed: when checked, causes SSL certificate errors from the PINsafe server to be ignored.

Secret: is the shared secret for the Swivel agent for the ISA Server, and needs to be the same as that on the Swivel server. After you enter this value, you will be prompted to enter it again, to confirm that it is correct.

Authentication configuration tab:

Piterie Eva Filer Configuration       Image: Authoritochical Inst Numes         Piterie Authoritochical Inst Numes         Authoritochical Inst Numes         Inst Numes	
Seve Head Cose	

Authenticate to PINsafe: should be checked to use standard Swivel authentication. You should uncheck this if you are using the ISA filter to protect a Sharepoint website, as described in the ?Special Considerations for Sharepoint? section below. If you uncheck it, Swivel will not directly authenticate the login request. In this case, you should enable RADIUS authentication instead.

Ignore user domain: This will remove the AD domain of users, and when Swivel is using the SAM account name it should normally be checked, in this case, if you enter ?domain\user? as the logon username, only ?user? will be sent to Swivel. If it is not checked the full name will be sent to Active Directory and should be used when Swivel uses the User Principle Name.

Allow non-PINsafe users: when checked, users not known to Swivel may authenticate using only their AD credentials. This feature is useful for transition to Swivel, where not all users have Swivel accounts. If checked, the OTC field is not shown initially, only when the username is checked and found to exist in Swivel. Note that this feature is not compatible with RADIUS authentication.

The last two options on this tab should not be used - they do not work, and are there for future enhancement.

Hosts configuration tab:

Only authenticale bosts shown below:	
www.swigel.dev.loc.d	
Save Read Cose	

This feature is new to version 1.2. Previously, when installed, the PINsafe ISA filter would affect all authentication requests through the ISA Server. This option allows you to apply PINsafe authentication per host name. It can either be configured to authenticate all host names except those specified, or to authenticate only those hosts specified, and to ignore all others.

### 387.3 Confirm that the filter has been registered correctly

Once completed the filter will appear in the ISA Server Management Web Filters section. If the filter does not appear in the list of available filters check the Windows system event log for errors. The 32 bit installer handles cluster registration, for further information and manual registration see Microsoft_ISA_2006_Cluster_Integration

### 387.4 Modify the Listener

Modify the Listener used to publish OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, type:

?PINsafeOWA? for Outlook Web Access

and ?PINsafeWeb? or ?PINsafeRadius? for Sharepoint or other websites (?PINsafeISA? for TMG).

You should always use PINsafeRadius for Sharepoint, for reasons described below. You may use either set of forms for standard websites. Note that the TMG filter does not require a different set of custom pages for RADIUS.

Modify the properties for the relevant policy rule.

Then select Apply, and click Ok. Then select the Application Settings tab and UNCHECK the option to use customized HTML. Note that if you have customized your original OWA or Sharepoint login pages, you will need to apply the same customisation to the new Swivel pages. Please consult Swivel support for details of this.

Once you have configured everything, restart the Microsoft Firewall Service on the ISA server. It can take a long time to restart this service, and if you are connecting to the ISA Server via remote desktop, you may be temporarily disconnected from it.

## 388 SSL Certificate Considerations

There would appear to be an issue with a recent security update for ISA Server which prevents HTTP POST requests over SSL unless the target server certificate is fully trusted. This has consequences for the PINsafe ISA Server integration.

If you are not using SSL on your Swivel server, this issue will not affect you.

If you are using SSL, you must have a valid certificate on the Swivel server. This means:

- The certificate date must be current (i.e. not expired)
- The certificate must be issued by a trusted CA (see below for ways of managing this)
  The certificate subject must match the host name used by the ISA Server to connect to the Swivel server. In particular, this means that you must reference the Swivel server by name, not by IP address.

One way to manage this is to get a commercial certificate for the Swivel server. However, this costs money, and if your PINsafe server is not internet Gracing, is not necessary. A second option is if you have an internal certificate authority, you can use that to issue a certificate for the Swivel server (Windows Servers, for example, can optionally be configured as certificate authorities). If you do this, you need to make sure that the certificate authority server certificate is added to the trusted root certificates on the ISA Server, if it is not already. The third option is simply to generate a self-signed certificate on the Swivel server, with the correct host name, and to install that directly into the ISA Server trusted root store (see below).

For more detail, refer to the relevant knowledgebase documentation on generating SSL certificates if you are using a Swivel virtual or hardware appliance. Otherwise, refer to the relevant documentation for your operating system.

### 388.1 Installing a Self Signed Certificate into the ISA trusted root store

If you want to do is to trust the Swivel server certificate the following steps may be carried out:

- 1. Copy /home/swivel/.keystore to a suitable machine (it doesn?t have to be the ISA server).
- 2. Open the file in Keystore Explorer.
- 3. Right-click on the certificate (if there is more than one, it will probably be called ?swivel?). Select ?Export?, then ?Export key pair?.
- 4. Enter a password for the exported certificate. I recommend using ?lockbox?, but anything will do.
- 5. Select the export path. It doesn?t actually matter what the extension is.
- 6. Copy the exported certificate to the ISA Server. The remaining commands are done on the ISA Server.
- 7. Open ?mmc? from the Run dialog.
- 8. Select File -> Add/Remove Snap-in.
- 9. From the dialog, select ?Certificates? and click ?Add?.
- 10. Select ?Computer account?, then ?Local computer?.
- 11. Click OK.
- 12. Go to Certificates -> -> Trusted Root Certificate Authorities.
- 13. Right-click, then ?All Tasks?, ?Import?.

14. Select the exported certificate. You will need to enter the password. We recommend marking the key as exportable. Make sure the certificate is imported into the -> Trusted Root Certificate Authorities.

- 15. If you look under Certificates -> Personal -> Certificates, you should see the new certificate.
- 16. You may need to restart the Microsoft Firewall service before it shows the new certificate.
# **389 Special Considerations for Sharepoint**

A security hole has been discovered when using earlier versions of the ISA filter for Sharepoint authentication. It was possible to open a Sharepoint document from within Word (for example) and only provide the standard Active Directory credentials.

The new solution avoids this problem by using RADIUS to authenticate to Swivel, rather than using the ISA filter directly. One minor inconvenience with this is that users must authenticate through the Sharepoint web page before they can access any documents.

Note that if you disable Swivel authentication for Sharepoint, it is also disabled for all other websites. Therefore, if you want to use Swivel authentication on multiple websites for a single ISA Server, they must all use the standard Swivel authentication, or all use RADIUS.

1. On the ISA filter configuration application, uncheck the Authenticate option. This means that Swivel will not authenticate the logon request directly. Instead, you should use RADIUS to perform Swivel authentication, as described below.

2. On the Authentication tab you should check the option ?Collect additional credentials in the form?. This will require you to select ?RADIUS OTP? as the authentication validation method. Click the ?Configure Validation Servers? button, and add the Swivel server as a RADIUS server. Make a note of the shared secret you set for the server.

3. In order for users to be able to open documents from other, non-browser applications once they have authenticated, you must enable persistent cookies. On the Forms tab, click the Advanced button. It is recommended that you select persistent cookies for private computers only. This means that users on public computers will have to open documents from the Sharepoint web site.

4. On the ISA server, create a rule to allow RADIUS authentication from the ISA server to the Swivel server

5. On the Swivel server, enable the RADIUS server (on the RADIUS > Server page). On the RADIUS > NAS page, add the ISA Server as a new NAS, and enter the shared secret you set on the ISA Server. If you wish to restrict access to a particular group of users, select that group, otherwise leave the Group drop-down as ?ANY?.

6. On the policy rule, on the Authentication Delegation tab, select ?NTLM Authentication?.

Once you have configured everything, reboot the ISA server.

# **390 Verifying Installation**

## **390.1 Outlook Web Access**

Navigate to the URL on which ISA Server publishes OWA. The customisation is visible in the addition of a One Time Code field and a Start Session button. Attempting to login with a correct username and password but no one time code should result in failure. Only when a correct Swivel one time code is entered in addition to the Exchange or Sharepoint credentials should the user be logged into OWA.

Note that if a username is entered in the form Domain\username, the Domain\ portion of the username will be stripped before being passed to the Swivel server. This permits the use of sAMAccountName as the username attribute for synchronisation between Swivel and Active Directory.

**Dual Channel Login** 

<b>Office</b>	Outlook Web Access
Security ( show exp	lanation )
🕥 This is	a public or shared computer
🔵 🛛 This is	a private computer
Use Ou	utlook Web Access Light to change my password after logging on
Domain\user name:	graham
Password:	
One Time Code:	••••
	Start Session Log On
Connected to N Secured by Mic © 2006 Microsoft	Microsoft Exchange rosoft Internet Security and Acceleration Server Corporation. All rights reserved.

Single Channel Login

Security (show expla	ination )			
This is a This is a This is a	public or shared o	omputer		
📕 Use Ou	tlook Web Access I	ight		
📃 I want 1	to change my pass	word after logging o	n	
Domain\user name: Password: One Time Code:	graham •••••	Start Session	Log On	
1 2	3 4 5 7 <b>3 5</b>	6 7 8 1 8 0 1	γ ο 6 9	
Connected to M Secured by Microsoft	icrosoft Exchange osoft Internet Sec	urity and Acceleratio	on Server	

### 390.2 Sharepoint

Navigate to the URL on which ISA Server publishes Sharepoint. You will notice that there are two sets of credentials to enter. The Swivel credentials are entered in the top part, and the Active Directory credentials in the lower part. Enter the username in the first box as domain/user. Click the Start Session button to get a TURing image. Enter the Swivel password and one-time code in the next two boxes. (NOTE: the Swivel password and one-time code are actually concatenated and submitted as a single value. You can, if you prefer, enter them that way in the Passcode field ? password first).

In the final box, enter your Active Directory password, and click submit.

(NOTE: you actually have to enter different usernames for Swivel and Active Directory ? with the domain prefix for AD and without for Swivel. However, this is handled automatically for you. You will notice, if you fail login, that the Swivel username has changed, and the AD username has been inserted in the lower set of credentials.)

# **391 Additional Options**

## **391.1 RADIUS Authentication**

Set the Swivel server as the RADIUS server (and add the ISA Server as a NAS on Swivel). If you want to use the TURing image, then the Swivel ISA filter is required, but disable authentication in the filter configuration. PINsafeRADIUS custom login pages provided with the filter can be used.

## 391.2 Turning off Automated Security Strings

When a user enters their username and then their AD password, they will usually generate a single channel TURing image or for Dual channel On Demand authentication, automatically send an SMS message. This option is for the the integration using the OWA filter and will stop the automated display of single channel TURing images and the automated sending of SMS security strings.

The automation can be disabled by disabled by editing C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINsafe\OWA\HTML\usr_pwd.htm (Exact path may vary depending upon installation).

First Make a backup copy of the file

Edit the file in a text editor

Locate the setUserExists function

below this locate and remove the entire line ShowTuring();

Modified login page showing SMS on request

Security ( show exp	planation )
<ul> <li>This is</li> <li>This is</li> </ul>	a public or shared computer a private computer
can on Domain\user name	y use the Light dient.
Password:	
One Time Code:	
	New SMS

## 391.3 Editing the Security String Request Buttons

The message request buttons can be edited to display different messages.

The default International English language version is located in the the following file:

C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINsafeOWA\HTML\nls\en\strings.txt (Path may vary with installation, and different language files may also be edited)

First Make a backup copy of the file

Edit the file in a text editor

Find the line L_StartSession_Text="Get Image" (May also be L_StartSession_Text="Start Session" or L_StartSession_Text="Refresh Image")

Modified login page



# 392 Uninstalling

## 392.1 Modify the Listener

Modify the Listener used to remove OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, remove the tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, remove:

?PINsafeOWA? for Outlook Web Access

Modify the properties for the relevant policy rule.

Then select Apply, and click Ok. Then select the Application Settings tab and CHECK the option to use customized HTML.

Uninstall the Swivel software using the Remove Programs.

reboot the ISA server

## 393 Known Issues

## 394 Troubleshooting

NOTE: After any changes are made, always restart the Microsoft Firewall service

The Swivel authentication filter logs its activity to the standard Windows debug log. This can be accessed using a tool such Sysinternals DebugView available as freeware from:

#### Sysinternals DebugView

To include logging of output from the filter the option Capture Global Win32 must be enabled in the Capture menu.

With regard to the Single Channel TURing image, the ISA server login page does not use SCImage, the image request comes through the filter, so that the the Swivel server noes not need to be accessed directly from the internet. If the filter is not working, then no image will appear.

Single Channel image does not appear:

- Check Swivel ISA filter settings
  Check the Firewall service is started
- Check the ISA server logs for any error messages
- Use a fully qualified hostname instead of IP address for the Swivel server
- Is an SSL connection being used • Is a self signed cert being used, if so try without SSL using http or install a valid public certificate
- Check the Swivel ISA filter is correctly installed. On the ISA Server Management: under Configuration, Add-ins for the server, "PINsafe
- Authentication Filter" should be enabled
- From the ISA server check a Single Channel image can be generated in a web browser connecting to the Swivel server using:

Swivel virtual or hardware appliance

https://<PINsafe server IP>:8080/pinsafe/SCImage?username=test

For a software only install see Software Only Installation

• If you see a red cross where the Single Channel Image should be right click on it and select properties. Copy the Address (URL) which should look something like: https://<ISA URL>/PINsafeISAFilter.dll?username=graham&random=197405. Copy this line and paste into the URL bar of the web browser and see if a Single Channel Image is generated.

If a user is able to login without the One Time Code, then the ISA filter may not be installed.

If IP addresses, rather than host names is used, with SSL enabled, you must check the option to "permit self-signed certificates". This option actually means to ignore all certificate errors, as you will get when referencing a server by the IP address, rather than the name.

#### The following error can be seen when trying to install the Swivel ISA Filter on an ISA cluster:

Error 1904. Module C:\Program Files\Microsoft ISA Server\PINsafeISAFIlter.dll failed to register. HRESULT -2147024891. Contact your support

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

The "PINSafe Authentication Filter" then does not appear in the Web Filters tab.

#### See Microsoft ISA 2006 Cluster Integration

The ISA 2006 filter will not work with ISA 2004.

See also: troubleshooting OWA 2007 publishing rules on ISA Server 2006

## **395 Additional Information**

## 395.1 Note on Activesync and RADIUS authentication

If you are using the same listener for ActiveSync etc, then don't use the RADIUS (or RADIUS OTP) option, as this will affect authentication for the other types as well. Since using the AgentXML approach only affects forms authentication, it shouldn't affect ActiveSync, which doesn't use FBA.

## 395.2 ISA and OWA

Information regarding the configuration of ISA Server to publish OWA or Sharepoint may be found in the ISA Server help under Firewall policy.

## 396 Microsoft ISA 2006 web page customisation How to Guide

### 396.1 Microsoft ISA 2006 web page customisation How to Guide

NOTE: if you need to be able to support pass-through support for non-PINsafe users, the following article is insufficient. The current recommendation is to start with the files provided with the PINsafe ISA filter, and to customise them as required. Please contact support@swivelsecure.com for more details. Use the following article only if you do not need support for non-PINsafe users.

### 396.2 Overview

This is a brief outline of how to go about customising your forms-based authentication web pages in ISA server to support PINsafe authentication. It is assumed that you are reasonably familiar with modifying HTML pages.

## 396.3 Web Page Customisation

### 396.3.1 Install the ISA filter

First of all, you should install the latest version of the PINsafe ISA filter for ISA Server 2006, see Microsoft_ISA_2006_Integration. This includes customised pages for Outlook Web Access (OWA) and for general web access (the documentation specifically references Sharepoint, but it will work for other web applications).

You should only need to use this document if you wish to customise these pages further, or if you already have customised authentication pages to which you wish to add PINsafe functionality.

### 396.3.2 Obtain the ISA login pages

If you have not already got a customised set of ISA login pages, the simplest way is to make a copy of the entire contents of C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\ISA. This folder contains 3 sub-folders: HTML, cHTML and xHTML. The latter two are for mobile standards, which PINsafe does not currently support, principally because those standards do not support JPEG images, which is the format that TURing images are generated in, so only the HTML folder is of interest. The copy should be made into a folder under C:\Program Files\Microsoft ISA Server\CookieAuthTemplates. The name of the folder should correspond to the name you enter in the custom form name in the listener properties. Within this folder, 4 files potentially need to be modified: strings.txt, usr_pcde.htm, usr_pwd.htm and usr_pwd_pcode.htm. Additionally, if international support is required, other strings.txt files will need to be modified. These files are under the nls sub-folder, one for each language. Note that, for international characters to be displayed correctly, the strings.txt file must contain Unicode characters, so you will need to use a text editor that supports reading and saving Unicode files (e.g. NOT Notepad).

The strings.txt file supplied in the pinsafeWeb (or pinsafeOWA) folder of the PINsafe ISA filter installation should be sufficient for your needs, unless you have added other customised strings to your web pages.

Note also that if you have added custom images and/or stylesheets, you will need to include them in the new custom folder.

#### 396.3.3 Customising the web pages

#### 396.3.3.1 Change the Banner Logo

It is possible to change the logo displayed at the top of the login page. The page may look like this:

	···· ··· ···· ···· ····
Internet Security &	
Acceleration Server 2006	
Security (chow evide ration)	· · · · · · · · · · · · · · · · · · ·
<ul> <li>This is a public or shared computer</li> <li>This is a private computer</li> <li>Warning Brickhold Arc data option of a private BRACH computer</li> </ul>	
Remote Access Credenbals ( anou-eto-ministon )	
User name: One Time Code:	
Refresh Image           1         2         3         5         5         7         9         9           1         2         3         5         5         7         9         9           2         3         4         5         5         7         9         9	
Internal Network Credentials (chrom coplosation) Use a different user name Password:	
Log On	
© 2006 Microsoft Corporation, All rights reserved.	

The image shown here at the top is in GIF format and is 500x115 pixels. On a 32-bit machine the picture can be found in "C:\Program Files\Microsoft ISA Server\CookieAuthTemplates\PINSafeOWA\HTML" - if the ISA server was installed to a non-standard location then this will not be the location. The file name of the logo is IgnTop.gif.

In order to update the picture for display you can simply substitute a new logo of exactly the same format and size then restart the ISA service to complete the installation of the new logo. This should then display the next time the page is accessed. The end result should look like this:

Caustonni Leogo	
Security ( the interval enables ) This is a public or shared computer	A Provide Provide A Provid
<ul> <li>This is a private computer</li> <li>Writing Construction this option into a commonly. Reaction of the computer of the commonly device the computer of the com</li></ul>	
Remote Access Credentals (	
Refresh Image	
Internal Network Credentials ( intern coplocation ) Use a different user name Password:	
Log On © 2006 Microsoft Corporation, All rights reserved.	
	A STATE OF A STATE OF A STATE

#### Troubleshooting

If the page is requested by a refresh it is possible that the browser will display a cached version of the site. Clearing the cache within your browser may fix this.

If the logo is not of the same format (GIF) or of the same size (500x115pixels) then it may fail to display correctly.

If the name of the new image differs in case to the original then it may fail to load correctly.

When swapping the images it is recommended that you rename the old picture file and add the extension ".old". This will allow you to easily revert the image should the need arise.

#### 396.3.3.2 Edit the strings.txt file

The entries added for PINsafe are:

L_OTC_Text = ?One Time Code:?

L_StartSession_Text = ?Start Session?

These are respectively the labels used for the one-time code text box and the TURing image request button. You can change these values (to the right of the = sign) to match your requirements, but ensure that the labels (to the left of the = sign) are as shown.

If you need to customise your pages for other languages, look in the nls sub-folder and find the sub-folder matching the language you need to use. Add strings with the same names as those shown above to the strings section. As noted above, please ensure that the files are saved as Unicode text.

Depending on what authentication method you are using, you may not need to modify all three of the login pages, as explained here:

- usr_pwd.htm is used for Active Directory plus PINsafe AgentXML authentication.
- usr_pcode.htm is used for RADIUS authentication as the ONLY form of authentication (i.e. when no Active Directory authentication is required).
- usr_pwd_pcode.htm is used when Active Directory authentication is used in conjunction with PINsafe RADIUS authentication.

The other 3 pages all need very similar modifications: they need a text box for the one-time code, a button to display the TURing image, a place to display the TURing image and the JavaScript necessary to display the image.

Starting with the last item, the following JavaScript should be sufficient:

Note that, for usr_pwd_pcode.htm only, the fourth line should read

username = document.getElementById("userid");

For the one-time code text box, both the id and the name attributes of the input field should be set to ?otc?:

<input id="otc" type="password" name="otc" />

For its label, use the value @@L_OTC_Text as the label text. This will be replaced by the label you defined in strings.txt:

<label for="otc">@@L_OTC_Text</label>

The button to display a TURing image should have an onclick event of ?onClickStartSession();?, and a value (label) of ?@@L_StartSession_Text?:

<input id="StartSession" type="button" value="@@L_StartSession_Text" name="StartSession" onclick="onClickStartSession();"/>

Finally, the placeholder for the TURing image should have an id of ?PINsafeImage?, and initially set to be invisible:

<img id="PINsafeImage" style="display:none;" />

## 397 Microsoft OWA 2003 IIS Integration

## 397.1 Introduction

PINsafe allows users to authenticate users of Outlook Web Access (OWA) on Microsoft Exchange Server 2003. An ISAPI filter installed on the Exchange server allows access to protected resources through the PINsafe authentication. NOTE: This document refers to the version of the filter numbered 1.2.0.0, and the configuration application with the same version number.

## **397.2 Prerequisites**

Microsoft Exchange 2003 with OWA. It should be configured as a front-end server for MS Exchange, with forms-based authentication enabled.

Microsoft 2003 Server

PINsafe server: Requires PINsafe 3.x. PINsafe does not need to be installed on the same machine, but the target server must be able to connect to a PINsafe server without any authentication except that provided by PINsafe.

Users are able to login using standard OWA

IIS Filter for OWA 2003

### 397.3 Baseline

Microsoft Exchange 2003 with OWA using IIS 6.0

Microsoft 2003 Server

PINsafe 3.7

## 397.4 Architecture

The Exchange server makes authentication requests against the PINsafe server by XML authentication

### 397.5 Installation

### 397.5.1 Ensure Active Server Pages are Allowed

Allow Active Server Pages: to verify this, select the Internet Information Services Manager expand the required server then click on Web Service Extension.



#### 397.5.2 Software Installation

On the Exchange server run the PINsafeIISFilter.exe. The filter must be installed in the Exchange Server authentication web folder, which by default is C:\Program Files\Exchsrvr\exchweb\bin\auth. If this is not correct, change the target folder before installation. Select Start Menu Folder. When details are correct click on Install. If the error ?Incorrect Command Line Parameters? is seen click on OK.

#### 397.5.3 Configuration of the IIS Filter

The Filter Configuration should start after installation or can be started through the Start Menu.

• PINsafe Server tab contains settings which define the PINsafe server which will be used to authenticate users.

Hostname/IP: The name or IP address of the PINsafe server.

Port: The port number used by the PINsafe server, 8080 for a software install or PINsafe virtual or hardware appliance (do not use 8443)

Context: The PINsafe install name usually pinsafe, or for a PINsafe virtual or hardware appliance proxy.

Secret: The common secret used to communicate with the PINsafe server. This value must be the same as the secret defined for the PINsafe agent.

SSL enabled Tick this box to require SSL (HTTPS) communication with the PINsafe server, for a PINsafe virtual or hardware appliance ensure the box is ticked.

**Permit self-signed certificates** Tick this box to allow SSL certificates to be self-signed. This also ignores other certificate errors, such as site names not matching. For a PINsafe virtual or hardware appliance tick this box until a valid certificate is applied.

Exclusions	Inclusions	Misc
PINsafe Server	Au	thentication
Hostname/IP:		
Port:	8080	
Context:	pinsafe	
Secret:		
SSL enabled		
Permit self-signed	d certificates	

• The Authentication tab contains the following settings:

Idle time (s): The length of time in seconds that the authentication cookie is valid, provided you make no OWA requests in that time. If you do, the cookie is refreshed and the countdown starts again.

Username header: The name of a cookie which will pass the username of the authenticated PINsafe user. If this value is blank, no cookie will be provided.

Single Indicates that single channel security strings (i.e. TURing image) are permitted.

Dual Indicates that dual channel security strings (i.e. via e-mail, SMS) are permitted.

On-demand dual Indicates that the login page should display a button to request dual-channel security strings.

Display password fields Indicates that the login page should show a field for PINsafe password as well as OTC.

Permit self-reset Indicates that the user self-reset page should be enabled.

Standard auth. for non-PINsafe Users If enabled, users that PINsafe does not recognise will be allowed to authenticate using standard Active Directory methods. Note that this option requires PINsafe 3.5 or later. The option to allow unknown users to authenticate without Swivel authentication only applies to users not known to Swivel at all. You cannot specify that it only applies to a group of users, and not to other users who are known to Swivel, but not in a particular group.

Idle time (s): Username header: PINsafe_User Channels Single Dual Options Options Display password fields				
Username header: PINsafe_User Channels Single Dual Options Display password fields	dle time (s):	300		
Channels ✓ Single ✓ Dual ✓ On-demand dual Options ✓ Display password fields	Jsername header:	PINsafe_Us	er	
Single Dual On-demand dual Options Display password fields	Channels	<u></u>		
Dual     On-demand dual     Options     Display password fields	🔽 Single			
On-demand dual Options Display password fields	🔽 Dual			
Options Display password fields	Con-demand dual			
Display password fields	Options			
	Display password	fields		
Permit self-reset	Permit self-reset			
🔲 Standard auth. for non-PINsafe Users	🔲 Standard auth. fo	or non-PINsafe	e Users	

#### Exclusions

**Excluded Paths:** This is a list of paths within the current website which should be exempt from PINsafe authentication. This is only relevant if the included paths list is empty, in which case all paths not on this list will be protected by PINsafe.

**Excluded addresses:** This is a list of IP addresses which are exempt from PINsafe authentication. All requests from these addresses are passed through without authentication.

Plivsare Server	Aut	hentication
Exclusions	Inclusions	Misc
Excluded addresses:		
1		<u></u>
		¥
Excluded paths:		
		<u>_</u>
		Y

Inclusions

**Included Paths** This is a list of paths within the current website which require PINsafe authentication. If this list is empty, the entire website will be protected except as indicated by the Exclusions tab. Paths should be one per line. You should at least ensure that the virtual folder ?/exchange? is listed.

PINsafeIISFilter for O	WA Configu	ration ver.	1.2.0.1
PINsafe Server	1	Authentic	ation
Exclusions	Inclusions		Misc
Included Paths:			
(exchange			<u> </u>
			*
	1	1	
OK		ancel	Apply

#### • Misc Tab

**Default path:** This is the path to which authenticated requests are directed if the login page is targeted directly. For this particular version of the filter, it should be ?/exchange?. If a user tries to access a protected page, she is redirected to the login page, and after authentication, back to the page she was trying to access. If the user requests the login page directly, she will be redirected to this location after authentication.

Logout path: Requesting this path will result in the user being logged out. Subsequent requests will require re-authentication, if relevant. If this path is empty, users can only be logged out by closing the browser, or if the authentication times out.

Virtual web path: This is the path to the PINsafe authentication pages. The default for this version of the filter is ?/exchweb/bin/auth?. You should only change this if your Exchange server has an unusual configuration.

Help URL: The URL for PINsafe IIS filter help. The filter does not come with help pages as standard, so this should only be filled in if help pages have been provided by the reseller or end user.

Internal OWA Host: This should be set to the URL of the OWA Exchange server, for example https://mail.myserver.com. Since this URL is called from the server itself, you could use https://localhost, but if you do that, make sure that you check the option to accept self-signed certificates, as the server certificate will not match the name ?localhost?.

Exclusions     Inclusions     Misc       Default path:     /exchange       Logout path:     //exchweb/bin/auth       Virtual web path:     /exchweb/bin/auth       Help URL:	PINsate Server	Au	thentication
Default path: /exchange   Logout path: /exchweb/bin/auth   Virtual web path: /exchweb/bin/auth   Help URL: /exchweb/bin/auth   Internal OWA Host: https://mail.myserver.com	Exclusions	Inclusions	Misc
Logout path:       /exchweb/bin/auth         Virtual web path:       /exchweb/bin/auth         Help URL:	Default path:	(exchange	
Virtual web path: /exchweb/bin/auth Help URL: Internal OWA Host: https://mail.myserver.com	Logout path:	[	
Help URL: Internal OWA Host: https://mail.myserver.com	Virtual web path:	/exchweb/bin/auti	h
Internal OWA Host: https://mail.myserver.com	Help URL:	[	
	Internal OWA Host:	https://mail.myser	ver.com

#### 397.5.4 Modifying the OWA Authentication Pages

The installation process replaces the existing owalogon.asp file with one customised for PINsafe. The existing file is renamed to owalogon.asp.old. Note that if you have customised the OWA logon page, other than simply replacing images or text messages, then you will not be able to use the customised pages as they are. You will need to combine your own customisations with those necessary for PINsafe authentication. For help with this, please contact your reseller, or Swivel Secure.

#### 397.5.5 Modifying the login Page to stop the Single Channel Image automatically appearing

By default the single channel authentication will appear when the username and AD password is entered and the user selects the OTC field. As a single channel session has started the PINsafe server is expecting an OTC to be entered from the Single Channel TURing image. If dual channel authentication is required then the automatic display of the Single Channel Turing image needs to be turned off. This can be done by modifying the login.asp file which by default is located in C:\Program Files\Exchsrvr\exchweb\bin\auth. The following needs to be removed from the username attribute field:

onblur=?checkUser()?

#### 397.5.6 Modifying the login Page to allow Dual Channel On Demand Delivery

If you want to use only dual-channel on-demand and no other method, then you can manage this by a simple change to image.asp (under /exchweb/bin/auth). Edit this file, search for "SCImage" and replace it with "DCMessage". Leave the onblur attribute as it was. Dual channel authentication for the user and also On Demand Delivery should be enabled on the PINsafe Administration console under Server/Dual Channel.

### 397.5.7 International OWA login Pages

If you want to use an internationalized version of the logon page, you will need to modify the installed files by hand, as follows:

1. Open an Explorer window on the OWA authentication folder (by default C:\Program Files\Exchsrvr\exchweb\bin\auth).

2. Copy all of the files in the authentication folder except owalogon.asp.old and owaauth.dll to the language-specific folder you intend to use (if you need to support multiple languages, you will need to copy all of them to each folder).

3. Rename owalogon.asp.old back to owalogon.asp.

4. In each folder, make a backup copy of logon.asp (which was in the folder before), and copy all the lines beginning ?CONST? from the beginning of the original logon.asp file to the copy of owalogon.asp you have just created, replacing similar lines in that file. You will also need to change the strings labelled ?CONST L_OTC_Text? and ?CONST L_StartSession_Text? with appropriate translations of the English strings ?OTC? and ?Show TURing?. Finally, rename owalogon.asp to logon.asp.

NOTE: Unlike previous versions of the PINsafe ISAPI filter (both standard and OWA), the PINsafe customisation is not visible immediately. Once you enter a username, the OTC field will appear, as will a TURing image. This means that it is no longer necessary to click a button to get a TURing image.

However, a button is provided should you wish to refresh the image (if the first one is too difficult to read, for example). Note that if you enable the option to allow standard authentication for non-PINsafe users, and the user is not recognised, no OTC field or TURing image will be displayed. Note also in this case there may be a small delay while the user is checked.

### 397.5.8 Applying Settings

After the changes have been made click apply and from the Services application, usually found from the Control Panel Administrative Tools, restart the World Wide Web Publishing Services.

### 397.5.9 Activating the ISAPI filter

- 1. On the Internet Information Services Manager Select the Properties for the website
- 2. Select ISAPI filters
- 3. Select Add ISAPI filter

4. Select the Path to the PINsafe ISAPI filter. Note that the actual file you require will be PINsafeIISFilter.dll, located in the sub-folder bin of the installation folder.

Default: c:\Program Files\Exchsrvr\exchweb\bin\auth\bin\

5. Ensure PINsafe ISAPI filter is top filter then click on OK





HTTP He	aders	Custom Errors	ASP.NET	Server Extensions
Web Site	ISAPI F	Iters Home Dire	ctory Docume	ents Directory Security
Filters ins order liste	talled here d below: Status	are active for this We Filter Name	b site only. Filters a	are executed in the
T.	1	Pinsafe IIS Filter	High	Bemove
				Edg
_				Disable

### 397.5.10 Configure The PINsafe Server

Configure a PINsafe Agent (For standard XML Authentication)

- 1. On the PINsafe Management Console select Server/Agent
- 2. Enter a name for the Agent
- 3. Enter the Exchange IP address
- 4. Enter the shared secret used above on the Exchange Filter

5. Click on Apply to save changes

Г

Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	•••••	
	Group:	ANY	
	Authentication Modes:	ALL	Delete
	Name:	IIS	
	radine.		
	Hostname/IP:	192.168.1.1	
	Hostname/IP: Shared secret:	192.168.1.1	
	Hostname/IP: Shared secret: Group:	192.168.1.1	

### **Configure Single Channel Access**

1. On the PINsafe Management Console select Server/Single Channel

2. Ensure ?Allow session request by username? is set to YES

Server>Single Channel 🛛	
Please specify how single channel security string	gs are delivered.
Image file:	turing.xml 💌
Rotate letters:	No 💌
Allow session request by username:	Yes 🔽
Only use one font per image:	Yes 💌
Jiggle characters within slot:	No 💌
Add blank trailer frame to animated images:	Yes 💌
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static 💌
Multiple AUthentications per String:	No 💌
Generate animated images:	No 💌
Random glyph order when animating:	No 💌
No. Characters Visible:	1
	Apply Reset

## 397.6 Verifying the Installation

To test the modifications, simply attempt to connect to Outlook Web Access. You should see the usual OWA authentication page, with two additions. Firstly, a third text box, for you to enter your PINsafe one-time code, and secondly, a new button labelled ?Show TURing? (or the equivalent if you have changed the language). To log on, enter your username (including domain if required) and click the ?Show TURing? button, if you are using TURing images. Enter your domain password and one-time code. Note that you should NOT use PINsafe passwords in this case. The authentication mechanism assumes that you have no PINsafe password, so will fail if you have. Now click ?Log On?, and if your credentials are correct, you should see the OWA interface as before.

## 397.7 Uninstalling the PINsafe Integration

Uninstall the PINsafe IIS filter then, the original Logon.aspx must be restored by renaming Logon.asp.old to Logon.aspx.

Note that the installation creates a new Logon.aspx file in /owa/auth, and renames the original to Logon.asp.old. To complete uninstallation this file must be copied back again.

## 397.8 Troubleshooting

#### 397.8.1 General Errors

Check the PINsafe and Windows server logs, and the IIS log C:\Windows\System32\LogFiles\W3SVC1 (the last directory may be different if you have more than one website on the same server).

Add an entry to the hosts file on the OWA server (C:\Windows\System32\drivers\etc\hosts). Add a new line to the file containing the following:

127.0.0.1 <owaserver.domain>

Replace <owaserver.domain> with the full external host name used to access the OWA server (not including https://). Then change the internal OWA host name on the PINsafe configuration to https://owaserver.domain (replacing owaserver.domain as before).

Reboot the Exchange server if it has not been started

Check the AD User is not required to Change their Password

Check the AD User account is not locked

#### User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

Turing image appears but user cannot authenticate.

Verify that the OWA is configured to use port 8080 and context pinsafe. port 8443 and context proxy will cause problems with authenticating users but allow the Turing image to be displayed.

#### 397.8.2 No Login Page Errors

No login page, check the Exchange version

Check to see if an International version of OWA is being used

### 397.8.3 Single Channel (Turing) Image issues

Red Cross instead of Turing image, right click on red cross and look at its properties. Ensure PINsafe server is running.

If you do not see a Turing image when using start session then in a web browser test the following link from the IIS server. If an image is not seen, then there is a problem either with communicating with the PINsafe server or the Allow Image request by username may be set to No.

For PINsafe software and virtual or hardware appliance installs:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

#### 397.8.4 Active Server Pages Errors

If the web page is redirected to the owalogon.asp page but an error message appears, then ensure that the Active Server Pages are allowed. To verify this select the Internet Information Services Manager, expand the required server then click on Web Service Extensions.

#### 397.8.5 ISAPI Filter Issues

NOTE: after the first time you authenticate to OWA, you should check that the ISAPI filter is loaded and running properly. Go to the web site properties dialog and locate the ISAPI filters tab. If the PINsafe filter doesn?t have a green arrow next to it, or the priority shows as ?Unknown?, then it is not working properly. You will still get redirected to the login page, and the built-in OWA security will handle that, but without the filter, it is possible for a knowledgeable person to authenticate with just the username and password, and bypass PINsafe.

The following procedure should ensure that the filter is loaded correctly:

1. Check which application pool your web application is running as, then go to the properties page for that application pool.

2. On the Identity tab, change the user to ?Local System?. You will be warned that this is a potential security risk, but don?t worry ? it won?t be left like this.

3. Restart IIS.

4. Authenticate to OWA. This should ensure that the filter is loaded: go back and check it.

5. You can now go back to the application pool and change the identity back to what it was originally: it would appear that it is only necessary to run as an administrator to get the filter to register initially.

#### 397.8.6 Name resolution issue

The Exchange server may be looking for exchange.company.com from the internal network but cannot resolve it. Edit the hosts file mapping the name to 127.0.0.1.

## 397.9 Known Issues and Limitations

PINsafe requires Forms Based Authentication (FBA), whereas iPhone and other Smart Phones (plus Outlook Anywhere) will require Non Forms Based Authentication (NFBA). You cannot have FBA and NFBA running on the same front end Exchange server. You would have to create a new Exchange server as a front end to the existing Exchange server and put the PINsafe OWA filter on that. You should be able to maintain services to the existing Exchange server whilst creating a new Exchange front end. Eventually you should be able to disable access to the old OWA, but maintain NFBA authentication to your other services.

To check if FBA is enabled, in the exchange manager, go to the server, select protocols, http and choose properties.

Microsoft have published a workaround for this issue, see Microsoft OWA with OMA on Exchange 2003

## 397.10 Useful Links

HTTP to HTTPS Redirect [1]

### 397.11 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

# 398 Microsoft OWA 2007 IIS Integration

# **399 Introduction**

PINsafe allows users to authenticate users of Outlook Web Access (OWA) using Microsoft Exchange Server 2007.

Active Sync users are able to receive email without PINsafe authentication as this uses a separate URL.

## **400 Prerequisites**

Microsoft Exchange 2007 with OWA

Microsoft 2003/8 server

Microsoft .Net Framework version 3.5

PINsafe 3.x

Users are able to login using standard OWA

IIS Filter for OWA 2007 version 2.7. This uses a different authentication mechanism from 2.6, which resolves problems reported by some users. Also some cosmetic fixes: in particular, Pinpad images are correctly sent as PNG format, rather than JPG.

Older versions:

IIS Filter for OWA 2007 version 2.6, including support for Pinpad and Change PIN

IIS Filter for OWA 2007 version 2.3

IIS Filter for OWA 2007 version 2.0

Login page for OWA 2007 8.2.301 (not necessary for version 2.6).

# 401 Baseline

For version 2.3 or later:

- Microsoft Exchange 2007 service Pack 3 with OWA using IIS
  Microsoft 2008 server
  PINsafe 3.7 or later

For version 2.0

- Microsoft Exchange 2007 service Pack 1 with OWA using IIS
  Microsoft 2003 server
  PINsafe 3.7 or later

# **402 Architecture**

The Exchange server makes authentication requests against the PINsafe server by XML authentication

## 403 Installation

### 403.1 Software Installation

Run the executable to install it on the Exchange Server. If your Exchange Server instance is not installed in the default location (C:\Program Files\Microsoft\Exchange Server\V14), you will need to modify the installation path. The installation path should be <ExchangeServerRoot>\ClientAccess\OWA

### 403.2 Configuration of the IIS Filter

After installation modify the settings. The Filter Configuration should start after installation or can be started through the Start Menu. If the Exchange Server installation is not in the default location, select the OWA directory as above in which to modify the web.config file.

#### 403.2.1 Swivel Settings

Server Name/IP: The Swivel server IP address or hostname

Port: Swivel server port, for a Swivel virtual or hardware appliance use 8080 (not 8443)

Context: Swivel install name, for a Swivel virtual or hardware appliance use Swivel (not proxy)

Use SSL Select tick box if SSL is used, for a Swivel virtual or hardware appliance tick this box. This also ignores other certificate errors, such as site names not matching.

Secret: The shared secret that must be entered also on the Swivel server Administration Console under Server/Agents

Accept self-signed certificates Where SSL is used with self signed certificates, for a Swivel virtual or hardware appliance tick this box until a valid certificate is installed.

**Proxy Server** These are used to retrieve TURing or PINpad images. If you are using a version of Swivel that does not support Pinpad natively (3.9 or earlier), you will need the special version of the virtual or hardware appliance proxy that does support Pinpad. If you are not using Pinpad, you can set these to be the same as the first set of values: if you are not using an virtual or hardware appliance, you MUST set them to be the same.

Proxy Port: Swivel server port, for a Swivel virtual or hardware appliance use 8443

**Proxy Context:** Swivel install name, for a Swivel virtual or hardware appliance use proxy

Proxy Use SSL Select tick box if SSL is used, for a Swivel virtual or hardware appliance tick this box. This also ignores other certificate errors, such as site names not matching.

	WA IIIte	r configuration		
PINsafe	OWA	Authentication	Excluded	
		PINsafe		Proxy
Server	Name/IP:	pinsafe.swive	ldev.local	pinsafe.swiveldev.local
	Port	8080		8443
	Context	pinsafe		proxy
		Vise SSL		Use SSL
	Secret			
Confir	m Secret:			
		Accept sel	f-signed certificate	S
				More
0	K	Cancel	Apply	

#### 403.2.2 OWA Settings

Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

OWA Path: OWA path, usually /owa, unless this has been explicitly changed

Logon Path: Logon path Usually /owa/Logon.aspx

Logoff Path: Logoff path /owa/Logoff.aspx

Auth. URL: This is the URL for OWA authentication and is usually https://<exchange.mycompany.com>/owa/auth/owaauth.dll

PINsafe OWA filt	er configuration
PINsafe OWA	Authentication Excluded
Server URL:	https://mail.swiveldev.local
OWA Path:	/owa/
Logon Path:	/owa/auth/Logon.aspx
Logoff Path:	/owa/auth/Logoff.aspx
Auth. URL:	https://mail.swiveldev.local/owa/auth/owaauth.dll
ОК	Cancel Apply

#### 403.2.3 Authentication Settings

**Cookie Secret Change:** This is an experimental setting, which increases security by changing the secret used to encrypt the authentication cookie at a specified interval. It is recommended that you leave this at 0, i.e. never change it. In particular, do not change this if you have multiple OWA servers, as it will cause problems.

Idle Time: The length of time in seconds that the authentication cookie is valid, provided you make no OWA requests in that time. If you do, the cookie is refreshed and the countdown starts again.

Allow non-PINsafe Users If this option is ticked, non Swivel users are allowed to authenticate using standard OWA authentication. This requires Swivel 3.5 or higher. The option to allow unknown users to authenticate without Swivel authentication only applies to users not known to Swivel at all. You cannot specify that it only applies to a group of users, and not to other users who are known to Swivel, but not in a particular group.

Filter Enabled The filter enabled option is mainly for testing, but also to handle situations such as enabling mobile access to the same Exchange Server i.e. ActiveSync and Windows Mobile Device Center. If the filter is disabled, you still need to authenticate through Swivel if you use the standard login page, but it is possible to authenticate using only AD credentials if you have a way to call the AD authentication filter directly.

Ignore Domain Prefix If this option is ticked, any prefixed domain (i.e. anything before the '\' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Ignore Domain Suffix If this option is ticked, any suffixed domain (i.e. anything after the '@' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Show TURing image If this option is ticked, a TURing image is shown to authenticate users.

Show Message on-demand If this option is ticked, a button is displayed to request a security string to be sent via SMS or email.

Show Pinpad If this option is ticked, an Pinpad button array is shown to authenticate users. You cannot have both TURing and Pinpad enabled.

Auto-show image If this option is ticked, the TURing or Pinpad image is requested as soon as the user enters the username and tabs away from it. If this option is not ticked, the user must click a button to show the image.

PINsafe OWA filter configu	iration	× )
PINsafe OWA Authentic	ation Excluded	
Cookie Secret Change:	0	hours
Idle Time (secs):	300	
Allow non-PINsafe Us	sers 🔽 S	Show TURing image
Filter Enabled		Show Message on-demand
Ignore Domain Prefix		Show Pinpad
Ignore Domain Suffix	<b>V</b> 4	uto-show Image
OK Can		Apply

### 403.2.4 Excluded Settings

**Excluded Paths:** This allows paths to be set for which authentication is not required to reach them. The paths shown on the display are added by default. The configuration program automatically detects the current build of OWA and includes that.

**Excluded/Included IP addresses:** You can choose to enable PINsafe authentication only for certain source IP addresses. Typically, you will do this if you wish to allow internal access to OWA without PINsafe authentication. Selecting "Exclude IP addresses below" will exclude the listed addresses from PINsafe authentication, while "Only include IP addresses below" will apply PINsafe authentication only to those IP addresses listed. For example, if you know that all external requests will come via a firewall at 192.168.0.99, you can select ?Only include IP addresses below?, and enter the single IP address as the address to include. Note that you can enter IP address ranges here using CIDR notation, for example 192.168.0.0/24 or 192.168.0.0/25.255.255.0. PINsafe will always display addresses using the latter format, irrespective of how they are entered. IPv6 addresses are not currently supported.

PINsafe OWA filter configuration	×
PINsafe OWA Authentication Excluded	
Excluded Paths:	
/owa/auth/owaauth.dll /owa/auth/ /owa/8.1.436.0/	
Exclude IP addresses below	
·	
OK Cancel Apply	

## 403.3 Configure The PINsafe Server

### 403.3.1 Configure a PINsafe Agent (For standard XML Authentication)

- 1. On the PINsafe Management Console select Server/Agent
- 2. Enter a name for the Agent
- 3. Enter the Exchange IP address
- 4. Enter the shared secret used above on the Exchange Filter
- 5. Click on Apply to save changes

Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	•••••	
	Group:	ANY	
	Authentication Modes:	ALL	Delete
			Sec. 35, 35, 7, 7, 7
	Name:	IIS	
	Name: Hostname/IP:	IIS 192.168.1.1	
	Name: Hostname/IP: Shared secret:	IIS 192.168.1.1	
	Name: Hostname/IP: Shared secret: Group:	IIS 192.168.1.1	

## 403.3.2 Configure Single Channel Access

- 1. On the PINsafe Management Console select Server/Single Channel
- 2. Ensure ?Allow session request by username? is set to YES

Server>Single Channel 🛛	
Please specify how single channel security string	gs are delivered.
Image file:	turing.xml 💌
Rotate letters:	No 💌
Allow session request by username:	Yes 💌
Only use one font per image:	Yes 💌
Jiggle characters within slot:	No 💌
Add blank trailer frame to animated images:	Yes 💌
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static 💌
Multiple AUthentications per String:	No 💌
Generate animated images:	No 💌
Random glyph order when animating:	No 💌
No. Characters Visible:	1
- A	Apply Reset

# 404 Additional Installation Options

## 404.1 Modifying the login Page to stop the Single Channel Image automatically appearing

NOTE: this section refers to earlier versions of the filter. In version 2.6 or later, this can be set using the configuration program.

By default the single channel authentication will appear when the username and AD password is entered and the user selects the OTC field. As a single channel session has started the PINsafe server is expecting an OTC to be entered from the Single Channel TURing image. If dual channel authentication is required then the automatic display of the Single Channel Turing image needs to be turned off. This can be done by modifying the login.asp file which by default is located in C:\Program Files\Exchsrvr\exchweb\bin\auth. The following needs to be removed from the username attribute field:

onblur=?checkUser()?

## 404.2 Modifying the login Page to allow Dual Channel On Demand Delivery

If you want to use only dual-channel on-demand and no other method, then you can manage this by a simple change to image.asp (under /exchweb/bin/auth). Edit this file, search for "SCImage" and replace it with "DCMessage". Leave the onblur attribute as it was. Dual channel authentication for the user and also On Demand Delivery should be enabled on the PINsafe Administration console under Server/Dual Channel.

# 405 Verifying the Installation

Enter a username and AD password then the PINsafe OTC for dual channel authentication. For single channel authentication enter the username, AD password then click on the button to generate a Single Channel Turing Security String, enter the OTC and login.

NOTE: if you have checked the option to allow non-PINsafe users, the OTC field and TURing button/image will not be displayed until you enter a username. If the username is not known to PINsafe, these elements will not appear. Similarly, if you have restricted the IP addresses to which PINsafe applies, the additional fields will not be displayed if PINsafe authentication is not required.

Security ( show	v explanation )
о т о т	his is a public or shared computer his is a private computer
Domain\user n	se Outlook Web Access Light ame: graham
Password:	
One-Lime Codi	: Log On New Security String
<b>.</b>	234567890
	5-9/3 2 8 1 5 10 4 2
# 406 Uninstalling the PINsafe Integration

Uninstall the PINsafe IIS filter then, the original Logon.aspx must be restored by renaming Logon.asp.old to Logon.aspx.

Note that the installation creates a new Logon.aspx file in ClientAccess\owa\auth\, and renames the original to login.aspx.sav. To complete uninstallation this file must be copied back again.

## 407 Troubleshooting

Check the PINsafe and 2007 server logs

Logon page takes a long time to load. The first time the OWA modification is started, the PINsafe page may take a while to load.

No login page, check the Exchange version in <path to Exchange>\ClientAccess\Owa

Look for folders consisting of 4 numbers separated by dots, for example "8.3.213.0". The first number will always be "8" for OWA 2007. You will need to ensure that the highest such folder is included in the list of excluded paths. In version 2.6 or higher, this should be handled automatically.

In version 2.0 of the filter, the file login.aspx needs to be modified so that it references the correct exchange install version. A program to automatically modify the login page is here. In versions 2.3 and higher, logon page modification is automatic.

1. Unzip and copy to <path to Exchange>\ClientAccess\Owa\auth.

2. Rename logon.aspx logon.aspx.current, rename logon.aspx.bk logon.aspx.

3. Open a command prompt and change directory to <path to Exchange>\ClientAccess\Owa\auth and run the OWAModifyLogonfor IIS program from in command line specifying logon.aspx i.e. OWAModifylogonforIIS.exe logon.aspx. If the option to allow authentication for non PINsafe users is being used then use the option switch *true*, e.g. OWAModifylogonforIIS.exe logon.aspx true. Using the option switch *false* will stop non PINsafe user authentication.

4. Check the file has been modified by the datestamp which should have changed for logon.aspx.

5. On the PINsafe IIS Filter Update the PINsafe filter under the Excluded path using the highest OWA version.

Red Cross instead of Turing image, right click on red cross and look at its properties. Ensure PINsafe server is running.

If you do not see a Turing image when using start session then in a web browser test the following link from the IIS server. If an image is not seen, then there is a problem either with communicating with the PINsafe server or the Allow Image request by username may be set to No.

For Swivel virtual or hardware appliances:

https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>

For a software only install see Software Only Installation

Blank page after an authentication. A login page may be displayed on the Exchange server. Verify the settings on the PINsafe filter point to the DNS name:

Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

Auth. URL: This is the URL for OWA authentication and the is usually https://<exchange.mycompany.com>/owa/auth/owaauth.dll

User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

### 407.1 Name resolution issue

The Exchange server may be looking for exchange.company.com from the internal network but cannot resolve it. Edit the hosts file mapping the name to 127.0.0.1. Note that because of security restrictions in OWA, the OWA server must be referred to by name, not by IP address, and the SSL certificate must be valid, and must be for the named host.

## 408 Known Issues and Limitations

Updates to the OWA 2007 server may require changes to the Excluded paths. You will also probably need to reapply the logon page changes.

If you wish to use the PINsafe filter with dual channel authentication, on demand or in advance, the logon page will need to be manually modified. Please contact Swivel support (support@swivelsecure.com) for more information.

# 409 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

# 410 Microsoft OWA 2010 IIS Integration

# **411 Introduction**

Swivel allows users to authenticate users of Outlook Web Access (OWA) 2010 with Microsoft Exchange Server running on Microsoft 2008 server. Active Sync users are able to receive email without Swivel authentication as this uses a separate URL. This article describes how to integrate Swivel with OWA 2010.

# 412 Compatibility

Microsoft Exchange Version and update release	<b>Build Version</b>	Compatibility Status
Exchange Server 2010	14.0.639.21	Compatible (old release only)
Exchange Server 2010 SP1	14.1.218.15	Compatible
Update Rollup 1 for Exchange Server 2010 SP1	14.1.255.2	Compatible
Update Rollup 2 for Exchange Server 2010 SP1	14.1.270.1	Compatible
Update Rollup 3 for Exchange Server 2010 SP1	14.1.289.7	Compatible
Update Rollup 4 for Exchange Server 2010 SP1	14.1.323.6	Compatible
Update Rollup 5 for Exchange Server 2010 SP1	14.1.339.1	TBC
Update Rollup 6 for Exchange Server 2010 SP1	14.1.355.2	Compatible
Update Rollup 7 for Exchange Server 2010 SP1	14.1.421.2	Compatible
Exchange Server 2010 SP2	14.2.247.5	Compatible
Update Rollup 1 for Exchange Server 2010 SP2	14.2.283.3	TBC
Update Rollup 2 for Exchange Server 2010 SP2	14.2.298.4	TBC
Update Rollup 3 for Exchange Server 2010 SP2	14.2.309.2	TBC
Update Rollup 4 for Exchange Server 2010 SP2	14.2.318.4	TBC
Update Rollup 5 for Exchange Server 2010 SP2	14.2.328.5	Compatible
Update Rollup 5-v2 for Exchange Server 2010 SP2	14.2.328.10	Compatible
Update Rollup 6 for Exchange Server 2010 SP2	14.2.342.3	Compatible
Exchange Server 2010 SP3	14.3.123.3	Compatible
Update Rollup 7 for Exchange Server 2010 SP3	14.3.210.2	Compatible
Update Rollup 8 (v2) for Exchange Server 2010 SP3	14.3.224.2	Compatible

**Note:** Updates may result in the login page customisation being removed. In this case, you must select the option "Reapply Logon Page Changes" from the Swivel filter start menu. Updates to the 2010 server may also require changes to the Excluded paths. See the **Troubleshooting** and **Known Issues** and **Limitations** sections before updating.

## **413 Prerequisites**

- Microsoft Exchange 2010 with OWA using IIS7
- Microsoft 2008 Server
- Swivel version 3.7 or later
- Users are able to login using standard OWA forms-based authentication.
- As the OWA server proxies the image request for Single channel TURing images and Pinpad, the Swivel server does not need a NAT.

The following is the latest release. Use this unless you have no Exchange service packs installed, in which case you need to use the older version, below. If you need a copy of an intermediate release for any reason, please contact support@swivelsecure.com.

### 413.1 Additional Prerequisites for Version 2.9

- Swivel Appliance version 3
- Microsoft .Net Framework 4.5 or later

NOTE: See notes below for additional installation requirements. Because of these additional requirements, it is recommended that you only upgrade to version 2.9 if you have a version 3 Swivel appliance.

## 414 File Downloads

Download links:

Version 2.8Version 2.9

### 414.1 OWA Filter Change History

Recent changes:

• 2.9.0 Support for TLS 1.1 and 1.2. See notes below for additional requirements. • 2.8.6 "Reapply Logon Page Changes" also updates default exclusions. • 2.8.5 • Fixed so that "/" is treated as a domain delimiter. • 2.8.4 Change PIN page modified to show one field at a time. • 2.8.3 Added hidden option to use previous authentication method. Prevent Pinpad sessions being cached. • 2.8.2 Fixed problem with names containing apostrophes. • 2.8.1 Now supports direct upgrading - no need to uninstall a previous version before installing the new one. This only applies to upgrading from version 2.7 or later. Change PIN Pinpad page selection of OTC field made more intuitive
 Fix for bug introduced by changes in 2.7.7 when not using alternative usernames • 2.7.7 Allow alternative usernames to work with versions of Swivel prior to 3.10 - see below. Fixed some issues with Change PIN using Pinpad • 2.7.6 Fixed problems with public/private flag
Changed Pinpad login to use session ID rather than username • 2.7.1 • Uses a slightly different authentication mechanism, since some users have reported problems with version 2.6.

Version 2.6 - if the new authentication mechanism causes problems with earlier service packs.

(Older release for OWA 2010 no service pack)

## **415 Architecture**

The Exchange server makes authentication requests against the Swivel server by XML authentication

## 416 Installation

NOTE: it is only necessary (or indeed possible) to install on Microsoft Exchange Client Access Servers. No installation is required on back end servers.

### 416.1 Preparation for Installing Version 2.9

As noted above, you should only upgrade to version 2.9 if your Swivel appliance requires TLS 1.1 or 1.2, i.e. you have appliance version 3 or higher. Note that it is possible to enable support for TLS 1.0 on version 3 appliances, in order to support legacy applications, but for security reasons it is recommended that you do not do this.

Support for TLS protocol versions 1.1 and 1.2 require Microsoft.Net Framework version 4.5 or later and ASP.Net version 4.0. If your Microsoft Exchange server is running on Windows Server 2012 or later, you may already have this, but Server 2008 does not have the requsite .Net Framework installed by default.

Note that the following procedure will require that the Exchange web server is restarted, so a small amount of down time is expected.

Download and install the requisite framework from the Microsoft website, ensuring that ASP.Net support is enabled.

Open IIS manager, and go to Application Pools. Select each MSExchange... application pool, click Basic Settings and change the .Net Framework version to v4.0.30319 (the last number may be different).

Once you have updated all the MSExchange application pools to ASP.Net version 4, restart IIS.

### 416.2 Upgrading to Version 2.9

Version 2.9 uses a different installation mechanism from previous versions. For this reason, it is not possible to upgrade to 2.9 without uninstalling previous versions first. However, it is possible to keep the settings from the previous version as follows:

Under C:\Program Files\Microsoft\Exchange Server\V14\Owa\PINsafeConfig, locate and run ForceUninstall.exe as Administrator. If this program does not exist, you will need to use the alternative mechanism below. Type "yes" to confirm removal, then "n" to prevent the settings being removed. Note that this technique does not remove the program from Programs and Features. You should attempt to remove it from here also, and when you get a warning that the program cannot be removed, accept the option to remove it from the list.

If the ForceUninstall program does not exist, you can use the following manual method:

Under C:\Program Files\Microsoft\Exchange Server\V14\Owa, edit web.config. Search for "PINsafe settings". Copy everything from this line down to "End of PINsafe settings" into a new file and save it. Now uninstall as normal. After installing version 2.9, the configuration program will appear, with blank settings. Cancel this program, then edit web.config as before. You should have default settings for the Swivel filter installed. Remove these and replace with the saved settings. Now run the configuration program again and make any changes as necessary.

### 416.3 Software Installation

Run the executable to install it on the Exchange Server. If your Exchange Server instance is not installed in the default location (C:\Program Files\Microsoft\Exchange Server\V14), you will need to modify the installation path. The installation path should be the root Exchange path.

NOTE: it is not necessary to uninstall the previous filter before installing version 2.7.x or 2.8.x, as long as the previous filter is version 2.7 or later.

## 416.4 Configuration of the IIS Filter

After installation modify the settings. The Filter Configuration should start after installation or can be started through the Start Menu. If the Exchange Server installation is not in the default location, select the OWA directory as above in which to modify the web.config file.

#### 416.4.1 Swivel Settings

Server Name/IP: The Swivel server IP address or hostname

Port: Swivel server port, for a Swivel virtual or hardware appliance use 8080 (not 8443)

Context: Swivel install name, for a Swivel virtual or hardware appliance use pinsafe (not proxy)

Use SSL Select tick box if SSL is used, for a Swivel virtual or hardware appliance tick this box. This also ignores other certificate errors, such as site names not matching.

Secret: The shared secret that must be entered also on the Swivel server Administration Console under Server/Agents

Accept self-signed certificates Where SSL is used with self signed certificates, for a Swivel virtual or hardware appliance tick this box until a valid certificate is installed.

**Proxy Server, Port, Context, Use SSL** These are used to retrieve TURing or Pinpad images. If you are using a version of PINsafe that does not support Pinpad natively (3.9 or earlier), you will need the special version of the virtual or hardware appliance proxy that does support Pinpad. If you are not using Pinpad, you can set these to be the same as the first set of values: if you are not using a virtual or hardware appliance, you MUST set them to be the same.

∭ PIXsie OWA I PIXsia OWA I	free configuration Authentication Excluded Advanced	)	X	
	Piblazía	Proxy		We not the second state of
Server Name/19:	pinsafe.swiveklev local	pinsafe.swiveklev local	]	
Port:	8080	8080		
Context:	pinsafe	pinsafe		and the state of t
	🗹 Uae SSL	🗹 Uaa SSL		
Sacrat:				
Confirm Sacrat:	🗌 Accept est eigred certificates			
			Nore	
OK	Cancel Agely	Varsion 2.3.0.0 Copyrig	n ⊜Swivel Scoure 2016	2-21-22A

#### 416.4.2 OWA Settings

Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

OWA Path: OWA path, usually /owa, unless this has been explicitly changed

Logon Path: Logon path Usually /owa/auth/Logon.aspx

Logoff Path: Logoff path /owa/auth/Logoff.aspx

Auth. URL: This is the URL for OWA authentication and is usually https://<exchange.mycompany.com>/owa/auth/auth.owa

PINacia OWA A	er configuration 🔀 Inartication Excluded Activaticat	איייייייייייייייייייייייייייייייייייי
Server URL:	https://localhost	
OWA Path:	/owa/	
Logan Path:	/owa/auth/Logon.aspx	Managaran Kutha sa anagaran sa Wata Asun Propionis (Rogisto Provid
Lagaii Path:	/owa/auth/Logoff.aspx	
Auth. URL:	/owa/suth.owa	CALLER AND AND AND A CALLER AND
Change PIN URL:	/owa/suth/ChangePin.aspx	at an address and the collect the start startings of the
		**************************************
		CONSTRUCTION OF STRUCTURE AND AND A DESCRIPTION
OK	Cancel Apply Varsion 2.0.0.0 Copyright © Swivel Secure 2016	

#### 416.4.3 Authentication Settings

**Cookie Secret Change:** This is an experimental setting, which increases security by changing the secret used to encrypt the authentication cookie at a specified interval. It is recommended that you leave this at 0, i.e. never change it. In particular, do not change this if you have multiple OWA servers, as it will cause problems.

**Idle Time:** The length of time in seconds that the authentication cookie is valid, provided you make no OWA requests in that time. If you do, the cookie is refreshed and the countdown starts again. If users are being prompted for authentication after short time periods then this value may need to be increased.

Allow non-PINsafe Users If this option is ticked, non Swivel users are allowed to authenticate using standard OWA authentication. This requires Swivel 3.5 or higher. the option to allow unknown users to authenticate without Swivel authentication only applies to users not known to Swivel at all. You cannot specify that it only applies to a group of users, and not to other users who are known to Swivel, but not in a particular group.

Filter Enabled The filter enabled option is mainly for testing, but also to handle situations such as enabling mobile access to the same Exchange Server i.e. ActiveSync and Windows Mobile Device Center. If the filter is disabled, you still need to authenticate through Swivel if you use the standard login page, but it is possible to authenticate using only AD credentials if you have a way to call the AD authentication filter directly.

Ignore Domain Prefix If this option is ticked, any prefixed domain (i.e. anything before the '\' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Ignore Domain Suffix If this option is ticked, any suffixed domain (i.e. anything after the '@' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Show TURing image If this option is ticked, a TURing image is shown to authenticate users.

Show Message on-demand If this option is ticked, a button is displayed to request a security string to be sent via SMS or email.

Show Pinpad If this option is ticked, an Pinpad button array is shown to authenticate users. You cannot have both TURing and Pinpad enabled.

Auto-show image If this option is ticked, the TURing or Pinpad image is requested as soon as the user enters the username and tabs away from it. If this option is not ticked, the user must click a button to show the image.



#### 416.4.4 Excluded Settings

**Excluded Paths:** This allows paths to be set for which authentication is not required to reach them. The paths shown on the display are added by default. The configuration program automatically detects the current build of OWA and includes that.

**Excluded/Included IP addresses:** You can choose to enable PINsafe authentication only for certain source IP addresses. Typically, you will do this if you wish to allow internal access to OWA without PINsafe authentication. Selecting "Exclude IP addresses below" will exclude the listed addresses from PINsafe authentication, while "Only include IP addresses below" will apply PINsafe authentication only to those IP addresses listed. For example, if you know that all external requests will come via a firewall at 192.168.0.99, you can select ?Only include IP addresses below", and enter the single IP address as the address to include. Note that you can enter IP address ranges here using CIDR notation, for example 192.168.0.0/24 or 192.168.0.0/255.255.255.0. PINsafe will always display addresses using the latter format, irrespective of how they are entered. IPv6 addresses are not currently supported.

PNaste OV/A fitter configuration         X           PNaste OV/A fitter configuration         Excluded	
Excluded Paths:	
/owa/14.3.181.6/ /owa/auth.owa /owa/auth/	
Exclude IP addresses below	
OK Cancel Apply Version 2.3.0.0 Capyright © Swivel Secure 2016	

#### 416.4.5 Advanced Settings

**SSL Protocols:** This indicates which protocols can be used for https communication with the Swivel server. The default allows SSLv3 and TLSv1, but the recommended setting for appliance version 3 is TLSv1.1 and TLSv1.2.

Web Proxy Settings: If the Exchange server needs to connect to a proxy server to access the Swivel server, you should specify the details here. Unless you are aware of such details, leave these as "None".

User Agent string: and Custom headers: These settings modify the http request sent to the Swivel server. Typically, you will not need to use these, but you may be aware of firewall rules between the servers which require such settings.

**Test User:** and **Test Settings** In order to test the settings, the configuration program will send a session start request on behalf of a user. You should enter a username that exists in the Swivel database (the default is 'admin'), then click Test Settings to confirm that the connection between the OWA Server and the Swivel server is correctly configured.

∭RIGER OVA fiter co	niguration	2	
SSL Protocols	Silien Texculoso Web Proxy Saltings None		
User Agent String:		Test Daer: admin	
Örstern Handars:		Test Settings	
OK Ci	ocal Apply Vasion 3	2.3.0.0 Copyright ^{agi} Swivel Secure 2016	

### 416.5 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

- 1. On the Swivel Management Console select Server/Agent
- 2. Enter a name for the Agent
- 3. Enter the Exchange IP address
- 4. Enter the shared secret used above on the Exchange Filter
- 5. Click on Apply to save changes

Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	•••••	
	Group:	ANY	
	Authentication Modes:	ALL	Delete
			0
	Name:	IIS	
	Name: Hostname/IP:	IIS 192.168.1.1	
	Name: Hostname/IP: Shared secret:	IIS 192.168.1.1	
	Name: Hostname/IP: Shared secret: Group:	IIS 192.168.1.1 ANY	

#### **Configure Single Channel Access**

1. On the Swivel Management Console select Server/Single Channel

Server>Single Channel 🥘	
Please specify how single channel security string	gs are delivered.
Image file:	turing.xml 💌
Rotate letters:	No 💌
Allow session request by username:	Yes
Only use one font per image:	Yes 💌
Jiggle characters within slot:	No 💌
Add blank trailer frame to animated images:	Yes 💌
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static 💌
Multiple AUthentications per String:	No 💌
Generate animated images:	No 💌
Random glyph order when animating:	No 💌
No. Characters Visible:	1
	Apply Reset

## 416.6 Using additional attributes for authentication

When using additional attributes for authentication see User Attributes How To

## 417 Additional Installation Options

### 417.1 Modifying the login Page to stop the Single Channel Image automatically appearing

NOTE: this refers to older versions of the filter. In versions 2.5 and higher, this is set in the configuration program.

By default the single channel authentication will appear when the username and AD password is entered and the user selects the OTC field. As a single channel session has started the Swivel server is expecting an OTC to be entered from the Single Channel TURing image. If dual channel authentication is required then the automatic display of the Single Channel Turing image needs to be turned off. This can be done by modifying the login.asp file which by default is located in C:\Program Files\Exchsrvr\exchweb\bin\auth. The following needs to be removed from the username attribute field:

onblur=?checkUser()?

## 417.2 Modifying the login Page to allow Dual Channel On Demand Delivery

NOTE: this refers to older versions of the filter. In versions 2.5 and higher, this is set in the configuration program.

If you want to use only dual-channel on-demand and no other method, then you can manage this by a simple change to image.asp (under /exchweb/bin/auth). Edit this file, search for "SCImage" and replace it with "DCMessage". Leave the onblur attribute as it was. Dual channel authentication for the user and also On Demand Delivery should be enabled on the Swivel Administration console under Server/Dual Channel.

# 418 Verifying the Installation

Enter a username and AD password then the Swivel OTC for dual channel authentication. For single channel authentication enter the username, AD password then click on the button to generate a Single Channel Turing Security String, enter the OTC and login.

The below image shows the login page with PINpad.

	Neb App	
Security ( show e	xplanation )	
<ul> <li>This is a public or shared computer</li> <li>This is a private computer</li> </ul>		
🔲 Use the	light version of Outlook Web App	
User name:	swiveldev\demouser	
Password:		
One-Time Code:		
	2 0 1 9 7 4 8 6 3 5 Refresh	
	2 0 1 9 7 4 8 6 3 5 Refresh	Change PIN

## 419 Uninstalling the Swivel Integration

Uninstall the Swivel IIS filter, this should restore all the original files. If it does not work then find the file Logon.aspx.sav located in ClientAccess\owa\auth\ which can be restored to the original Login.aspx.

WARNING: In versions of the filter earlier than 2.5, the login page customisation program did not check if the customisation was already done. This could cause the file Logon.aspx.sav to be overwritten with a customised page. In this case, you will need to locate another copy of the original file, or contact support@swivelsecure.com for assistance.

### 419.1 Uninstalling Manually

NOTE: This procedure should only be undertaken if uninstalling using the menu option (or Programs and Features) fails. For safety, you are advised to make copies of all modified or removed files to a safe location outside the Exchange Server installation.

Firstly, locate the OWA folder. The default location for this is C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa.

Edit web.config in this folder: note that you may need to open your editor as Administrator in order to be able to change it. Search for the <modules> section. Within this, there should be a line such as the following:

<add type="com.swivelsecure.owafilter.PINsafe0WAFilter, PINsafe0WAFilter, Version=2.8.5.1, Culture=neutral, PublicKeyToken=xxxx" name="PINsa

The Version number and PublicKeyToken may vary. Remove this line, making sure not to remove anything else.

Locate the section beginning with

and ending with

Remove everything within this section. If you intend to reinstall the filter later, you might want to copy these settings somewhere for later reference. Alternatively, make a backup of the entire web.config.

Save the modified web.config.

Restart IIS to release the Swivel filter.

Delete the folder "PINsafeConfig" and all its contents.

Go into the "Bin" subfolder and delete the 3 DLLs beginning with "PINsafe": PINsafeClient.dll, PINsafeLogin.dll and PINsafeOWAFilter.dll.

Go into the "auth" subfolder and delete the following files:

- ChangePIN.aspxCheckClient.aspx
- CheckUser.aspx
- pinpadBlank.png
- pinpadClear.png pinpadNext.png
- pinpadPrev.png
- pinpadRefresh.png
- pinsafe.js
- pinsafe_cp.js
  PINsafeLogon.aspx
- SCImage.aspx
- SCPinpad.aspx
- SessionStart.aspx
- turingBlank.jpg
- Logon.aspx.old

Depending on which version of the filter you have, you may not have all of these files.

The final step is to restore the original logon page. You should have a file named Logon.aspx.sav. If this file does not exist, please contact support@swivelsecure.com for help. Delete the file Logon.aspx, and rename Logon.aspx.sav to Logon.aspx.

Now test that your OWA logon works without Swivel. Some older versions of the filter would apply the logon page modification multiple times, which means that Logon.aspx.sav also had the Swivel modifications. If you find that the Logon page still has Swivel modifications, then please contact support@swivelsecure.com to request advice on restoring the original Logon page.

## 420 Change PIN

The OWA filter includes a page for the user to change their PIN. It can be configured to redirect to the change PIN page automatically if the user's PIN has expired, and you can also include a link to the Change PIN page on the login page.

If you selected the Change PIN page in error, and want to return to the login page, then click the "Cancel" button ("Skip" button before 2.8.4) to return without changing your PIN.

NOTE: from version 2.8.4 onwards, the fields are shown one at a time. Click "Next" or press Tab to show the next field, or "Back" to go back and correct a field. See the Pinpad section below for example screen shots.

### 420.1 Change PIN with PinPad

The following instructions refer to the Change PIN page from version 2.8.4 onwards. See the following section for older versions.

The initial screen (with or without Pinpad) looks like this:

Outlook Web App
Swivel PIN Change Utility
Username: Cancel Back Next

Enter your username and click "Next" or press Tab to show the next field and the Pinpad:

Outlook [®] Web App		
Sw	vivel PIN Change Utility	
Username:	user1	
Current OTC:		
Cance		

Click the buttons corresponding to the digits of your current PIN and then "Next":

Outlook	Outlook ⁻ WebApp		
Sw	Swivel PIN Change Utility		
Username:	user1		
Current OTC:			
New OTC:			
Cance	Back Next		
	4 5 1		
	9 6 3		

Click the buttons corresponding to the digits of your new PIN and then "Next":

Outlook Web App	
Swive	l PIN Change Utility
Username:	user1
Current OTC:	••••
New OTC:	
Confirm New OTC:	
Cancel	Back       Change Pin         4       5       1         9       6       3         0       2       8         R       7       C

Enter your new PIN again, to confirm, and then click "Change Pin".

#### 420.1.1 PinPad prior to Version 2.8.4

When PinPad is enabled, there are 3 OTC fields, all of which can potentially use the Pinpad. For this reason, additional buttons are provided to select the field which is the target of the Pinpad:



You will notice that the current OTC field is highlighted in green. To select the next field, click on the down arrow button, or to go back to the previous field, click the up arrow button. You can also select an OTC field simply by clicking on it, or its label.

The "R" button will refresh the Pinpad (i.e. show a new pad), and the "C" button will clear the selected OTC field.

## **421 Troubleshooting**

Check the Swivel and OWA server logs

No login page, check the Exchange version. The filter needs to match the Exchange version number, and the file login.aspx needs to be modified so that it references the correct exchange install version.

Red Cross instead of Turing image, right click on red cross and look at its properties. Ensure Swivel server is running.

If you do not see a Turing image when using start session then in a web browser test the following link from the OWA server. If an image is not seen, then there is a problem either with communicating with the Swivel server or the Allow Image request by username may be set to No.

For Swivel virtual or hardware appliances and software installs:

http(s)://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

## 421.1 Enabling debug logging

Additional logging can be configured for troubleshooting, and will log from the time it was enabled.

edit C:\Program Files\Microsoft\Exchange Server\v14\ClientAccess\OWA\web.config

Locate

<add key="PINsafeEnableDebug" value="true" /> <add key="PINsafeDebugLocation" value="C:\Users\Public\Documents\PINsafeOWAFilter.log" />

### 421.2 User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

### 421.3 Turing image appears but user cannot authenticate

Verify that the OWA is configured to use port 8080 and context pinsafe. Port 8443 and context proxy will cause problems with authenticating users but allow the Turing image to be displayed. Note that this refers to the main PINsafe settings (for version 2.6 or higher) - the proxy settings SHOULD have these values if required.

## 421.4 User Authenticates Successfully to Swivel but OWA Login Page is Redisplayed

If you have entered the correct credentials, and the Swivel logs show successful authentication, but you are still redirected to the login page, the problem might be related to host names and/or SSL certificates.

First of all, if you connect to OWA using the IP address, or "localhost" from the OWA server itself, the Swivel filter will redirect you to the host name configured in the filter. This may result in the authentication cookie being lost, because the domain name doesn't match. In this case, attempting to authenticate a second time, with the correct host name, should succeed.

The second possibility is that the SSL certificate on the OWA Server doesn't match the host name used by the OWA filter, or the certificate has expired or is not trusted. This will result in authentication to OWA, from the Swivel filter, failing.

The solution for a production server is to ensure that the Exchange Server has a commercial SSL certificate, and that the Swivel OWA filter uses the host name that matches this.

For a development environment, you can generate a self-signed certificate with the correct host name, and add this to the list of trusted certificates on both the OWA server itself and the client (the latter might not be necessary). You might also need to add the host name to the hosts file on one or both of these.

NOTE: Version 2.7 or later of the filter should eliminate most of these problems. If you are still having problems of this nature with 2.7, please contact support@swivelsecure.com.

### 421.5 Name resolution issue

The Exchange server may be looking for exchange.company.com from the internal network but cannot resolve it. Edit the hosts file mapping the name to 127.0.0.1. Also ensure that the internal CA certificate is trusted by the OWA server.

Again, this problem is no longer relevant in version 2.7 onwards.

## 422 Known Issues and Limitations

### 422.1 Known Issues with Version 2.9

It has been observed that the first time the website is accessed after installing the 2.9 filter, an error page is seen. This disappears after refreshing the page, and does not appear to recur.

#### 422.1.1 Problems With Connection Settings

We have experienced problems with installations of the filter when Exchange 2010 is installed on Windows Server 2012, or when certain security updates are installed in Windows Server 2008. While the exact cause is not yet known, it seems to be related to SSL connection settings. We have found success in making adjustments to the SSL settings and User Agent string.

There is a beta release of version 2.8.7 available from here which allows you to adjust these settings.

#### 422.1.2 Default Exclusions Not Applied

There is a known issue with versions up to 2.8.5 that if you apply an update to Exchange that causes the Exchange version number to change, the folder containing the latest version of images etc. is not automatically added to the list of exclusions. Even though it is shown in the configuration program, it isn't saved.

The recommended solution is to update to 2.8.6. Here, if you reapply the logon changes after an update, it will also update the version-specific inclusions.

The workaround for this is to alter another configuration item, then save the configuration. You can subsequently change the other item back again, but making another change will force the exclusions to be updated.

#### 422.1.3 One-time Code Not Shown

There is a known issue if you are using the option to allow unknown users to log on without Swivel credentials. With certain versions of the core, users are not recognised, even though they are known to exist in the Swivel database.

Another problem, Swivel may not recognise email addresses if the Swivel username is not the email address.

Both of these problems can be resolved by the same solution: you need to use a hidden option:

Edit the OWA web.config file (by default in C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa). Note that you will probably need to open your text editor as Administrator in order to save changes.

Locate the following line:

<add key="PINsafeMultiUsername" value="False" />

If the above line is found, change value to "True".

If you cannot find the above line, search for

Insert the following line before the above line:

<add key="PINsafeMultiUsername" value="True" />

Note that this option will not work with versions of PINsafe earlier than 3.8.

#### 422.1.4 Private Computer Option Doesn't Stay Selected

If your login page always defaults to Public computer and you have to select Private every time you log in, please upgrade to the latest version of the filter.

#### 422.1.5 Swivel Customisation Lost

Updates may result in the login page customisation being removed. In this case, you must select the option "Reapply Logon Page Changes" from the Swivel filter start menu. IMPORTANT: in versions earlier than 2.5, make sure you do not use this option on a page that has already been customised. This will cause the page to become corrupted, and will also overwrite the backed up, unmodified file.

Updates to the 2010 server may also require changes to the Excluded paths. In version 2.8.6 or later, running "Reapply Logon Page Changes" fixes this too. In version 2.5 or later, the updates are handled by the configuration program, but if you do not change any other settings, the update will not be applied.

#### 422.1.6 Later Versions of the Filter Not Working With Service Pack 1

We have had reports of the latest filter not working with Exchange Server Service Pack 1. The recommended solution is to upgrade to the latest service pack, but you might like to try the following (version 2.8.3 or later):

Insert the following line in web.config (see description above):

<add key="PINsafeUseOldAuthentication" value="True" />

This option reverts to the authentication mechanism used in version 2.6 and earlier. It is not known whether this is the cause of the problems seen, but it has been shown to work in some installations.

#### 422.1.7 Logging

By default, the filter does not record any audit information, but it may be useful to do so for monitoring and debugging purposes. You can enable logging by adding the following line in web.config:

<add key="PINsafeEnableDebug" value="True" />

This writes logs to C:\Users\Public\Documents\PINsafeOWAFilter.log. You can change the file location with the following option:

<add key="PINsafeDebugLocation" value="FullFilePath" />

Replace *FullFilePath* above with the full path of the file to write to. Make sure that the account that OWA is running as has write permissions to that file/folder. </nowiki>

## 423 Multiple Swivel Servers

Versions 2.5 and later include the option to add multiple Swivel servers. Then, if the first one is unavailable, the filter will try the other servers in the order listed. The filter will always remember the last Swivel server successfully contacted and try that one first.

To support multiple servers, there is an additional button on the Swivel tab of the configuration program, which brings up a secondary dialogue containing a list of available servers. Use this to add or delete Swivel servers, and to select one to modify (the details are modified on the main dialogue).

# 424 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.

# 425 Microsoft OWA 2013 IIS Integration

## 426 Introduction

Swivel allows users to authenticate users of Outlook Web Access (OWA) 2013 with Microsoft Exchange Server running on Microsoft 2012 server. Active Sync users are able to receive email without Swivel authentication as this uses a separate URL. This article describes how to integrate Swivel with OWA 2013.

So far as the Swivel integration is concerned, there are no significant differences between OWA 2013 and 2016 or 2019. Therefore, the OWA 2013 filter should work with OWA 2016 and 2019 as well.

# 427 Compatibility

Microsoft Exchange Version and update release	<b>Build Version</b>	<b>Compatibility Status</b>
Exchange Server 2013	15.0.516.32	Compatible
Exchange Server 2013 CU 3	15.0.775.38	Compatible
Exchange Server 2016	15.1.225.42	Compatible
Exchange Server 2019	15.2.858.5	Compatible

Note: Updates may result in the login page customisation being removed. In this case, you must select the option "Reapply Logon Page Changes" from the Swivel filter start menu. Updates to the 2013 server may also require changes to the Excluded paths. See the **Troubleshooting** and **Known Issues** and Limitations sections before updating.

## **428 Prerequisites**

- Microsoft Exchange 2013 or 2016 with OWA
- Microsoft 2012 Server R2
- Microsoft.Net Framework version 4.5
- Swivel 3.7 or later
- Users are able to login using standard OWA forms-based authentication.
- * As the OWA server proxies the image request for Single channel TURing images and Pinpad, the Swivel server does not need a NAT.

NOTE: above is the test environment used for the filter. It will probably work with earlier versions of the Operating System (e.g. 2008), as long as version 4.5 of the .Net framework is installed.

## 429 File Downloads

- Version 2.12. Changes:
  - Settings are retained on upgrade of this product or of OWA: the settings are now saved to a location outside the OWA folder (C:)ProgramData\Swivel Secure\OWA Filter). Note that this doesn't apply to upgrade from a version earlier than 2.12.
     Support for logging within the configuration program. Logs are written to C:\ProgramData\Swivel Secure\OWA Filter.

  - Version 2.12.3 ensure that data folder exists before trying to read from it.
     Version 2.12.2: Bug in program to re-apply logon page changes after OWA upgrade now fixed.
     Version 2.12.2: control over which attributes are checked for unknown users
- Version 2.12.2: more control over logging
   Version 2.12.2: fixed issue with Cookie encryption
   Version 2.11. The main change here is support for Push authentication. Due to technical issues, this version is available from a server that does not have https support. For this reason, you cannot simply click on the link in most browsers. Instead, you must right-click on it, copy the link address and open it in a new tab.
- Version 2.10. This is largely a rebranding of version 2.9. It also uses default settings that are more relevant for newer versions of Sentry, and references OWA 2016 and 2019. One notable change is that the reference to proxy server has been removed, as it is no longer necessary.

NOTE: We apologise that the original installer for version 2.10 was missing a file. This has now been corrected, but if you installed the original version and don't want to reinstall, you can simply unzip ChangePIN.aspx and place it in the swivel folder of the OWA web site. The usual location for this is C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\swivel.

- Version 2.9. This version includes support for TLS version 1.1 and 1.2. It is only necessary to upgrade to this version if you have a Swivel appliance version 3. Version 2 appliances work fine with version 2.8, and no other new features have been added.
  Version 2.8.7. Some minor updates copied from OWA 2010 filter, plus bug fix for images not displaying in certain circumstances. Now
- supports upgrading without uninstalling.

## 430 Architecture

The Exchange server makes authentication requests against the Swivel server by XML authentication

## 431 Installation

### 431.1 Software Installation

Run the executable to install it on the Exchange Server. If your Exchange Server instance is not installed in the default location (C:\Program Files\Microsoft\Exchange Server\V15), you will need to modify the installation path. The installation path should be the root Exchange path.

### 431.2 Configuration of the IIS Filter

After installation modify the settings. The Filter Configuration should start after installation or can be started through the Start Menu. If the Exchange Server installation is not in the default location, select the OWA directory as above in which to modify the web.config file.

#### 431.2.1 Swivel Settings

Server Name/IP: The Swivel server IP address or hostname

Port: Swivel server port, for a Swivel appliance use 8080 (not 8443)

**Context:** Swivel install name, for a Swivel appliance use Swivel (not proxy)

Use SSL Select tick box if SSL is used, for a Swivel appliance tick this box. This also ignores other certificate errors, such as site names not matching.

Secret: The shared secret that must be entered also on the Swivel server Administration Console under Server/Agents

Accept self-signed certificates Where SSL is used with self signed certificates, for a Swivel appliance tick this box until a valid certificate is installed.

**Proxy Server, Port, Context, Use SSL** These are used to retrieve TURing or Pinpad images. If you are using a version of PINsafe that does not support Pinpad natively (3.9 or earlier), you will need the special version of the appliance proxy that does support Pinpad. If you are not using Pinpad, you can set these to be the same as the first set of values: if you are not using an appliance, you MUST set them to be the same. Version 2.10 removes the proxy settings altogether.

<u>M</u> a	P. Nsaie O	WA filter configuration	
PINsafe DWA .	Authentication Excluded		
	PINsafe	Proxy	
Server Name/1P:	pinsafe.swdsmo.local	pinsafe.swdemo.lacal	
Port:	8080	8080	
Context:	pinsafe	pinsafe	
	🖌 Use SSL	Vie SSL	
Secret:		1	
Confirm Secret:	000000	1	
		]	Anna Anna Anna Anna Anna Anna Anna Anna
	V Accept ser agned certin	Mars	
OX	Cancel Asp	y Version 2.8.0.12 Copyright ⊜ Swivel Secure 2014	

#### 431.2.2 OWA Settings

Server URL: Exchange Server URL, Example: https://<exchange.mycompany.com>

OWA Path: OWA path, usually /owa, unless this has been explicitly changed

Logon Path: Logon path Usually /owa/auth/Logon.aspx

Logoff Path: Logoff path /owa/auth/Logoff.aspx

Auth. URL: This is the URL for OWA authentication and is usually /owa/auth/auth.owa
Change PIN URL: This is the URL for the Change PIN page. Note that the default URL is actually incorrect, but this value is currently ignored anyway.

	P Nsaie OWA filter configuration	
PINsafe OWA A	uthentication Excluded	ning and a set of a single state of a
Sarver URL:	https://exch.swdemo.local	
OWA Petr:		an According to the second sec
Logon Path:	/awa/auth/Logan.aspx	
Logoif Path:	/owa/auth/Logoff.aspx	
Auth. URL:	/owa/auth.owa	
Change PIN URL:	/owa/auth/ChangePin.aspx	
ΟX	Cancel Apply Version 2.8.0.12 Copyright © Swivel Secure 2014	
Hamming		

#### 431.2.3 Authentication Settings

**Cookie Secret Change:** This is an experimental setting, which increases security by changing the secret used to encrypt the authentication cookie at a specified interval. It is recommended that you leave this at 0, i.e. never change it. In particular, do not change this if you have multiple OWA servers, as it will cause problems.

Idle Time: The length of time in seconds that the authentication cookie is valid, provided you make no OWA requests in that time. If you do, the cookie is refreshed and the countdown starts again. If users are being prompted for authentication after short time periods then this value may need to be increased. The idle time on the Swivel OWA filter is in addition to the session timeout built into OWA. The Swivel timeout will never increase the OWA timeout, only reduce it. Therefore, it will not compromise the security of the public computer settings.

Allow non-PINsafe Users If this option is ticked, non Swivel users are allowed to authenticate using standard OWA authentication. This requires Swivel 3.5 or higher. the option to allow unknown users to authenticate without Swivel authentication only applies to users not known to Swivel at all. You cannot specify that it only applies to a group of users, and not to other users who are known to Swivel, but not in a particular group.

Filter Enabled The filter enabled option is mainly for testing, but also to handle situations such as enabling mobile access to the same Exchange Server i.e. ActiveSync and Windows Mobile Device Center. If the filter is disabled, you still need to authenticate through Swivel if you use the standard login page, but it is possible to authenticate using only AD credentials if you have a way to call the AD authentication filter directly.

Ignore Domain Prefix If this option is ticked, any prefixed domain (i.e. anything before the '\' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Ignore Domain Suffix If this option is ticked, any suffixed domain (i.e. anything after the '@' character) is removed before sending the username to PINsafe. The full username is sent to OWA.

Show TURing image If this option is ticked, a TURing image is shown to authenticate users.

Show Message on-demand If this option is ticked, a button is displayed to request a security string to be sent via SMS or email.

Show Pinpad If this option is ticked, an Pinpad button array is shown to authenticate users. You cannot have both TURing and Pinpad enabled.

Auto-show image If this option is ticked, the TURing or Pinpad image is requested as soon as the user enters the username and tabs away from it. If this option is not ticked, the user must click a button to show the image.

Show Change PIN link If this option is ticked, a link to the Change PIN page will be shown on the login page.

Redirect to Change PIN on PIN expiry If this option is ticked, users are automatically redirected after successful login to the Change PIN page, if their PIN has expired.

<b>\$</b>	PINsafe OWA filter configuration				
PINsafe OWA Authentication	Excluded				
Cookie Secret Change: 0	hours				
Idle Time (secs): 300	Idle Time (secs): 300				
Allow non-PINsafe Users	Show TURing image				
✓ Filter Enabled	Show Message on-demand				
✓ Ignore Domain Prefix	Show Pinpad				
Ignore Domain Suffix	Auto-show Image				
Show Change PIN link	Redirect to Change PIN on PIN expiry				
OK Cancel	Apply Version 2.8.0.12 Copyright © Swivel Secure 2014				

### 431.2.4 Excluded Settings

Excluded Paths: This allows paths to be set for which authentication is not required to reach them. The paths shown on the display are added by default.

**Excluded/Included IP addresses:** You can choose to enable PINsafe authentication only for certain source IP addresses. Typically, you will do this if you wish to allow internal access to OWA without PINsafe authentication. Selecting "Exclude IP addresses below" will exclude the listed addresses from PINsafe authentication, while "Only include IP addresses below" will apply PINsafe authentication only to those IP addresses listed. For example, if you know that all external requests will come via a firewall at 192.168.0.99, you can select ?Only include IP addresses below?, and enter the single IP address as the address to include. Note that you can enter IP address ranges here using CIDR notation, for example 192.168.0.0/24 or 192.168.0.0/255.255.255.255.0. PINsafe will always display addresses using the latter format, irrespective of how they are entered. IPv6 addresses are not currently supported. To add multiple addresses, enter them into a text editor, one per line then copy and paste all entries, into the excluded field.

<b>\$</b>	PINsafe OWA filter configuration
PINsafe OWA Authentication	Excluded
Excluded Paths:	
/owa/auth.owa /owa/auth/	
Exclude IP addresses below	✓
	× ×
OK Cancel	Apply Version 2.8.0.12 Copyright © Swivel Secure 2014

### 431.2.4.1 External/Internal User Authentication

Using the above excluded IP addresses it is possible to configure a range of IP addresses for users, such as internal users, that will not be required to use Swivel authentication.

### 431.3 Configure The Swivel Server

### 431.3.1 Configuring Swivel for Agent XML Authentication

To allow communication from the OWA server to the Swivel server we need to configure an agent, see Agents How to Guide

### 431.3.2 Configuring Swivel for Single Channel Images

If Swivel Single Channel images are to be used for authentication, then the following guide can be used.

Single Channel How To Guide

### 431.3.3 Configuring Swivel for Dual Channel Authentication

If Swivel Dual Channel authentication methods are to be used, refer to the following guide:

**Transport Configuration** 

# 432 Verifying the Installation

Enter a username and AD password then the Swivel OTC for dual channel authentication. For single channel authentication enter the username, AD password then click on the button to generate a Single Channel Turing Security String, enter the OTC and login.

The below image shows the login page with PINpad.



# 433 Change PIN

The Change PIN page is reasonably self-explanatory, but using Pinpad with change PIN may need some clarification.

You will notice on the screen shot that "Old OTC:" is highlighted. This means that clicking on the Pinpad digits will enter the corresponding digit into that field. To change the active field, either click on the field itself, or click the arrow keys in the Pinpad display.

The R key will refresh the Pinpad display (i.e. display a new security string), and the C key will clear the currently-active field.



# 434 Uninstalling the Swivel Integration

Uninstall the Swivel IIS filter, this should restore all the original files. If it does not work then find the file Logon.aspx.sav located in the Exchange Server folder (default is C:\Program Files\Microsoft\Exchange Server\V15) under the sub-folder FrontEnd\HttpProxy\owa\auth\. Rename this to restore the original Login.aspx.

# 435 Troubleshooting

Check the Swivel and OWA server logs

No login page, check the Exchange version. The filter needs to match the Exchange version number, and the file login.aspx needs to be modified so that it references the correct exchange install version.

Red Cross instead of Turing image, right click on red cross and look at its properties. Ensure Swivel server is running.

If you do not see a Turing image when using start session then in a web browser test the following link from the OWA server. If an image is not seen, then there is a problem either with communicating with the Swivel server or the Allow Image request by username may be set to No.

For Swivel appliances and software installs:

http(s)://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

# 435.1 Enabling debug logging

Additional logging can be configured for troubleshooting, and will log from the time it was enabled.

edit C:\Program Files\Microsoft\Exchange Server\v15\FrontEnd\HttpProxy\owa\web.config

Locate

<add key="PINsafeEnableDebug" value="true" /> <add key="PINsafeDebugLocation" value="C:\Users\Public\Documents\PINsafeOWAFilter.log" />

## 435.2 User regularly times out after a short interval

The session is kept open by user activity. If this is insufficient then increase the cookie idle timeout value.

### 435.3 Turing image appears but user cannot authenticate

Verify that the OWA is configured to use port 8080 and context pinsafe. Port 8443 and context proxy will cause problems with authenticating users but allow the Turing image to be displayed. Note that this refers to the main PINsafe settings (for version 2.6 or higher) - the proxy settings SHOULD have these values if required.

## 435.4 User Authenticates Successfully to Swivel but OWA Login Page is Redisplayed

If you have entered the correct credentials, and the Swivel logs show successful authentication, but you are still redirected to the login page, the problem might be related to host names and/or SSL certificates.

First of all, if you connect to OWA using the IP address, or "localhost" from the OWA server itself, the Swivel filter will redirect you to the host name configured in the filter. This may result in the authentication cookie being lost, because the domain name doesn't match. In this case, attempting to authenticate a second time, with the correct host name, should succeed.

The second possibility is that the SSL certificate on the OWA Server doesn't match the host name used by the OWA filter, or the certificate has expired or is not trusted. This will result in authentication to OWA, from the Swivel filter, failing.

The solution for a production server is to ensure that the Exchange Server has a commercial SSL certificate, and that the Swivel OWA filter uses the host name that matches this.

For a development environment, you can generate a self-signed certificate with the correct host name, and add this to the list of trusted certificates on both the OWA server itself and the client (the latter might not be necessary). You might also need to add the host name to the hosts file on one or both of these.

## 435.5 Name resolution issue

The Exchange server may be looking for exchange.company.com from the internal network but cannot resolve it. Edit the hosts file mapping the name to 127.0.0.1. Also ensure that the internal CA certificate is trusted by the OWA server.

# 436 Known Issues and Limitations

Updates may result in the login page customisation being removed. In this case, you must select the option "Reapply Logon Page Changes" from the Swivel filter start menu.

There appears to be a problem locating the correct folder for OWA in some cases. We are investigating the cause of this, but meanwhile, if you are prompted to select the OWA folder, you should use the following:

C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HTTPProxy\owa

If Exchange Server is installed in a non-standard location, adjust the path accordingly, but the last part (FrontEnd\HTTPProxy\owa) should be the same.

# 436.1 TLS 1.2 Support

We have observed problems recently with the filter not working if TLS 1.2 only is enabled. We believe the problem is that the TLS 1.2 ciphers supported by Windows Server and the version of Java on our appliances do not overlap. If you are unable to connect the OWA filter to your Sentry appliance, it may be necessary to re-enable TLS 1.1 support on both the OWA filter and the appliance, and to enable the following cipher suite on the appliance: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA. In order to add this cipher suite, you will need command line access, so you will need assistance from Swivel Secure support.

# 436.2 Themes Support

The filter has been written and tested using the default theme (as seen in the screen shots). The screens may not look right (although they should still work) if the theme is changed. However, it should only be necessary to change the stylesheet in order to correct this. Please contact support@swivelsecure.com if you have difficulties getting the display looking right. In particular, the Change PIN page will only work with the default theme, and with the OWA 2013 versions listed above.

# 437 Multiple Swivel Servers

Versions 2.5 and later include the option to add multiple Swivel servers. Then, if the first one is unavailable, the filter will try the other servers in the order listed. The filter will always remember the last Swivel server successfully contacted and try that one first.

To support multiple servers, there is an additional button on the Swivel tab of the configuration program, which brings up a secondary dialogue containing a list of available servers. Use this to add or delete Swivel servers, and to select one to modify (the details are modified on the main dialogue).

# 438 Additional Information

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

# 439 Microsoft OWA with OMA on Exchange 2003

## 439.1 OWA and OMA on Exchange 2003 Integration Notes

the following Microsoft knowledge base article might be of interest:

http://support.microsoft.com/kb/817379

# 439.2 Article Summary

When you try to access a Microsoft Exchange Server 2003 computer by using Microsoft Office Outlook Mobile Access or Exchange ActiveSync, you may experience connection or synchronization problems. These issues can occur if either of the following conditions is true:

The Exchange virtual directory on an Exchange back-end server is configured to require SSL.

Forms-based authentication is enabled.

However, these issues do not occur if these same conditions are true on the Exchange virtual directory on a front-end server.

# 440 Microsoft Terminal Services Integration

### 440.1 Overview

PINsafe integrates with the Microsoft Windows GINA to allow authentication through Terminal Services. For further information see Microsoft Windows GINA login

# 441 Microsoft TMG 2010 Integration

## 441.1 Microsoft Forefront Threat Management Gateway (TMG) Integration Notes

### 441.2 Introduction

This document outlines the necessary steps to integrate Swivel authentication into Microsoft TMG Server 2010 for use with Swivel for Dual Channel authentication using SMS, Mobile Phone Clients and Single Channel using TURing, PINpad and the Taskbar. If the TMG server is part of a cluster then the filter needs to be installed on each server in the cluster.

### 441.3 Prerequisites

This installation guide assumes that publication of the relevant service has already been configured in TMG Server, following the relevant instructions. In addition a working Swivel server version 3.1 or later is required. Certain features of the filter require later versions of Swivel:

- If the option to allow unknown users is required, this requires Swivel 3.4 or later.
- If the option to use Pinpad is required, the Swivel version must be 3.9.2 or higher, or a version of the appliance proxy from 2012.

The Swivel Configuration utility requires .Net version 2 or higher. This is not supplied above and must be downloaded and installed if you do not already have it.

The TMG server and its configuration should be fully backed up prior to the Swivel integration.

Allow around 1 hour downtime per TMG server for the integration, and the integration will require a restart of the TMG Firewall Services. If you are replacing an older version of the Swivel filter, you must uninstall that version first. The filter configuration will not be lost. You will need to stop the TMG firewall service before uninstalling the old filter, or else you will be prompted to restart the server to complete uninstallation.

### 441.3.1 Swivel TMG 2010 Filter

The filter can be downloaded from here. NOTE: this is version 1.4.4 of the TMG filter, released 1/11/13. Version 1.4.4 fixes a bug found by some customers, whereby the login page was not detected in some circumstances, allowing authentication by password only. The same bug could also cause other failures, such as occasionally failing to show a TURing image. This version also adds better control over logging. See the included documentation for more details.

Version 1.4.3 was never released, but made detection of the required URLs case-insensitive.

Version 1.4.2 includes some bug fixes and enhancements, in particular:

- Redirecting to the login page after an incorrect one-time code now works correctly. This means that an error message is displayed if the
  one-time code is incorrect. It is also expected that this will resolve issues experienced by some customers whereby, having logged in once,
  users do not always have to re-enter their one-time code.
- The firewall service is restarted automatically after making configuration changes and before uninstalling the filter.

Version 1.4.1 fixes some bugs present in version 1.4.0. Version 1.4 includes a number of enhancements over previous versions. See the included documentation.

NOTE: if you are using this filter with RADIUS authentication, be aware that there are some errors in the file usr_pwd_pcode.htm. These need to be fixed manually - contact support@swivelsecure.com for details. An update with the correct script will be released shortly.

### 441.4 Baseline

Swivel 3.1 or later (3.6 or later preferred)

Microsoft Forefront TMG 2010

Web-based server, typically Microsoft IIS-based, to be protected, such as OWA or SharePoint.

### 441.5 Architecture

The TMG server makes authentication requests against the Swivel server by XML or RADIUS. Some of the additional features are only available in the XML authentication. For security reasons Sharepoint authentication should be configured using RADIUS. The Swivel installation creates a separate custom login.

## 441.6 Swivel Configuration

### 441.6.1 Configure a Swivel Agent For XML Authentication

1. On the Swivel Management Console select Server/Agent

- 2. Enter a name for the Agent
- 3. Enter the TMG internal IP address
- 4. Enter the shared secret
- 5. Click on Apply to save changes

Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	•••••	
	Group:	ANY	
	Authentication Modes:	ALL	Delete
	Name:	IIS	
	Hostname/IP:	192.168.1.1	
	Hostname/IP: Shared secret:	192.168.1.1	
	Hostname/IP: Shared secret: Group:	192.168.1.1	

# 441.6.2 Configure Single Channel Access

1. On the Swivel Management Console select Server/Single Channel

2. Ensure ?Allow session request by username? is set to YES

Server>Single Channel @	
Please specify how single channel security string	gs are delivered.
Image file:	turing.xml 💌
Rotate letters:	No
Allow session request by username:	Yes
Only use one font per image:	Yes 💌
Jiggle characters within slot:	No 💌
Add blank trailer frame to animated images:	Yes 💌
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static 💌
Multiple AUthentications per String:	No 💌
Generate animated images:	No 💌
Random glyph order when animating:	No 💌
No. Characters Visible:	1
	Apply Reset

### 441.6.3 Configure a RADIUS NAS entry for Sharepoint authentication

NOTE: this is only required if you wish to use RADIUS authentication with Swivel. This is recommended for SharePoint integration and optional for other solutions.

- 1. Ensure the RADIUS server is running on Swivel
- 2. On the Swivel Management Console select RADIUS NAS
- 3. Enter a name for the NAS
- 4. Enter the TMG internal IP address
- 5. Enter the shared secret
- 6. Click on Apply to save changes

# 441.7 Swivel TMG Filter Upgrade

If an existing filter is installed then installing the new filter will first uninstall the existing filter.

## 441.8 Swivel TMG Filter Installation

The following steps should be carried out on the TMG server. No configuration changes need to be performed on the Exchange server or Sharepoint server. For Additional Sharepoint configuration see the Special Considerations for Sharepoint below. To upgrade or reinstall the filter, first remove the existing Swivel TMG filter.

### 441.8.1 Publish OWA or Sharepoint

Publish Outlook Web Access, Sharepoint or your website as described in the TMG Server documentation, if you have not already done so. Ensure that they are working as expected without Swivel authentication before attempting to install the Swivel filter.

For OWA, TMG should be configured to redirect to /owa automatically, otherwise a failure in the Swivel authentication will redirect to the root path, which will give an error. This external link shows how to configure this: Setting up an OWA redirect in Forefront TMG 2010 the easy way

### 441.8.2 Configure TMG firewall rules

Create an access rule permitting HTTP access from the TMG Server to the correct port (commonly 8080) on the Swivel server. To do this, you will need to create a new protocol for outbound TCP on the appropriate port.

### 441.8.3 Install the TMG server software

NOTE: if you are installing in an Enterprise environment, you should always install on the Configuration Storage server first, and then on each array member. Be aware that the firewall service on member servers will stop when they try to synchronise with the configuration storage server, if that has the Swivel filter installed and the member does not. Once the filter is installed on the member server, you will be able to restart the firewall service.

Run PINsafeTMGFilter.exe to install the filter DLL. You will be prompted for the location in which to install the filter configuration, and also for the location of Microsoft TMG Server, usually C:\Program Files\Microsoft Forefront Threat Management Gateway.

Svivel TVG Alter Installation	and the second sec
Select destination directory	and the second
The Swivel filter will be installed to the directory shown below.	
- Cealination Gradiery Please select the location to which the Swivel filter will be installed.	
C:/Program Files/Svivel TMG Filter Bgwee	
- Microsoft Fereirent TMG Server Please geedify whare Microsoft TMG Server is installed.	
C:/Program Files/Microsoft Forefront Threat Management Gatewa Browse	
< <u>Sack</u> <u>Hext&gt;</u> <u>Cancel</u>	

Note that the installation process will include installation of Microsoft Visual C++ 2010 runtime libraries, if they are not already installed.

### 441.8.4 Register the Swivel TMG Filter

When installation is complete, you have the option to run the configuration program. Assuming you elect to do so, you will first be prompted to register the filter with TMG. You have a choice of registration types:

MiRegister Filter	←
© Register Automatically	
C Ragiatar Single Sarver	
C Register on Configuration Storage	· · · ·
C Register on Array Member	
C Register on Config. storage and Denicer	2
Ragister Cincel #	

The Automatic registration option should work in most situations. Only try the other options if automatic registration fails.

### 441.8.5 Configure the TMG filter

Configure the ISA filter using the configuration tool provided. This will optionally run immediately after installation. To start subsequently, select Start/Programs/Swivel TMG Filter/Configuration.

Svivel 14G F	itter Configuration	Same and the same same
Sarvar:	pinsaře.swiveklev.local	國和法律法法之
Port:	8080 Context: pinsafe	1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 -
🗵 Uka sam	a salitings for proxy?	
Proxy Port:	8080 Context: cinsafe	er er ha de de se
	⊠ ssi	· · · · · · · · · · · · · · ·
	Mow Self-Signed	
Sacrat:		
Confirm secret:		
Sava	Reex Cose	

#### 441.8.5.1 Swivel configuration tab

Server: is the name or IP address of the Swivel server (Hint: Use hostname to avoid problems with SSL certificates)

Port: is the port on which Tomcat is running. Swivel appliances require the use of XML authentication on port 8080 and the 8443 proxy port should not be used when integrating with TMG. (Hint: Use port 8080)

**Context**: is the name of the Swivel web application, usually ?pinsafe?. Note when using a Swivel appliance where the proxy port is available, the path Swivel using port 8080 should still be used, the TMG proxy provides security.

**Proxy port** and **Proxy context** may be required if you are using Pinpad together with an appliance that has the a proxy application that supports Pinpad, but does not have a version of Swivel that supports it directly. In this case, you should use proxy port 8443 and proxy context "proxy". You can still use these values if you are not using Pinpad, but you are using a Swivel appliance.

To clarify: the filter will use the proxy port and proxy context to retrieve TURing and Pinpad images (and message on-demand), but will use port and context to authenticate the user.

SSL: will, if checked, send requests to the Swivel server using https, rather than http. This applies to proxy as well: the current filter does not support connecting to one port on HTTP and the other on HTTPS.

Allow self-signed: when checked, causes SSL certificate errors from the Swivel server to be ignored.

Secret: is the shared secret for the Swivel agent for the ISA Server, and needs to be the same as that on the Swivel server. If you change this value, you must enter it twice to confirm the change.

#### 441.8.5.2 Authentication configuration tab



Authenticate to PINsafe (AgentXML): should be checked to use standard Swivel authentication. You should uncheck this if you are using the filter to protect a SharePoint website, as described in the ?Special Considerations for SharePoint? section below. If you uncheck it, Swivel will not directly authenticate the login request. In this case, you should enable RADIUS authentication instead.

Ignore user domain prefix: This will remove the AD domain prefix for users (anything before the '\' symbol), and when Swivel is using the SAM account name it should normally be checked. In this case, if you enter ?domain\user? as the logon username, only ?user? will be sent to Swivel. If it is not checked the prefix will be sent as part of the name to Swivel. If you use the domain prefix option in Swivel, you should uncheck this option.

Ignore user domain suffix: This will remove the AD domain suffix for users (anything after the '@' symbol). You should normally check this if you use sAMAccountName as the username for Swivel, but uncheck if you use userPrincipalName.

Allow non-PINsafe users: when checked, users not known to Swivel may authenticate using only their AD credentials. This feature is useful for transition to Swivel, where not all users have Swivel accounts. If checked, the OTC field is not shown initially, only when the username is checked and found to exist in Swivel. Note that this feature is not compatible with RADIUS authentication.

**Show TURing image**: when checked, entering a username or clicking the Start Session button on the login screen will display a TURing image for that user. It is not possible to prevent automatic display of the TURing image (i.e. only display when the button is clicked) from the configuration program, but this can be managed with a simple modification of the login page. Please contact Swivel for more information.

Show Dual Channel on-demand: when checked, a button is displayed allowing the user to request a security string via SMS or email (depending on how the strings transport is configured in Swivel). This option can be used together with the TURing or Pinpad option if required.

Show Pinpad: when checked, a Pinpad display is used to enter the one-time code. This option cannot be used with the TURing option, and requires that you have a version of Swivel or the appliance proxy that supports it.

#### 441.8.5.3 Hosts configuration tab

Swivel Authentication Applic	ations Logging	
mail.swiveklav local:443		
Add	cit Remove	
Sava	Resat Clo	33

This feature allows you to configure the filter to behave differently for different host names or ports on the TMG. It is only relevant if you are using the TMG to protect multiple websites.

If you add a new host, you will see the following form:

EditApplicat		· · · · ·
Hostname:	mail.av/iveldev.com	
Part:	443	
Sacret		
55666	<u>secrei</u>	
	🗷 Purbaolysista ka Swivet Mazari XMC)	anti anti a sana anti anti anti
	🔟 Ignore User Demain Prefix	
	📕 Igrore User Damein Suifa	fingen and an indiana
	🗹 Alow non-Swivel users	
	🗹 Shew TURing imaga	
	📕 Show Dual Channel en demand	an transfer the state of the st
ļ	Sava	
		1 A A A A A A A A A A A A A A A A A A A

Specify the host name and port that this configuration should apply to. If you leave either one blank, it will apply to all host names on a given port, or all ports for a given host name.

You can specify a different secret from the default here. This allows you to use different Agents in Swivel, so for example, restrict authentication by groups. Swivel supports multiple agents for the same server, provided that the secret is different.

The remaining options override the default options for those particular settings. In particular, if you uncheck "Authenticate to Swivel", you can specify that certain host names do not require Swivel authentication.

If a request comes in that does not match any host name/port combination in this list, the default settings will apply.

#### 441.8.5.4 Logging Configuration tab

🌐 Svivel TMG Fi	ter Configuration		
Swivel Authentice	dien Applications Loggi	M	
Logging lavel:	Warring 🔽		
	🤨 Log to Fla		
	C Use Calug Log		
Log Fle:			
C:\Lkars\P	lblic/Documents/PINsafeTi	NGFilerlog	
		Êrovise	
Save	Resat	Close	

Logging level controls how much data is logged: the levels are Debug, Info, Warning, Errors and None. The last option disables logging entirely. The most verbose level is Debug, and logs every single request received by the filter. It should only be used for troubleshooting.

You can choose to log to a file, or to a debug logger. The latter is provided for backward compatibility only ? you will need to have a debug logger installed to make use of it.

If you choose to log to a file, the default name is C:\Users\Public\Documents\PINsafeTMGFilter.log. Note that the log file does not roll over, but continues to fill up, so depending on what level of logging you use, you will need to back up or delete the log file regularly.

#### 441.8.6 Confirm that the filter has been registered correctly

Once completed the filter will appear in the ISA Server Management Web Filters section. If the filter does not appear in the list of available filters check the Windows system event log for errors.

#### 441.8.7 Modify the Listener

Modify the Listener used to publish OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, type:

?PINsafeExchange? for Outlook Web Access

and ?PINsafeISA? for Sharepoint or other websites.

Modify the properties for the relevant policy rule, then select Apply, and click OK. Then select the Application Settings tab and UNCHECK the option to use customized HTML. Note that if you have customized your original OWA or Sharepoint login pages, you will need to apply the same customisation to the new Swivel pages. Please consult Swivel support for details of this.

Once you have configured everything, restart the Microsoft Firewall Service on the TMG Server (not just activating TMG). It can take a long time to restart this service, and if you are connecting to the TMG Server via remote desktop, you may be temporarily disconnected from it.

## 441.9 SSL Certificate Considerations

There would appear to be an issue with certain security updates for TMG Server which prevents HTTP POST requests over SSL unless the target server certificate is fully trusted. This has consequences for the Swivel TMG Filter integration.

If you are not using SSL on your Swivel server, this issue will not affect you.

If you are using SSL, you must have a valid certificate on the Swivel server. This means:

- The certificate date must be current (i.e. not expired)
  The certificate must be issued by a trusted CA (see below for ways of managing this)
- The certificate subject must match the host name used by the TMG Server to connect to the Swivel server. In particular, this means that you must reference the Swivel server by name, not by IP address.

One way to manage this is to get a commercial certificate for the Swivel server. However, this costs money, and if your Swivel server is not internet facing, is not necessary. A second option is if you have an internal certificate authority, you can use that to issue a certificate for the Swivel server (Windows Servers, for example, can optionally be configured as certificate authorities). If you do this, you need to make sure that the certificate authority server certificate is added to the trusted root certificates on the TMG Server, if it is not already. The third option is simply to generate a self-signed

certificate on the Swivel server, with the correct host name, and to install that directly into the TMG Server trusted root store.

For more detail, refer to the relevant knowledgebase documentation on generating SSL certificates if you are using a Swivel appliance. Otherwise, refer to the relevant documentation for your operating system.

# 441.10 Special Considerations for Sharepoint

A security hole has been discovered when using earlier versions of the ISA filter for Sharepoint authentication. It was possible to open a Sharepoint document from within Word (for example) and only provide the standard Active Directory credentials.

The new solution avoids this problem by using RADIUS to authenticate to Swivel, rather than using the ISA filter directly. One minor inconvenience with this is that users must authenticate through the Sharepoint web page before they can access any documents.

Note that if you disable Swivel authentication for Sharepoint, it is also disabled for all other websites. Therefore, if you want to use Swivel authentication on multiple websites for a single ISA Server, they must all use the standard Swivel authentication, or all use RADIUS.

1. On the ISA filter configuration application, uncheck the Authenticate option. This means that Swivel will not authenticate the logon request directly. Instead, you should use RADIUS to perform Swivel authentication, as described below.

2. On the Authentication tab you should check the option ?Collect additional credentials in the form?. This will require you to select ?RADIUS OTP? as the authentication validation method. Click the ?Configure Validation Servers? button, and add the Swivel server as a RADIUS server. Make a note of the shared secret you set for the server.

3. In order for users to be able to open documents from other, non-browser applications once they have authenticated, you must enable persistent cookies. On the Forms tab, click the Advanced button. It is recommended that you select persistent cookies for private computers only. This means that users on public computers will have to open documents from the Sharepoint web site.

4. On the ISA server, create a rule to allow RADIUS authentication from the ISA server to the Swivel server

5. On the Swivel server, enable the RADIUS server (on the RADIUS > Server page). On the RADIUS > NAS page, add the ISA Server as a new NAS, and enter the shared secret you set on the ISA Server. If you wish to restrict access to a particular group of users, select that group, otherwise leave the Group drop-down as ?ANY?.

6. On the policy rule, on the Authentication Delegation tab, select ?NTLM Authentication?.

Once you have configured everything, reboot the ISA server.

# 441.11 Verifying Installation

### 441.11.1 Outlook Web Access

Navigate to the URL on which TMG Server publishes OWA. The customisation is visible in the addition of a One Time Code field and a Start Session button. Attempting to login with a correct username and password but no one time code should result in failure. Only when a correct Swivel one time code is entered in addition to the Exchange or Sharepoint credentials should the user be logged into OWA.

If you have enabled the option to allow non-Swivel users, then no Swivel customisation will be evident until after you enter the username and move to a different screen. The Swivel additional fields will then appear:

	anarder-starset@tawland.okBarchant.eEdgerth.advisi.are
Alf-man Re	oreginalitation and a second second
Outlook Web Ann	marker
agricar mearph	Martine and Back in the second Aller in the second
	( ) / / / / / / / / / / / / / / / / /
	and the second sec
A STATE AND A STATE AN	
Security (show applanation)	the second s
① This is a public or shared computer	
This is a private commutar	Calest were high, we will be the set of the
	articlas malatic strain
In the Orither Web Are Links	
Dise Contrack Web App Light	
Domain/user name: admin	The due to a the terms
	We want the care of the second
Password:	and share works to get a safe grap and share and share
0.7.01	weight of warming a standard and a standard
Une time Code:	
	services over as were to write a service
De Fredrik instru	and the second second
	and the second
1234557890	计中国公司 医白色
Later of Stars Produced	alter the post of the second second
· 你是这一次,你不是你了。"	and the second
Description of the second s	a the Marshall Course of the
	Level week states and
Connected to Microsoft Exchange	ACTIVITY OF CONTRACTORS AND A CONTRACTORS OF CONTRACTORS
Secured by Microsoft Forefront Threat Management Gateway © 2009 Microsoft Composition, All rights reserved	
S 2003 Photoant Carporation Ann gins reserves.	

### 441.11.2 Sharepoint

Navigate to the URL on which ISA Server publishes Sharepoint. You will notice that there are two sets of credentials to enter. The Swivel credentials are entered in the top part, and the Active Directory credentials in the lower part. Enter the username in the first box as domain/user. Click the Start Session button to get a TURing image. Enter the Swivel password and one-time code in the next two boxes. (NOTE: the Swivel password and one-time code are actually concatenated and submitted as a single value. You can, if you prefer, enter them that way in the Passcode field ? password first).

In the final box, enter your Active Directory password, and click submit.

(NOTE: you actually have to enter different usernames for Swivel and Active Directory ? with the domain prefix for AD and without for Swivel. However, this is handled automatically for you. You will notice, if you fail login, that the Swivel username has changed, and the AD username has been inserted in the lower set of credentials.)

## 441.12 Additional Options

### 441.12.1 RADIUS Authentication

Set the Swivel server as the RADIUS server (and add the ISA Server as a NAS on Swivel). If you want to use the TURing image, then the Swivel ISA filter is required, but disable authentication in the filter configuration. Swivel RADIUS custom login pages provided with the filter can be used.

### 441.12.2 Automatic sending of SMS

The login page can be configured to automatically send the user an SMS message when they have entered the username and proceed to the next field. On a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm".locate the following lines:

#### locate the following

#### function setUserExists(attribute)

Approximately 20 lines below this, you should find the following section:

```
if (btnMessage) {
    if (showMessage) {
        btnMessage.style.display = "";
    } else {
        btnMessage.style.display = "none";
    }
}
```

#### Insert a new line, as follows:

```
if (btnMessage) {
    if (showMessage) {
        btnMessage.style.display = "";
        ShowMessage();
    } else {
        btnMessage.style.display = "none";
    }
}
```

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

### 441.12.3 Removing the OTC button

If you don't want the button to appear at all, on a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm". Locate the following lines:

<input class="btn" id="btnImage" type="button" value="@@L_StartSession_Text" onclick="ShowTuring();" />

<input class="btn" id="btnMessage" type="button" value="@@L_SendMessage_Text" onclick="ShowMessage();" />

and delete them.

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

### 441.12.4 Disabling the Auto TURing feature

When a TURing image is generated it expects the user to authenticate with that image for the length of the Session Cleanup.

When using the XML authentication the automatic display of the TURing image can be prevented by editing the file: "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm". Delete the line *ShowTuring();* within the function *setUserExists(attribute)*.

### 441.13 Uninstalling

#### 441.13.1 Modify the Listener

Modify the Listener used to remove OWA or Sharepoint as follows: On the relevant firewall rule, right-click and select properties, select Listener, then click Properties. On the Forms tab, remove the tick the check box labelled ?Use customized HTML forms instead of the default?. For the form set directory, remove:

?PINsafeOWA? for Outlook Web Access

Modify the properties for the relevant policy rule.

Then select Apply, and click Ok. Then select the Application Settings tab and CHECK the option to use customized HTML.

Uninstall the Swivel software using the Remove Programs.

reboot the ISA server

## 441.14 Known Issues

### 441.15 Troubleshooting

NOTE: After any changes are made, always restart the Microsoft Firewall service

With regard to the Single Channel TURing image, the TMG server login page does not use SCImage directly: the image request comes through the filter, so that the the Swivel server does not need to be accessed directly from the internet. If the filter is not working, then no image will appear.

### 441.15.1 Filter status Check

This should be made in a web browser against the TMG login.

https://<path_to_TMG server>/PINsafeTMGFilter.dll?usepinsafe

This should return a series of 0s and 1s, Example: 10100110, the order can show the status as below:

- 1 Show one-time code field
- 2 ? Allow unknown users
- 3 ? Show TURing image
- 4 ? Show Message on demand
- 5 Show Pinpad
- 6 ? Ignore domain prefix
- 7 ? Ignore domain suffix

If it cannot contact the Swivel server, or if the filter is disabled, the first digit will be 0. NOTE: for versions of the TMG earlier than 1.4, the PINpad flag is not present.

### 441.15.2 Enabling Swivel logging

The Swivel authentication filter can optionally log its activity to a file. By default, no logging takes place, but you can enable logging by editing the filter registry key directly, using Regedit. The key to edit is

\\HKEY_LOCAL_MACHINE\Software\Swivel Secure\PINsafeTMGFilter

Create a DWORD value named "LogOptions". Set it to 2 to enable logging to a file. Set it to 1 to enable logging to the Windows debug log (see below), or 3 to enable both. Setting it to 0, or omitting it entirely, results in no logging.

The default log file is

C:\Users\Public\Documents\PINsafeTMGFilter.log

If you want to log to a different file, create a String registry value in the filter key named "LogFile", and set the value to the full path of the log file.

Older versions of the filter always log activity to the standard Windows debug log. Newer versions can optionally do this as well. This can be accessed using a tool such Sysinternals DebugView available as freeware from:

#### Sysinternals DebugView

To include logging of output from the filter the option Capture Global Win32 must be enabled in the Capture menu.

### 441.15.3 Single Channel image does not appear

- Check Swivel TMG filter settings
- Use a fully qualified hostname instead of IP address for the Swivel server
- Is an SSL connection being used
- Is a self signed cert being used, if so try without SSL using http or install a valid public certificate
- Is the certificate using the internal hostname or the external hostname? The hostname used by Swivel must match the certificate hostname.
  Check the Swivel TMG filter is correctly installed. On the TMG Server Management: under System, on the Web Filters tab, "Swivel
- Oneck the Swiver FMG filter is correctly in: Authentication Filter" should be enabled
- From the TMG server check a Single Channel image can be generated in a web browser connecting to the Swivel server using:

Swivel appliance

https://<PINsafe server IP>:8080/pinsafe/SCImage?username=test

or

https://<PINsafe server IP>:8443/proxy/SCImage?username=test

For a software only install see Software Only Installation

 If you see a red cross where the Single Channel Image should be right click on it and select properties. Copy the Address (URL) which should look something like: https://<ISA URL>/PINsafeISAFilter.dll?username=graham&random=197405. Copy this line and paste into the URL bar of the web browser and see if a Single Channel Image is generated. If a user is able to login without the One Time Code, then the TMG filter may not be installed.

If IP addresses, rather than host names is used, with SSL enabled, you must check the option to "permit self-signed certificates". This option actually means to ignore all certificate errors, as you will get when referencing a server by the IP address, rather than the name.

### 441.15.4 Page fails to display after failed login

An Access Forbidden message is displayed. After a login failure, the user is redirected to https://hostname/, rather than https://hostname/owa. You can configure the TMG firewall rule to automatically redirect to /owa. This external link shows how to configure this redirect: Setting up an OWA redirect in Forefront TMG 2010 the easy way

#### 441.15.5 Adding Swivel authentication stops other pages appearing

You can specify that PINsafe authentication only applies to certain host names, in which case the others are ignored. On the Swivel TMG filter disable Swivel authentication in the default configuration, then add an application with the host name that DOES require authentication, and set Swivel authentication ON for that one only, or if you want to be explicit, add all three host names, and disable Swivel authentication for the ones you don't want.

### 441.16 Additional Information

Information regarding the configuration of TMG Server to publish OWA or Sharepoint may be found in the TMG Server help under Firewall policy.

For assistance in Swivel installation and configuration please contact your reseller.

# 442 Microsoft UAG Integration

# 442.1 Introduction

This configuration document outlines how to integrate Swivel with Microsoft Forefront Unified Access Gateway using Active Directory authentication in addition to the Swivel authentication.

If installing Swivel on the UAG appliance it may be required to install Swivel to use a different port than the default 8080.

### 442.2 Prerequisites

Microsoft Forefront Unified Access Gateway
UAG and URL rewriting documentation
Swivel 3.x server with ChangePIN
ChangePIN configuration document
The following files are required to be uploaded to the UAG
images.asp
login.asp (Rename loginturingsms.asp as login.asp)
Portalname1postpostvalidate.inc
Token.inc
The files can be downloaded from here: UAG Files
UAG Update 1 requires a modified login page, this additional file can be downloaded here: UAG Update 1 Files
UAG SP1 through to SP4 requires modified login pages, the complete set of files can be downloaded here: UAG SP1 Files
UAG SP1 through to SP4 SMS only request button login also UAG SP1 through to SP4 TURing only request button login
RADIUS ChangePIN for UAG, backup then replace the file LoginContinue.asp

### 442.3 Baseline

Microsoft Forefront Unified Access Gateway 1.0.1101.0 Swivel 3.5

## 442.4 Architecture

The UAG makes authentication requests against the Swivel server by RADIUS or XML.

### 442.5 Installation

### 442.5.1 Configure The Swivel Server

### 442.5.1.1 Configure a RADIUS NAS entry

- 1. Ensure the RADIUS server is running on Swivel
- 2. On the Swivel administration Console select RADIUS NAS
- 3. Enter a name for the NAS
- 4. Enter the UAG internal IP address
- 5. Enter the shared secret
- 6. Click on Apply to save changes

# RADIUS>NAS 🥑

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther via the RADIUS interface.

NAS:	Identifier:	Device Name
	Hostname/IP:	192.168.0.1
	Secret:	•••••
	EAP protocol:	None
	Group:	ANY
	Authentication Mode:	All
	Change PIN warning:	No 🔻

### 442.5.1.2 Configure Single Channel Access

- 1. On the Swivel Management Console select Server/Single Channel
- 2. Ensure ?Allow session request by username? is set to YES

Server>Single Channel @	
Please specify how single channel security strir	ngs are delivered.
Image file:	turing.xml
Rotate letters:	No 💌
Allow session request by username:	Yes 💌
Only use one font per image:	Yes 💌
Jiggle characters within slot:	No 💌
Add blank trailer frame to animated images:	Yes 💌
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static 💌
Multiple AUthentications per String:	No 💌
Generate animated images:	No 💌
Random glyph order when animating:	No 💌
No. Characters Visible:	1
	Apply Reset

### 442.5.2 Configure the UAG

#### 442.5.2.1 Edit the UAG Configuration Files

Edit the file images.asp with the below URL to represent the Swivel server IP address and Swivel install name:

objWinHttp.Open "GET", "https://<hostname_of_pinsafe>:8443/proxy/SCImage?username=" & request.querystring("username"),false

Where <hostname_of_pinsafe> is your Swivel server hostname.

Then edit Token.inc with the required shared secret:

m_secret = "<secret>"

Where <secret> is your secret (do not enter the angle brackets).

#### 442.5.2.2 Copy the Configuration files

Note: Ensure any existing files are backed up first.

- 1. Copy Token.inc and Portalname1postpostvalidate.inc to: <path to UAG install>\von\InternalSite\inc\CustomUpdate
- 2. Copy login.asp file to: <path to UAG install>\von\InternalSite\CustomUpdate
- 3. Copy images.asp to: <path to UAG install>\von\InternalSite\Images\CustomUpdate

#### 442.5.2.3 Configure the TMG

Create a Threat Management Gateway rule to allow access from the UAG to the Swivel server

On the TMG configuration select New Access Rule and create a rule to allow traffic from the UAG to the Swivel server.

Port 8443 (or port 8080 for software installs, older virtual or hardware appliances and when using XML authentication)

From Local Host (i.e. the UAG)

To Swivel Server (or Internal Network)

**Outbound Traffic** 

### 442.5.2.4 Configure Login Page

Select the UAG Configuration GUI, From the Advanced Trunk Configuration select Authentication and set the Login Page to customupdate\Login.asp. This can be changed to reflect a different install location or trunk.

Application Access Portal SP URL In	ispection 🛛 🚽 Global URL Settings	
🍣 General 🕺 Authentication	Session 🥥 Applica	ition Custo
<ul> <li>Authenticate User on Session Login Select Authentication Servers:</li> <li>AD <ul> <li>Add</li> <li>Remove</li> <li>Token</li> <li>Remove</li> <li>Show Server Names</li> </ul> </li> <li>User Selects From a List of Servers <ul> <li>Show Server Names</li> </ul> </li> <li>User Must Provide Credentials for Each Selected Server</li> <li>Use the Same User Name</li> <li>Use Integrated Windows authentication <ul> <li>Enable NTLM protocol</li> <li>Enable Kerberos protocol</li> </ul> </li> <li>Enable Users to Add Credentials On-the-Fly</li> <li>Enable Users to Change Their Passwords <ul> <li>Notify User</li> <li>Days Prior to Expiration</li> </ul> </li> <li>Enable Users to Select Language</li> <li>Skip client compliance checks when accessing a SharePoint site outside of a session</li> <li>Login Page:</li> <li>Login.asp</li> <li>Permitted Authentication Attempts:</li> </ul>	Image: Construction       ✓InternalSite/LogoffMsg.at         Logoff URL:       ✓InternalSite/LogoffMsg.at         Wait       30       Sec. After Logoff URL to Terminate Session         Pass the Logoff to the Application Server       ✓         Send Logoff Response to Browser       ✓	isp isp

#### 442.5.2.5 RADIUS authentication Configuration

Swivel can be configured as the Primary authentication server or more usually is configured as a secondary authentication server. When using Swivel as a secondary authentication such as with Active Directory, ensure that the options for secondary authentication are selected.

To enable RADIUS authentication create a repository of type ?RADIUS? on the UAG configuration.

To use RADIUS do the following-

- 1. Access the UAG configuration GUI.
- 2. Click on Admin Authentication Users/Group repository
- 3. Select New to create a new repository
- 4. In the drop down menu, select ?RADIUS? and in the Name field enter Swivel RADIUS

5. Enter the IP of the Swivel server. Note, when using a Swivel HA pair, do not use the VIP address for RADIUS authentication, but use the real IP address.

- 6. Enter port 1812
- 7. If required enter a second IP/port
- 8. Enter a shared secret key of the same value as the Swivel server
- 9. Click on Add and apply this repository to the relevant trunk.
- 10. Ensure User must enter credentials for each server is selected.
- 11. If AD password is to be entered ensure that an AD authentication server is specified.
- 12. Activate the configuration
- 13. Configure Swivel as a RADIUS server



#### 442.5.2.6 Configuring the URL rewriting rules

To allow access to the images.asp

- 1. Select the required Trunk
- 2. Select Configure from the Advanced Trunk Configuration

### 3. Select the ?URL Set? Tab

4. Add a rule to permit access to the images.asp

InternalSite_Rule100

Note: This must be named InternalSite_Rule, example: InternalSite_Rule100 (use a high number to prevent it being overwritten by updates)

With parameters of:

Action: Accept

URL: /internalsite/images/customupdate/images.asp

Note: You can use /internalsite/images/customupdate/* for testing, and add additional rules to check the input.

Parameter: Handle (i.e. handle any parameters. For troubleshooting it may be useful to set this to ignore).

Method: Get

To Allow access to Swivel specific parameters:

Under Parameters select Add, add the following values:

Parameter 1:

- Name: username
  Name Type: String
  Value: ?[a-z0-9]+? (this is a basic regex and may need changing depending on the users username policy)
  Value Type: String
  Length: 1:100 (may need to up 100 depending on customer username length)
  Existence: Mandatory
  Occurrence: Single

- Occurrences: Single
- Max total length: -1
  Rejected values checking: on

Parameter 2:

- Name: random
- Name Type: String
  Value Type: Integer
- Existence: Optional
- Occurrences: Single • Max total length: -1
- · Rejected values checking: on
|                                                         |                  | Authentication                          | Session                      | la.              |             | 🥥 Appli         | cation Custo                |
|---------------------------------------------------------|------------------|-----------------------------------------|------------------------------|------------------|-------------|-----------------|-----------------------------|
| Server Name Trar                                        | nslation         | URL Inspec                              | ction                        | Global           | URL Setting | S               |                             |
| JRL List                                                |                  |                                         | _                            |                  |             |                 |                             |
| Name                                                    | Action           | URL                                     |                              | Parar            | meters      | Note            | Methods                     |
| 📄 🖌 InternalSite_Rule:                                  | 35 Accept        | /internalsite/redir                     | ecttoorigurl\.asp            | Hand             | lle         |                 | GET                         |
| 📄 🖌 InternalSite_Rule:                                  | 36 Accept        | /internalsite/win3                      | 2/java/[0-9a-z]+\.jar        | Rejec            | ct          |                 | GET                         |
| 📄 🖌 InternalSite_Rule                                   | 37 Accept        | /internalsite/scrip                     | ts/whale(j vb)sdata(         | Rejec            | ct          |                 | GET                         |
| 📄 🖌 InternalSite_Rule                                   | 38 Accept        | /internalsite/scrip                     | ts/whale(j vb)sanaliz        | Rejec            | ct          |                 | GET                         |
| 📄 🖌 InternalSite_Rule                                   | 39 Accept        | /internalsite/                          |                              | Hand             | lle         |                 | GET                         |
| 📄 🖌 InternalSite_Rule                                   | 40 Accept        | /internalsite/custo                     | omupdate/[0-9a-z_]*(         | Hand             | lle         |                 | GET                         |
| InternalSite_Rule                                       | 41 Accept        | /internalsite/on-d                      | lemandagent/.*               | Rejec            | ct          |                 | GET                         |
| InternalSite Rule                                       | 42 Accept        | /internalsite/scrip                     | ts/applicationscripts/(      | Rejec            | ct          |                 | GET                         |
| InternalSite Rule                                       | 43 Accept        | <ul> <li>/internalsite/image</li> </ul> | es/customupdate/.*           | Ignor            | re          | -               | GET                         |
| -                                                       | 1                | 25 S 000 0.000                          | (15) <u>51</u> 15) 49.       | 100              |             |                 |                             |
| I Other URLs Will Be Rejec                              | ted              | Cop                                     | y <u>P</u> aste              | Add Prim         | ary Add     | <u>E</u> xclude | <u>R</u> emove              |
| II Other URLs Will Be Rejec<br>'arameter List<br>I Name | ted<br>Name Type | Cop                                     | y <u>Paste</u>               | Add Pri <u>m</u> | ary Add     | Exclude         | Remove                      |
| II Other URLs Will Be Rejec<br>arameter List            | ted<br>Name Type | Op                                      | w <u>P</u> aste              | Add Prim         | ary Add     | <u>Exclude</u>  | <u>R</u> emove              |
| II Other URLs Will Be Rejec<br>'arameter List           | ted<br>Name Type | <u>C</u> op                             | y <u>Paste</u><br>Value Type | Add Prim         | ery Add     |                 | <u>R</u> emove<br>Existend  |
| II Other URLs Will Be Rejec<br>'arameter List<br>Name   | ted<br>Name Type | <u>C</u> op                             | w <u>Paste</u><br>Value Type | Add Prim         | ery Add     | <u>E</u> xclude | <u>R</u> emove<br>Existence |
| II Other URLs Will Be Rejec                             | ted<br>Name Type | Op<br>Value                             | y <u>Paste</u><br>Value Type | Add Prim         | ery Add     | <u>Exclude</u>  | Remove<br>Existend          |
| II Other URLs Will Be Rejec                             | ted<br>Name Type | Value<br>Value                          | vy <u>Paste</u>              | Add Prim         | e Length    | Exclude         | Remove<br>Remove            |
| Il Other URLs Will Be Rejec                             | ted<br>Name Type | Cop<br>Value                            | vy Paste                     | Add Prim         | e Add       | Exclude         | Remove                      |

Edit Rule to allow Access to the validate.asp

1. Select the validate.asp rule (Usually Internal_Rule2)

2. Under Parameters select Ignore

Alternatively add the following to the parameters list:

Turing

SMS

To Allow access to Swivel specific parameters:

Select the InternalSite_Rule2

Under Parameters select Add, add the following values:

Name: swivel

- Name Type: String
- Value:
- Value Type: String
- Length: 1:100

Existence: Optional

Occurrences: Multiple

Max total length: -1

Rejected values checking: on

Also add a Parameter with the following values:

Name: orig_url

Name Type: String

Value:

Value Type: String

Length: 1:200

Existence: Optional

Occurrences: Multiple

Max total length: -1

Rejected values checking: on

Name		Action	URL				Parame
Portal F	Rule 12	Accept	/(secure)?[^/]	+portalhomepag	e/scripts/(limitedp	oortal toolbarsc	Reject
Internal	Site Rule1	Accept	/internalsite/(o	wa/)?(customup	date/)?login\.asp		Handle
Internal	Site Rule2	Accept	▼ /internalsite/va	Handle			
Internal	Site_Rule3	Accept	/internalsite/(sessiontimeout scheduledlogoff postvalidate pas				Reject
Internal	Site_Rule4	Accept	/internalsite/setpolicy\.asp				Handle
Internal	Site_Rule5	Accept	/internalsite/validatecontinue\.asp				Handle
Internal	Site_Rule6	Accept	/internalsite/va	alidatechooseuse	r\.asp		Handle
Internal	Site_Rule7	Accept	/internalsite/cr	edentialssettings	s∖.asp		Handle
🗐 🖌 Internal	Site_Rule8	Accept	/internalsite/lo	ginchangepassw	ord\.asp		Handle
ECH tatana	Sita Dulaŭ	Accent	/internalsite/validatechangepassword\ asp				Handle
I other URLs will be	e rejected.		Conv	Pasta	Add Primary	Add Evolude	Bemove
I other URLs will be	e rejected.		Copy	<u>P</u> aste	Add Primary	Add Exclude	<u>R</u> emove
I other URLs will be arameter list Nar e	e rejected.	Value	<u>C</u> opy Value Type	<u>P</u> aste	Add Primary	Add Exclude	<u>R</u> emove es
I other URLs will be arameter list: Nar e secure	e rejected. Name Type String	Value [01]	<u>C</u> opy Value Type String	Length	Add Primary Existence Optional	Add Exclude	<u>R</u> emove es
I other URLs will be arameter list Nar e secure site_name	e rejected. Name Type String String	Value [01] [0-9a-z] +	Copy Value Type String String	Length	Add Primary Existence Optional Optional	Add Exclude Occurrence Single Single	<u>R</u> emove es
I other URLs will be arameter list: Nar e secure site_name site_redirector	Name Type String String String	Value [01] [0-9a-z]+ [^*'*`  ]*	Copy Value Type String String String String	Length 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Add Primary Existence Optional Optional Optional	Add Exclude Occurrenc Single Single Single	<u>R</u> emove es
I other URLs will be arameter list: Nar e secure site_name site_redirector swivel	e rejected. Name Type String String String String String	Value [01] [0-9a-z]+ [^*'*` ]*	Copy Value Type String String String String String	Length 1.1 1.1 1.256 ↓ 1:100	Add Primary Existence Optional Optional Optional Optional	Add Exclude Occurrenc Single Single Multiple	<u>R</u> emove es
I other URLs will be arameter list: Nar e secure site_name site_redirector swivel trusted	e rejected.          Name Type         String         String         String         String         String         String         String         String	Value [01] [0-9a-z] + [^*'*` []*	Copy Value Type String String String String String String	Length ↓1 ↓1 ↓200 0:256 ↓1:100 0:1	Add Primary Existence Optional Optional Optional Optional Optional	Add Exclude Occurrenc Single Single Single Multiple Single	<u>R</u> emove es

me		Action	- 1	LIDI				Param
Dortal Dula:	17	Accont		((cocure))[()]	Loortalbomonad	o (acrieta (/limit	adaartal Itaalbaraa	Deject
ToternalSite	Dule1	Accept		/(secure)![ /]	+por tainomepag	e/scripts/(innit date/\2login\ :	eupor tarptooloarse.	. Reject
InternalSite	_Rule1	Accept	-1	<ul> <li>Internalsite/(over)/: (customopdate)/: login (asp</li> </ul>			Handle	
TotornalSite	_Rule2	Accept	-	<ul> <li>Internalsite/validate\vasp</li> <li>Internalsite/(cossignitimeguit/scheduledlogaff/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualidate/pactualid</li></ul>			Deject	
Internaisite	_Rule3	Accept		/internalsite/(sessiontimeout scheduledlogoff postvalidate pas.		Iboarvaiidare ibas	, Rejett	
Thermalsite		Accept		/internaisite/se	tpolicy (, asp			Handle
	_Rules	Accept		/internaisite/va	lidatecontinue (	asp		Handle
	_Ruleo	Accept		/internaisite/va	lidatechooseuse	r\.asp		Handle
	_Rule7	Accept		/internalsite/cre	edentialssettings	;\.asp		Handle
InternalSite	_Rule8	Accept		/internalsite/log	ginchangepasswi	ord\.asp		Handle
IIIII InternalSite	Rule9	Accent		/internalsite/va	lidatechancenas	sword).asn		Handle
ther URLs will be reje	ected.			<u>C</u> opy	Paste	Add Pri <u>m</u> ar	y Add <u>E</u> xclude	<u>R</u> emove
ther URLs will be reje rameter list	ected.			<u>С</u> ору	Paste	Add Pri <u>m</u> ar	y Add Exclude	Remove
ther URLs will be reje ameter list 'Name	ected.	e	Value	<u>С</u> ору	Paste	Add Primar	y Add Exclude	  
ther URLs will be reje rameter list: ™Name ∭ login_type	ected. Name Typ String	e	Value [0-9]+	Сору	<u>P</u> aste	Add Primar	y Add Exclude	Remove
ther URLs will be reje ameter list Name login_type login_type	ected. Name Typ String String	e 💽	Value [0-9]+	Сору	Paste	Add Pri <u>m</u> ar	y Add Exclude Value Type String String	
ther URLs will be reje ameter list: Name login_type login_url password	ected. Name Typ String String String	e	Value [0-9]+	<u>С</u> ору	Paste	Add Pri <u>m</u> ar	y Add Exclude Value Type String String String	
ther URLs will be reje ameter list Name login_type corig_url password rds_sso	ected. Name Typ String String String String String	e	Value [0-9]+ [a-z]*	<u>C</u> opy	<u>P</u> aste	Add Pri <u>m</u> ar	y Add Exclude Value Type String String String String	     
ther URLs will be reje	ected. Name Typ String String String String String String	e	Value [0-9]+ [a-z]* [^/\/*	<u>C</u> opy	Paste	Add Pri <u>m</u> ar	y Add Exclude Value Type String String String String String String	Eemove Leng 1:2 ▼ 1:20 0:35 0:4 0:50
ther URLs will be rejet ameter list: Name login_type login_type login_type password password rds_sso repository repository resource_jd	ected. Name Typ String String String String String String String	e 💽	Value [0-9]+ [a-z]* [^/* [0-9a-2	<u>C</u> opy	Paste	Add Pri <u>m</u> ar	y Add Exclude Value Type String String String String String String String String String	Eemove Leng 1:2 ▼ 1:20 0:35 0:4 0:50 0:32
ther URLs will be reje ameter list: Name login_type login_type login_type password rds_sso rds_sso repository resource_id	ected. Name Typ String String String String String String String	e	Value [0-9]+ [a-z]* [^/*' [0-9a-2	<u>C</u> opy	Paste	Add Pri <u>m</u> ar	Value Type String String String String String String String String String	Eemove Leng 1:2 ▼ 1:20 0:35 0:4 0:50 0:32
ther URLs will be rejet ameter list: Name login_type login_type login_type password repository repository resource_id	ected. Name Typ String String String String String String String	e	Value [0-9]+ [a-z]* [^/* [0-9a-2	<u>С</u> ору "П* ]+	Paste	Add Primar	y Add Exclude Value Type String String String String String String String	Eemove Leng 1:2 ▼ 1:20 0:35 0:4 0:50 0:32

To allow access to the ChangePIN application

- Select the required Trunk
- Under Applications select Add
- Click the Web Applications Radio App and Generic Web App then Next
- Enter Application name ChangePIN and Application Type: pinsafe then Next
- Enter the ChangePIN IP address, and under path the location of the ChangePIN install (normally changepin), set the port to 8443, then Next
- Select Next
- Check details are correct, specifically https://<IP Address>:8443/changepin and then Finish

NOTE: If changing the IP address then change the IP address in the Application Properties on the Web Servers and the Portal Applications tabs.

## 442.6 Verifying the Installation

Browse to the login page, select TURing and enter a username, the Turing image should appear. Test using the SMS option. Check for requests on the Swivel server.

UAG Login Page

Log On	
User name:	
192.168.0.165 Password	t:
PINsafe Password:	
Language:	English (en-US)
	Log On
Please enter your user	mame in order to continue.

UAG login using SMS

Application and	Network Access Porta	1
SMS 🤨	Turing C	
Log On		
User name:	graham	
AD Server Password:		
PINsafe Password:	••••	
Please enter your usern This site is intended for author If you experience access prol	ame in order to continue.	

UAG login using Turing Single Channel Image

SMS C	Turing •
Log On	
User name:	graham
AD Server Password:	•••••
PINsafe Password:	••••
	Log On
	Log On
1 2 3 4 5	Log On
1 2 3 4 5	
1 2 3 4 5 4 3 9 0 B	Log On 6 7 8 9 0 2 7 5 1 6

Successful RADIUS authentication

The following user logged into trunk "test" (secure=0): User: admin; Source IP: 192.168.9.87; Authentication Server: PINsafe RADIUS; Session: B9FCC62A-B073-445D-9AAE-2FB1109EE5E6.

## 442.7 Troubleshooting

Check the Swivel server logs and system event logs for any errors or lack of communication as well as the UAG logs. Attempt a login and if required the TURing image, to generate an event then view it under under Admin/Web Monitor/Event Viewer/Security. Check the ISA server logs.

From a web browser on the UAG check to see if it is possible to generate a Turing image https://<IP address of Swivel server>:8443/proxy/SCImage?username=test

If the changes made in the UAG are not reflected in the login page, allow sufficient time for the rules to be written on the TMG (wait 10 minutes).

# Request failed, the URL contains an illegal path. Trunk: test; Secure=0; Application Name: Whale Internal Site; Application Type: InternalSite; Rule: Default rule; Source IP: 192.168.9.87; Method: GET; URL: /InternalSite/Images/customupdate/images.asp?username=admin

URL blocking by the UAG. Check that the image can be rendered and that the URL rewriting rules are correct

### The URL /internalsite/images/customupdate/images*.asp contains an illegal path. The rule applied is Default rule. The method is GET.

When the message *The rule applied is Default rule* is seen, it means that no rule has been matched and by default the URL is blocked. In the above example the path is incorrect to images.asp.

### Http 500 error

If you get an http 500 error when using xml based integration you may need to edit the token.inc file so that

Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")

Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5.1")

Ensure that the UAG can resolve the Swivel server name when hostname is used for connecting by RADIUS. Try with the IP address of the Swivel server.

## 442.8 Additional Configuration Options

### 442.8.1 RADIUS Challenge and Response

The UAG and Swivel supports the use of Challenge and Response authentication.

On the Swivel Administration Console ensure two-stage authentication is set to "Yes" for the RADIUS NAS definition. Secondly, under Server -> Dual Channel, ensure On demand authentication is set to "Yes".

In order to use two-stage authentication on Swivel, all users have to have a password defined. There are two ways to manage this: either set a password for each user under user administration, or enable the option to check password with repository (under Policy -> Password), in which case Swivel uses the AD password. Either way, you need to enter the password for Swivel as well as the AD password. (It might be possible, using the repository password option, to have a custom page that copies the AD password to the Swivel password, but this has not been tested).

If the Swivel password is entered correctly, you will be sent a security string, and a second login page will be displayed, to enter your one-time code.

#### 442.8.2 PINpad Integration

PINpad integration can be accomplished using these files, and a slight modification to the installation procedure. Please note that this zip file reflects the relative locations of the 3 files included, starting from "InternalSite". The login page goes into /InternalSite/customupdate and the other two into /InternalSite/images/customupdate.

Please ensure that you have Pinpad enabled on your Swivel virtual or hardware appliance, following the instructions here.

Use pinpad.asp instead of images.asp from the original integration, and edit this in a similar way, replacing the internal URL for the Swivel appliance. Keep everything from "/proxy/SCPinPad" as it is. You will also need to make a similar change to StartSession.asp. One important difference to recognise with this solution is that it makes a session start request explicitly. Therefore, you cannot use the /proxy application. Instead, you must use port 8080 and context /pinsafe on a virtual or hardware appliance. This also means that you must have PINsafe version 3.9.2 or later, since earlier versions do not support PINpad natively. Make sure that the firewall rule is configured appropriately. If you have an earlier version of PINsafe, either upgrade, or use this older solution. If you use the older solution, note the differences below, and ignore any references to StartSession.asp.

Use /customupdate/loginpinpad.asp as the login page.

When configuring the URL rewriting rules, you will need to include pinpad.asp and StartSession.asp in /images/CustomUpdate as accepted pages, unless you have allowed all pages in /images/CustomUpdate. Either set "ignore" for all parameters for these pages, or else permit the following parameters:

• pinpad.asp:

- sessionid (or username for the old solution)
- ♦ padno
- StartSession.asp
  - ♦ username
     ♦ random

NOTE: this login page assumes that PINsafe is the primary authentication. If it is the secondary, you need to edit the login page (loginpinpad.asp) and change the following line

var PINSAFE_PASSWORD_INDEX = 0;

to this:

var PINSAFE_PASSWORD_INDEX = 1;

### 442.8.3 ChangePINpad Integration

When publishing access to ChangePINpad, ensure that you enable the following paths during creation:

Application Propert	ties (pinsafe)	×
Heb Ser Download/U General Address type: Addresses:	Endpoint Policy Settings      ver Security     Portal Link     Security     Ortal Link     Security     Web Settings     Authorization     Ore Settings     Subnet     Regular expression	
Paths: HTTP ports:	/changepin /proxy	
HTTPS ports:	8443	
☐ Add the def	ault port to the host	
O Help	OK Cancel	

This should in turn create the following rules:

pinsafe_Rule1	Accept 🗾	/changepin(/.* \$)	Ignore 🔽	POST, GET
pinsafe_Rule1_Proxy	Accept	/proxy(/.* \$)	Ignore	POST, GET

Beware that if you add paths to the published application afterwards, the rules for these paths will not be created. So ensure that you enter the paths at creation time.

### 442.8.4 Button size and aspect ratio

The Button size and aspect ratio is controlled by the settings in the login page:

document.all.otp.innerHTML = '<img src="/InternalSite/customupdate/FetchTuring.asp? username=' + otpusername +'" height="81" width="300">'; }

change the height and width settings to the value that is appropriate.

### 442.8.5 XML Authentication

Configuring XML authentication (when not using RADIUS)

XML authentication has not been tested with the current version of UAG and is supplied for reference if required, RADIUS authentication is the preferred method of authentication.

Note that when using a Swivel virtual or hardware appliance with a proxy configured, the XML requests need to be made to the https://<IP>:8080/pinsafe address rather than the proxy address. This applies currently to all Swivel virtual or hardware appliance versions.

This step is not required when RADIUS authentication is used. RADIUS authentication is the preferred method of authentication. To enable the token.inc file, create a repository of type ?Other? on the UAG configuration. The repository you create must match the name of the file (ie, if the inc file is called Token.inc, the repository must be named Token).

Configure a Swivel Agent (For XML Authentication)

- 1. On the Swivel Administration Console select Server/Agent
- 2. Enter a name for the Agent
- 3. Enter the UAG internal IP address
- 4. Enter the shared secret
- 5. Click on Apply to save changes

Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	•••••	
	Group:	ANY	
	Authentication Modes:	ALL	Delete
	Name:	IIS	
	Name: Hostname/IP:	IIS 192.168.1.1	
	Name: Hostname/IP: Shared secret:	IIS 192.168.1.1	
	Name: Hostname/IP: Shared secret: Group:	IIS 192.168.1.1 ANY	

To create the repository, do the following-

- 1. Access the UAG configuration GUI.
- 2. Click on Admin Authentication Users/Group repository
- 3. Select New to create a new repository
- 4. In the drop down menu, select ?Other? and in the Name field type in the name of the inc file (See screen shot below)
- 5. Click on Add and apply this repository to the relevant trunk.
- 6. Activate the configuration

Edit the file Token.inc with the required shared secret and to represent the Swivel server IP address and Swivel install name, Note for all Swivel installs this needs to point to the PINsafe server on port 8080 and not the proxy port 8443.

m_secret = "secret"
objWinHttp.Open "GET", "https://192.168.1.1:8080/pinsafe/AgentXML?xml=" & m_request, false

Note If you get an http 500 error when using xml based integration you may need to edit the token.inc file so that

Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")

is replaced with

Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5.1")

Edit the file Portalname1postpostvalidate.inc to represent the PINsafe server IP address and changePIN install name:

```
'response.redirect "https://192.168.1.1:8443/changepin"
g_orig_url = "https://192.168.1.1:8443/changepin"
```

Add Serve	r				×
Type: Name:	🔔 Ot	her			
C Use a	a Different It Server	Server for Built-In L	User/Grou Isers/Grou	up Authoriz ups	ation
Help			A	dd	Cancel

## 442.9 Known Issues and Limitations

If upgrading the UAG to a higher service pack, the configuration files, particularly login.asp may be overwritten. Verify the files after an upgrade. Also note that the URL rewriting rules may differ from version to version, so these should also be verified.

Upgrading from RTM Update 2, to SP1 will cause the InternalSite rules, on the UAG to be removed, or changed back to defaults.

If the login page is viewed incorrectly as a mobile page then this workaround will allow the correct page to be displayed, and works with Windows 7 and Windows 8.

## 442.10 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

# 443 Microsoft Windows Credential Provider Integration (Legacy OS)

# 444 Introduction

Microsoft Windows Credential Provider is used in the desktop operating systems Windows Vista, 7, 8 and 8.1, and in the server operating systems Windows Server 2008 and 2012, including Remote Desktop Gateway. For newer operating systems (Windows Vista and Server 2012 R2 onwards), see Windows Credential Provider. For integration with the older Windows GINA used in Windows 2000, 2003 and XP see Microsoft Windows GINA login.

Users can authenticate using the Swivel Credential Provider allowing 2FA (Two Factor Authentication), or strong authentication at the Windows Logon. Offline authentication is also supported for single Channel authentication, following at least one successful authentication against the Swivel server with Third Party Authentication configured.

For new features in recent releases of the Credential Provider, see below.

## 444.1 Swivel Credential Provider FAQ

Q). Does the Credential provider support offline authentication? A). Offline authentication is permissible for Swivel users who have previously authenticated to the device. Offline local authentication is always single channel, even if single channel is normally disabled.

Q). Do all users have to authenticate using Swivel? A). Swivel does have the option to Allow Unknown Users, users known to Swivel will be prompted for authentication in this instance.

Q). Is it possible to define users who do not have Swivel authentication? A). Only by using the Allow Unknown Users for non Swivel user authentication.

Q). Is it possible to login without AD password, A). No the AD password is required.

# **445 Prerequisites**

Swivel 3.x Server

Connectivity to Swivel server during installation (with Third Party Authentication for GINA enabled)

Microsoft Windows Vista, 7 or 8 (including 8.1); Microsoft Windows 2008 or 2012 Server (including R2).

Microsoft.Net Framework version 4.

Swivel Windows Credential Provider 64 bit (version 4.6) or

Swivel Windows Credential Provider 32 bit (version 4.6) or

Both of the above files in a single zip

Documentation only

A separate Swivel Credential Provider license is not required, but the users authenticating to Swivel must be licensed.

User with AD account and valid password.

# 446 Baseline

Swivel 3.7 Windows 7, Windows 2008 Server R2

# 447 Architecture

Swivel is installed as a Windows Credential Provider, and when a Windows login is made, AD username and password is checked against AD and the username and Swivel OTC is sent to the Swivel server using XML authentication, or locally if offline authentication is enabled.

## 447.1 Offline Authentication

Swivel allows offline authentication using single channel but not dual channel authentication. For offline authentication the user attempting to authenticate must have made at least one successful authentication against the Swivel server while Offline Authentication has been enabled. Swivel caches a limited number of strings for authentication, and cycles through these so there is no limit on the number of authentications which can be made. Swivel Account lockout is disabled for Swivel offline authentication. ChangePIN will not function when the Swivel server is not contactable. Local authentication is always single channel, even if single channel is normally disabled.

# 448 Swivel Integration Configuration

## 448.1 Configure a Swivel Agent

- 1. On the Swivel Management Console select Server/Agent
- 2. Enter a name for the Agent

3. Enter the Credential Provider IP address. You can limit the Agent IP to an IP address range like: 192.168.0.0/255.255.0.0 where the mask of 255 requires an exact match and 0 allows any value, so the previous example would allow any Agent in the range 192.168, or you can use an individual IP address for the Credential Provider.

- 4. Enter the shared secret used above on the Credential Provider
- 5. Enter a group, (Note in this instance ANY is not a valid group and will cause authentication to fail)
- 6. Click on Apply to save changes

Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	•••••	
	Group:	ANY	
	Authentication Modes:	ALL	Delete
	Name:	IIS	
	Hostname/IP:	192.168.1.1	
	Shared secret:	•••••	
	Group:	ANY	
l	Authentication Modes:	ALL	Delete

Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

## 448.2 Configure Single Channel Access

- 1. On the Swivel Management Console select Server/Single Channel
- 2. Ensure ?Allow session request by username? is set to YES

Server>Single Channel @	
Please specify how single channel security strin	gs are delivered.
Image file:	turing.xml
Rotate letters:	No 💌
Allow session request by username:	Yes 💌
Only use one font per image:	Yes 💌
Jiggle characters within slot:	No 💌
Add blank trailer frame to animated images:	Yes 💌
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static 💌
Multiple AUthentications per String:	No 💌
Generate animated images:	No 💌
Random glyph order when animating:	No 💌
No. Characters Visible:	1
	Apply Reset

## 448.3 Create a Third Party Authentication

If offline authentication is to be allowed, a third party authentication must be created with an Identifier of WindowsGINA. (Even though the GINA is not part of Credential Provider the third party authentication module is still used and must be configured)

- 1. On the Swivel Management Console select Server/Third Party Authentication
- 2. For the Identifier Name enter: WindowsGINA (Even though the GINA is not used, this must be entered as WindowsGINA)
- 3. For the Class enter: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA
- 4. For the License Key, leave this empty as it is not required
- 5. For the Group select a group of users (Note: the option Any cannot be selected)
- 6. Click Apply to save the settings

To allow offline authentication to be made a successful authentication must be made with the third party authentication in place.

Identifier:	WindowsGINA	
Class:	com.swiveltechnologies.pinsafe.server.thirdpar	ty.WindowsGINA
License key:		
Group:	PINsafeUsers 👻	

# 449 Microsoft Windows Swivel Credential Provider Installation

The Credential Provider is provided as a Microsoft Installer .msi file. You must run this as an administrator.

Ensure that the correct Swivel Windows Credential Provider is used: SwivelCredentialProvider_x86.msi for 32-bit or SwivelCredentialProvider_x64.msi for 64-bit.

Double-click the .msi file to run it. Alternatively, you can install from the command line, using the msiexec command.

The first page is the licence agreement:



Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

When the install has completed, the following dialog is shown:

🙀 Swivel Credential Provider	Setup	
	Completed the Swivel Credential Provider Setup Wizard Click the Finish button to exit the Setup Wizard.	
	📝 Launch the configuration program	
	Back Finish Cancel	

Ensure that the tick box is checked for Launch the configuration program to configure the Swivel instance then click on Finish.

# 449.1 Windows Swivel Credential Provider configuration

<u>S</u> ettings <u>H</u> e	lp	
Server Settings Server: Port: Context: Secret: Confirm Secret:	pinsafe.swiveldev.local 8080 pinsafe •••••	Authentication Options
SSL Use SSL [ Authentication M Aways	Accept self-signed SSL certificates	Allow Unknown Users Offline Require for Unlock Screen Require for Credential UI If Swivel Server unavailable:
<ul> <li>Swivel auther</li> <li>Remote Only</li> <li>Swivel auther</li> <li>Never</li> <li>Swivel auther</li> </ul>	ntication is applied to both local and remote logins. Intication is applied to remote logins only. Intication is never applied.	<ul> <li>Fail authentication</li> <li>Use standard authentication</li> <li>Use offline authentication</li> <li>Always use offline auth.</li> </ul>

The following options are available:

Server: The Swivel virtual or hardware appliance or server IP or hostname. To add resilience for use the VIP on a swivel virtual or hardware appliance, see VIP on PINsafe Appliances

NOTE: it has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name in this section.

Port: The Swivel virtual or hardware appliance or server port

Context: The Swivel virtual or hardware appliance or server installation instance

Secret: and Confirm Secret: A shared secret which must be entered onto the Swivel virtual or hardware appliance or server

Use SSL The Swivel server or virtual or hardware appliance uses SSL communications

Accept self signed SSL certificates Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts).

Authentication Mode, Always Swivel authentication is required for remote and local logins

Authentication Mode, Remote Only Swivel authentication is required for remote logins only

Authentication Mode, Never Swivel authentication is not used

Show TURing images Show TURing images if requested

Show Request String Show the Request string image to allow the user to obtain a new security string by dual channel

Test Mode With test mode the user can switch user to a standard authentication, see below

Ignore Domain Swivel will remove any domain prefix (domain\username) or suffix (username@domain) before matching username. This does not affect Windows authentication usernames.

Allow Unknown Users Online If the username is not recognized by Swivel, the user can authenticate using Windows credentials only. Any Swivel OTC entered will be ignored. If the user is known then they must authenticate using Swivel authentication.

Allow Unknown Users Offline If offline authentication is used, users that do not have credentials cached locally can authenticate using Windows credentials only. Any OTC entered will be ignored. If the user has previously authenticated in online mode, then they must enter the correct one-time code.

If Swivel unavailable, Fail authentication If the Swivel server cannot be contacted then authentication will fail

If Swivel unavailable, Use standard authentication If the Swivel server is unavailable use standard authentication, the OTC field is displayed but ignored.

If Swivel unavailable, Use offline authentication If the Swivel server cannot be contacted a locally generated Turing image can be used for authentication. If this option is enabled, users will be able to force offline mode using a checkbox on the login dialog.

Always use local auth A local Turing image is always used and the Swivel server is not contacted. All users must previously have authenticated using online authentication (unless the option "Allow unknown users offline" is enabled).

The remaining options are available from the Settings menu:

ungs neip	
Export Settings Ctrl+E	Authentication (
Import Settings Ctrl+I	Show TUR
Test Connection Ctrl+T	Show Peg.
Save Ctrl+S	Test Node
Save & Exit Alt+F4	🛃 Ignore Dan
Evit Chrla.Ed	Alow Ucke

Export Settings Export settings as an XML file. These can be used to import settings elsewhere.

Import Settings Import settings from an XML file exported elsewhere.

Test Connection Tests link to Swivel server:

A correct configuration should produce a dialogue box with Swivel Connection settings are correct.



Incorrect settings will produce a dialogue box with Either the Swivel agent has not been defined, or the secret is wrong



Save Save the current settings.

Save and Exit Save the current settings and close the program.

Exit Close the program without saving the settings. You will be prompted to confirm if any settings have been changed.

## 449.2 Additional Installation Options

### 449.2.1 Manually configuring the Swivel Login

### NOTE: It is recommended to use the Swivel Login Configuration Tool where possible.

If it is not possible to use the configuration utility the Swivel Login settings may be edited manually in the registry. The following values found within the "HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\Swivel Credential Provider" key are used by the Login:

PINsafeServer - The name or IP of the Swivel server PINsafePort - The Swivel server port PINsafeContext - The Swivel server context PINsafeSecret - The Swivel agent secret PINsafeProtocol - 1 for https, 0 for http PINsafeAllowSelfCert - 1 to allow SSL requests to a Swivel server with certificate errors, 0 not to PINsafeLoginSelect - determines when Swivel authentication is required: always, remote or disabled. PINsafeShowTURing - 1 to show the TURing request link, 0 not to PINsafeRequestString - 1 to show the request string link, 0 not to PINsafeAllowDefaultLogin - 1 to allow default login if Swivel unavailable, 0 not to PINsafeUseLocalAuth - When to use local TURing authentication: always, fallback or never. PINsafeDisableFilter - 1 to enable test mode. 0 to hide the standard authentication option PINsafeAllowUnknownUsers - 1 to allow unknown users in online mode PINsafeAllowUnknownOffline - 1 to allow unknown users in offline mode PINsafeIgnoreDomain - 1 to ignore the domain prefix when checking Swivel users The following values may be seen in this registry key also, but should not be changed: **PINsafeBackgroundsFolder PINsafeFontsFolder PINsafeResourceDLL PINsafeHelpUrl** Directory Uninstaller Version

### 449.3 Test Mode

In Test Mode the Windows Credential Provider has an additional login that can be used as a standard user login. In test mode the last successful login will be selected for login.



The Swivel credentials will always be on the left, the standard credentials on the right.

## 449.4 Importing Configurations

You can import credentials exported from other installations using the Import Settings menu item. Alternatively, if you need to install the Credential Provider on a large number of machines, you can modify the .msi file and replace the blank LoginSettings.xml file included with your own custom version. If you do not have the ability to modify MSI files, you can email your settings to support@swivelsecure.com and request a custom build.

# 450 Verifying the Installation

At the windows login a password and OTC login field should be available with Request Image and Request String options available.



If a Dual Channel login is made then the user should be able to enter their OTC. Note the Get Image should not be pressed, otherwise the log will be expecting a Single Channel login for the length of the session timeout (default 2 minutes).



Selecting the Request Image button should generate a Single channel Image for authentication. The Swivel log should show a session request message: Session started for user: username.



A successful login should appear in the Swivel log: Login successful for user: username

A failed login should not allow a login, and the following message should be displayed in the Swivel log: Login failed for user: username

# 451 ChangePIN

A user is usually able to change the password by using the Ctrl-Alt-Del keys (CTL-Alt-End for remote sessions). With the Windows Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the Other Credentials. This will not function for Offline authentication.

With Swivel authentication a user never changes enters PIN and this is true for ChangePIN. A user enters their current OTC, and then enters an OTC for what they wish their new PIN to be. PIN enforcement may be in place to the Swivel server to prevent the choosing of poor PIN numbers.

A user may use a single channel image or a dual channel security string to change their PIN.

Username
Old OTC
New OTC
Confirm New OTC
Request Image Request String
Other Credentials Cancel
Windows Server 2008 Standard

A successful Change PIN will show the message Your PIN was changed successfully

PINsafe Change PIN	<
Your PIN was changed successfully	
ОК	]
Administrator	
••••	
••••	
••••	7
Request Image Request String	
Other Credentials Cancel	
Windows Server 2008 Standard	

The Swivel server will also display in the logs a changePIN message Change PIN successful for user: username

# 452 Uninstalling the Swivel Integration

Use the Uninstall option from the Program menu, right click on the Windows Credentials provider and click on Uninstall. Note that uninstalling and reinstalling the Credential Provider will remove the settings, so if you need to reinstall at any point, make sure you have an exported settings file saved.

# 453 Troubleshooting

Test Mode enables you to login using the Standard Windows authentication and not Swivel authentication. If you disable Test Mode the additional logon users disappear and the machine will then be purely using Swivel.

If there is a problem then use Windows Safe Mode to login and enable Test Mode again. Safe Mode uses Standard Windows authentication.

#### Pressing Ctrl+Alt+Del reverts user back to login screen

A normal login may be attempted after a short period. This can occur as the Windows login screen may appear before a network connection has been made during boot. To prevent the login screen from not being accessible, enable the option in group policy to Wait until network is ready before user logon.

#### User must select the back button and select Other User to logon

This occurs when the system is running in Test mode. Disable the Test mode to allow normal login.

#### Change Pin is displayed instead of the logon screen

This has been seen on Dell laptops that have the Dell Control Point Security Manager installed. Remove this prior to the Windows Swivel Credential Provider installation.

#### FLUSHING_IMAGE_CACHE, ClientAbortException: java.net.SocketException: Connection reset

This error message can be seen in the Swivel log when a Windows login is attempting to use an animated gif. Turn off animated gifs and switch to 'Static', on Swivel - This is set under Server > Single Channel > Image Rendering.

#### Double User Entry at login, enforced test mode when test mode is disabled

Some fingerprint scanning software may cause this issue, this has been seen on an IBM Thinkpad. Check in the registry under the following

\\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters

look for keys which have values of: Fingerprint Logon Credential Provider Filter

and

\\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers

look for keys which have values of: Fingerprint Logon Credential Provider

To test if these are the cause, on a test system, either remove the fingerprint software (disabling may still leave the registry keys) or backup the keys by exporting them, then remove them.

## 453.1 Disabling the Swivel Login

If the Swivel Login fails to load correctly it can be disabled using the following process:

Using the F8 boot menu start Windows in safe mode

Either run the Swivel Login Configuration and edit the settings or

Using regedit.exe remove the "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowNT\CurrentVersion\WinLogon\ginadll" registry value

**Reboot Windows** 

Following this process the standard Windows Login should be restored allowing access.

### 453.2 Error Messages

#### Unable to contact PINsafe server

Version 4.x only supports TLSv1 which means if you are running a version 3 Appliance, you must enable TLSv1 under Tomcat > SSL Protocols > Enable TLS1.0.



#### Wrong Parameter or Parameter is incorrect

This message is displayed at the Windows login and can have several causes, check the Swivel logs for errors:

- The user must exist in AD and Swivel
- When an incorrect OTC is entered, when using local authentication. Unfortunately, local authentication will not work with the "Connect To" dialog. However, you should still get the remote desktop login displayed, and will be able to authenticate to this.
- The user account is locked in Swivel
- The Swivel Sever Agent has not been configured correctly

#### Please enter a one-time code first

OTC miss	ing 🔀
	Please enter a one-time code first
	ОК

A One Time Code was not entered in the OTC field during login.

### Either the Swivel agent has not been defined, or the shared secret is wrong



### AgentXML request failed, error: The agent is not authorised to access the server.

The credential Provider is not permitted to connect to the Swivel server. Add an Agent for communication.

The user name or password is incorrect.



**Check Password with Repository**: If this setting is enabled against the Agent, then you should disable it to prevent it attempting to check for a password against the repository. This is a potential cause when receiving "The user name or password is incorrect".

# AgentXML request failed, error: No suitable authentication method for the user "Administrator" was found. The user may be missing from the user repository or a synchronisation has not yet occurred.

The user Administrator is not defined as a Swivel user

#### Session start failed for user: x, error: No Data for user was found. or error: No data for the user was found

The requested user does not exist in the database. If the user does exist in the repository (e.g. Active Directory) then Swivel needs to sync with that repository.

#### Dual channel message request failed, error: On-demand dual channel delivery is disabled.

A dual channel message request was made but the On-demand delivery is not enabled. If it should be enabled, on the Swivel Administration console select Server/Dual Channel, then set On-demand delivery to Yes.

#### AgentXML request contained third party data for a third party class that does not exist. Third Party Class ID: WindowsGINA.

and

#### error: The third party class could not be found.

The Third Party Authentication class does not exist or has been created incorrectly. Create the class, see Create a Third Party Authentication

#### The third party class could not be found

This error can also be created when the Swivel Administration console Server/Agents, Group is set to Any. A group should be specified.

#### Failed to change PIN. Please check your credentials and try again.

PINsafe C	hange PIN	×
8	Failed to change PIN. Please check your credentials and try again.	
	OK	

The user has failed to change the PIN number. This could occur if the Swivel server cannot be contacted.

Unhandled exception has occurred in your application. If you click Continue the application will ignore this error and attempt to continue. If you click Quit, the application will close immediately.

The remote Server returned an error: (502) Bad Gateway.



This error has been seen when a Test Connection is made from the Credential Provider and can be caused by being unable to connect to the Swivel server. Check for network settings such as proxy settings on the local server, and if an SSL connection is required.

# **454 Release Notes**

## 454.1 Release of Version 4.6

4.6.2.1. released 27th June 2016.

The main change in version 4.6 is that there is better support for offline authentication: it has been observed in previous versions that the strings ran out after a number of offline authentications. This has now been resolved.

There is a known issue with version 4.6, in that it requires Microsoft Update KB2999226 to have been applied. This should be applied automatically by Windows Update, but if you have a problem installing or running the program, check that this update has been applied.

## 454.2 Release of Version 4.5

4.5.4.1, released 4th February 2015.

Version 4.5 includes the following fixes and enhancements over previous versions:

- Swivel authentication is optionally applied to the Unlock screen as well as the login screen
- Swivel authentication may be disabled (and by default is disabled) when connecting to remote computers
- The image window resizes dynamically depending on the type of image. The scale option is on the Settings drop-down menu.

### 454.3 Release of Version 4.4

Version 4.4 includes the following fixes and enhancements over the previous releases:

- It is fully-compatible with Windows 8 and Windows 2012 Server.
- It switches to single-channel mode if local authentication is enabled and the Swivel server is not available.
- Unlike the previous beta, version 4.3, this version is compatible with ALL Windows Operating Systems from Windows Vista onwards.
- If the user's password has expired, they are correctly redirected to the change password page.
- A problem which occasionally caused crashes when entering the username has now been resolved.
- You can now import settings exported from other installations.
  The installer is now a standard Windows MSI file. This makes it possible to customise the installation to contain your company's settings file, if you have the tools to modify MSI files. Alternatively, you can send your exported settings to support@swivelsecure.com, who can create a custom installer for your organisation.

# 455 Known Issues and Limitations

This version of the Swivel Credential Provider is not compatible with the Swivel version 3 appliance. An update will be available shortly.

The Swivel Windows Credential Provider does not support the use of

- Pinpad
- Animated gifs

for Single Channel authentication.

It has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name for the Swivel server.

Local authentication only works in single channel mode: the dual channel strings are not available offline. To use offline authentication, TURing image display must be enabled, even if normal authentication is dual channel.

If a Swivel server has been configured with a Single Channel login configuration that is not viewable, the following options are available to recover access:

- Login using dual channel
- Login using an image generated elsewhere such as on the Swivel Administration console or Taskbar on another server
- Alter the settings on the Swivel server to serve a permitted image
- Login offline if permitted
- Login to safe mode as described elsewhere

In Windows 8 and Windows Server 2012, the Credential Provider appears as a single key icon, which you must select before logging on. In some cases, where Windows should show the last used credential, you will need to click the back arrow and then select the Credential Provider. A similar problem occurs with the Unlock screen. An updated version, specific to Windows 8 and Windows Server 2012, will be released in due course.

By default, the credential provider assumes that administrator is the local administrator, rather than the domain administrator, so you have to explicitly state the domain name to logon as domain administrator. This is a feature of the default credential provider as well.

In the Swivel administration console, the Windows GINA menu item is present, but there are no configurable options, so is not selectable.
## **457 Introduction**

Built on Windows Server 2008 R2, Windows SBS 2011 Standard includes Microsoft Exchange Server 2010 SP1, Microsoft SharePoint Foundation 2010 and Windows Software Update Services.

This configuration document outlines how to integrate Swivel with Microsoft Small Business Server 2011 authentication in addition to the Swivel authentication.

# **458 Prerequisites**

Microsoft Small Business Server 2011

Swivel 3.x server

Swivel Small Business Software.

# 459 Baseline

Swivel 3.9

## 460 Architecture

The SBS makes authentication requests against the Swivel server by XML.

## 461 Installation

### 461.1 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

- 1. On the Swivel Management Console select Server/Agent
- 2. Enter a name for the Agent
- 3. Enter the Exchange IP address
- 4. Enter the shared secret used above on the SBS
- 5. Click on Apply to save changes

Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	•••••	
	Group:	ANY	
	Authentication Modes:	ALL 💌	Delete
	Name:	IIS	
	Name: Hostname/IP:	IIS 192.168.1.1	
	Name: Hostname/IP: Shared secret:	IIS 192.168.1.1	_
	Name: Hostname/IP: Shared secret: Group:	IIS 192.168.1.1 ANY	

#### **Configure Single Channel Access**

- 1. On the Swivel Management Console select Server/Single Channel
- 2. Ensure ?Allow session request by username? is set to YES

Server>Single Channel @	
Please specify how single channel security string	gs are delivered.
Image file:	turing.xml 💌
Rotate letters:	No
Allow session request by username:	Yes
Only use one font per image:	Yes 💌
Jiggle characters within slot:	No 💌
Add blank trailer frame to animated images:	Yes
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static 💌
Multiple AUthentications per String:	No 💌
Generate animated images:	No 💌
Random glyph order when animating:	No 💌
No. Characters Visible:	1
	Apply Reset

### 461.2 Configure the SBS 2011

1. Extract the files from the zip folder

2. Copy all the DLLs from the Bin folder to the Bin folder of the SBS application (by default C:\Program Files\Windows Small Business Server\Bin\WebApp\RemoteAccess).

3. Copy pinsafe_image.aspx from the AccountPage folder of the zip to the AccountPage folder of the SBS application.

4. Backup the existing SBS server Logon.aspx. Modify the existing Logon.aspx on the SBS server by locating the relevant sections in the customised Swivel Logon.aspx and copying to the SBS server Logon.aspx. Search for "Swivel Customisation Start". There are three separate sections. Copy each section into the existing Logon.aspx file (the end of the section is marked by "Swivel Customisation End"). It should be clear from the original file where the sections should go.

5. Backup the existing SBS server web.config. Modify the existing web.config on the SBS server by locating the relevant sections in the customised Swivel web.config and copying to the SBS server web.config. There are three sections to change, marked as before. The first one adds the Swivel filter as a HTTP module. The second adds an exclusion to default authorization, so that the TURing image can be displayed without having to authenticate. The third is the list of settings for the PINsafe server. You may find you have to create the <appSettings> section as well as inserting the settings, or you may find that there is a single, empty <appSettings /> entry. In the latter case, replace that with the entire <appSettings> section in the custom file. You will need to change the value="" entries to match the PINsafe settings for your local environment.

6. Finally, restart IIS (this may not be strictly necessary, but it's always best to make sure).

# 462 Verifying the Installation

# 463 Troubleshooting

# 464 Additional Configuration Options

# 465 Known Issues and Limitations

# 466 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

# 467 Netgear

## **468 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.

# 469 Baseline

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

## 470 PINsafe configuration

### 470.1 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

RADIUS>Server	0
Please enter the details for the	he RADIUS server.
Server enabled:	Yes
IP address:	0.0.0.0
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No 💌
Filter ID:	No 💌
Additional RADIUS logging:	Both 💌
Enable debug:	Yes 💌
Radius Groups:	Yes 💌
Radius Group Keyword:	POLICY
	Apply Reset

#### 470.1.1 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.

# RADIUS>NAS 🥑

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther via the RADIUS interface.

NAS:	Identifier:	Device Name
	Hostname/IP:	192.168.0.1
	Secret:	•••••
	EAP protocol:	None
	Group:	ANY
	Authentication Mode:	All
	Change PIN warning:	No 💌
		Apply Reset

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.

#### 470.1.2 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

#### 470.1.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

## **471 Netgear Configuration**

### 471.1 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.

### 471.2 Single Channel TURing Integration

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

#### 471.2.1 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

#### 471.2.2 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>
<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

F		GEAR PROSAFE		NETGEAR ProSafe VPN Fire	Usa wall FV	er Po <b> 53</b> 3
Ne	twork (	Configuration   Security   VPN   Users   Adm	inisti	ration   Monitoring   Web Su	pport	Lo
		:: IPSec VPN :: SSL VPN :: Certifica	ates	Connection Status		
Po	licies	Resources Portal Layouts SSL VPN Client Port	Forw	arding		
		Operation succ	eede	ed.		
	List of	Layouts				(?
	Layout Name	Description	Use Count	Portal URL t	A	ction
	SSL- VPN*		1	https://192.168.1.1/portal/SSL- VPN	🥟 edit	۰ 🛞
		<pre><img id="t"/> <script></script></pre>				

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.



### NETGEAR ProSafe VPN Firewall FVS33



### 471.3 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

### 471.4 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">
<iscript>
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>
```

# 472 Netilla Integration

Netilla Integration Guide

# **473 Nortel VPN Integration**

Nortel VPN Gateway

Integration Guide

Version 1.0 March 2009

## **474 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.

## **475 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.

Managing: SSL-7.1.1.0 on 3050		Tue, Mar 31, 2009 3:07:46 PM	Logged as 🔹 🔢
VPN Gateways » VPN	2 » Auth Server-2 »	General	
Authentication Ser	vers		
0 -1 -1 N 0 41 41 41 -			
Add New Authenticatio	n Server		
VPN:	2		
Auth Id:	1 💌		
Name:	PINSAFE		
Display Name:	PINSAFE		
Domain Name:			
Mechanism:	radius 🔽		
		Upt	late Back

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.

Managing: SSL-7.1.1.0 on 3050		Tue, Mar 31, 2009 3:15:23 PM	Logged as	E
VPN Gateways » VPN	-2 » Auth Server-2	[RADIUS] » Add/Modify Server		
RADIUS Servers				
	ar			
Add New RADIOS Serv				
VPN:	2			
Auth Id:	2			
IP Address:	192.168.50.50	(format: 10.10.1.75)		
Port:	1812			
Shared Secret:	•••••			
Shared Secret (again):	•••••			
		Up	date Back	)

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.

## **476 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.

VPN Gateways » VPN-2 » Login Page		Tue, Ma	ar 31, 2009 3:43:	47 PM Logged	as es
Portal Login Page					
Lets you specify a custom text to be displayed on	the Portal Login page, a	as an ordinary text str	ing or as HTM	L code 🝳	
General White-lists Black-lists Present	tation <b>Login Page</b>	Custom Content	Full Access	Language	
Please enter text in the box below:					
kinput type=button name=btnTuring	g value=Turing on	nclick=ShowTur:	ing()> 🔺		
<img id="turing" style="visibility:&lt;/td&gt;&lt;td&gt;hidden"/>		-			
<script language="JavaScript"></script>					

#### 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 t = dilength - 1;
d(3)_innerHTML = '<input name="user" id="user" size="20" type="text" onblur = "ShowTuring()">';
var t = dilength - 1;
var t = document.getElementById("ptext");
if(ppText = document.getElementById("turing");
var use = document.getElementById("turing");
var use = document.getElementById("turing");
var use = document.getElementById("ser").insafe/SCImage?username=";
if (user=") {
    alert ("Please enter your username first!");
    document.getElementById("ser").focus();
    }
}else{
    //Set the image SRC and make it visible
    var t = document.getElementById('f');
    var d = 1.getElementById('f');
    var d = 1.getElementById('f');
    ing.src = ingUrl + user + "random=" + Math.ceil(10000*Math.random());
    ing.sryle.visibility = "visible";
    }
}
```

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.

Login Status:	not logged in
Username:	trainee1
	1 2 3 4 5 6 7 8 9 0
	HZLYTEUWSA
	* Case sensitive
Passcode:	
Password:	
Login Service:	default 👻
	Login Get Another Image

# 477 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.

# 478 OpenVPN integration

### 478.1 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.

### 478.2 Prerequisites

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

### 478.3 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

### 478.4 Integration

### 478.4.1 PINsafe Integration

On the Swivel appliance

1.-) Configure and enable RADIUS Server:

RADIUS>Server	0	
Please enter the details for th	e RADIUS server.	
Server enabled:	Yes 3	
IP address:		gi di shi ya ka shikari.
Authentication port:	1812	
Accounting port:	1813	
Maximum no. sessions:	50	
Permit empty attributes:	No 3	
Additional RADIUS logging:	Both	
Enable debug:	No	
Radius Groups:	No 0	
Radius Group Keyword:		
Session TTL:	60	
Use Challenge/Response:	No	

Set the option Server Enabled to Yes

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

RAD	ius>nas 🛛			
Please e via the l	enter the details for any RADIUS interface.	RADIUS network access	servers. A NA	
NAS:	Identiñer:	openypn		
	Hostname/IP:	192.168.52.133		
	Secret:	000000000000000000000000000000000000000		
	EAP protocol:	None 🕴		
	Group:	PlNsafeUsers 🕴		
	Authentication Mode:	All		and the stand stand stand
	Vendor (Groups):	None		
	Change PIN warning:	No		
	Two Stage Auth:	No	Delete	

- 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

#### 478.4.2 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 hingly 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"

#### 478.4.3 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:

DpenVPN Connection	
Current State: Connecting	
Fri Sep 23 18:27:22 2011 OpenVPN 2.1_rc19 i686-pc-mingw32 [SSL] [LZO2] [PKCS1	11] built on Jul 16 2009
· · · · · · · · · · · · · · · · · · ·	
OpenVPN - User Authentication	
Username:	
Password:	
OK Cancel	
Disconnect Beconnect	Hide

OpenVPN-GUI for Windows

para el VPN.
Usuario:
lawrence
Clave:

Tunnelbick for Mac OSX

## 479 Palo Alto Networks Integration

### 479.1 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.

### 479.2 Prerequisites

Palo Alto Networks Firewall Palo Alto Networks documentation Swivel 3.x, 3.5 or later for RADIUS groups

### 479.3 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

### 479.4 Architecture

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

### 479.5 Swivel Configuration

#### 479.5.1 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

RADIUS>Server @		
Please enter the details for the RADIUS server.		
Server enabled:	Yes 💌	
IP address:	0.0.0.0	
Authentication port:	1812	
Accounting port:	1813	
Maximum no. sessions:	50	
Permit empty attributes:	No 💌	
Filter ID:	No	
Additional RADIUS logging:	Both	
Enable debug:	Yes 💌	
Radius Groups:	Yes 💌	
Radius Group Keyword:	POLICY	
	Apply Reset	

### 479.5.2 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.

# RADIUS>NAS 🥑

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther via the RADIUS interface.

NAS:	Identifier:	Device Name
	Hostname/IP:	192.168.0.1
	Secret:	•••••
	EAP protocol:	None
	Group:	ANY
	Authentication Mode:	All
	Change PIN warning:	No 💌
		Apply Reset

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.

#### 479.5.3 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

### 479.6 Palo Alto Networks Configuration

#### 479.6.1 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.
RADIUS Server Profile	=			0		
Name Domain Timeout Retries	PINsafe  Administrator Use Only  3  C C C C C C C C C C C C C C C C C C					
3				→ 🗙		
Server	IP Address	Secret	Port			
PINsafe	10.0.20.11	*********	1812			
+Add -Delete						
			Ск	Cancel		

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

Dashboard ACC Monitor Policies Objects Network Dev	
Setup	ce
Setup Setup	
Config Audit Name Location Servers	
Resolution Availability Swivel Radius Name: Swivel IP: 10.0.20.11 Port: 1812	
Certificates	
Response Pages	
System	
Config	
E HIP Match	
Alarms Manage Loop	
Server Profiles	
SNMP Trap	
Syslog	
Ch PADUIS	
LDAP	
Rev Kerberos	
Subsers	
Authentication Profile	
Authentication Sequence - Add - Delete Cone	
switvel   Logout	

#### 479.6.2 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.

Profile Name	Swivel		J		
Lockout					
Failed Attempts 10	(0 - 10)				
	1(0-00 mma)				
User Groups		Users			
			Edit (	llow List	
			Luite P	and yr Last.	
Authentication	RADIUS -				
Server Profile	PINsafe	-			

<b>paloalto</b>									
NETWORKS		Dashboard	AC	C Monitor	Policies	s Objects	Network	k Devic	e
								_	
HIP Match				Locko					
Alarms		Name		Failed Attempts (#)	Time (mins)	Allow List		Authentication	Ser
Manage Logs		Local				al		Local	
SNMP Trap		Swivel		10	5	all		RADIUS	PIN
Syslog Email RADIUS LDAP Carberos Users Users User Groups Authentication Profile Authentication Profile Authentication Sequence Clent Certificate Profile Clent Certificate Profile Clent Certificate Profile Scheduled Log Export Carbert Certificate Profile Construction Software SSL-VPN Clent Carbert Certificate Software SSL-VPN Clent Carbert Updates Licenses Support Master Key and Diagnostics	swith	NewD	elete	Clone					

### 479.6.3 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.

Add/Edit SSL VPN								0	
General	Nar	ne p	oinsafe						
Client Configuration	Authentication Interface Settings								
	Server Certificate	Por	rtal1		-	Tunnel Interface	tunnel.1	-	
	Authentication Profile	Sw	ivel		-	Max User	10		
	Client Certificate Profile	No	ne		-		Enable IPSec		
	Custom Login Page	No	ne		*				
		D pag	Redirect HTTP tr je	affic to HTTPS k	gin				
	Gateway Address								
	Inter	face	ce ethernet1/1					-	
	đ	noice	IP	*	192	.168.1.1		*	
	Timeout Configural	tion							
	Login Lifetime D	ays		*	3				
	Inactivity Logout H	ours		*	3				
L									
							( ×	Cancel	

#### 479.6.4 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.

GlobalProtect Gateway		
General Client Configuration HIP Notification	Name SSL-GW Authentication Server Certificate Gateway Authentication Profile Client Certificate Profile GlobalProtect-Cert-Profile Timeout Configuration	Tunnel Interfa Max U Group Na
	Login Lifetime Days 30 Inactivity Hours 2 Logout 2 Tunnel Gateway Address Interface ethernet1/1 IP Address	Group Passwe

## 479.7 Additional Configuration Options

#### 479.7.1 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

Ele View Edit Help Status: Connecting Warnings/Errors Discovering network GlobalProtect Gateway Authentication Please enter password for gateway OK Cancel	

#### Enter OTC

<b>GlobalProtect</b> File View Edit Help		_ 🗆 ×
Status: <b>Connecting</b> Warnings/Errors Discovering network	DalProtect Gateway Authentication	
		▼

🗊 GlobalProtect	
Eile <u>V</u> iew Edit <u>H</u> elp	
Status: Connected	
Warnings/Errors	
	<b>_</b>
GlobalProtect	12:5

### 479.8 Testing

Connect to the GlobalProtect Client and authenticate using RADIUS authentication.

### 479.9 Troubleshooting

Check the PINsafe logs for RADIUS requests.

### 479.10 Known Issues and Limitations

None

### 479.11 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

# 480 Salesforce.com

# **481 Introduction**

This document covers the integration of Swivel with Salesforce.com.

# **482 Prerequisites**

Salesforce.com Adminisrative Account

Swivel virtual or hardware appliance or server

PINsafe salesforce software Download and unzip the salesforce.war file

The Swivel server needs to be accessible accross the internet for the Salesforce.com server to connect, and the IDP is usually deployed so that it can also be access from the Internet. For security using a Swivel hardware or virtual appliance, the IDP is usually deployed in /webapps2 and accessible on port 8443 (or using a PAT on the appliance using 443)

# 483 Baseline

Salesforce 11, 12 Swivel 3.8, 3.9

# **484 Architecture**

Salesforce.com users authenticate using SAM-L authentication against Swivel

# 485 Installation

## 485.1 Salesforce.com Configuration

### 485.1.1 Allow Authentication

Contact Salesforce.com to enable Federated SSO

### 485.1.2 Configure Single Sign On

Using an administrative user logon to Salesforce.com and select 'Setup' from the top right button with the the user name on.



Each version of Salesforce is slightly different but each should have a screen similar to the below reached from Setup->Administrative Setup->Security Controls->Single Sign-On Settings

Hanne Challer StartHare 4					
Parsonal Setup	Single Sign-On Setting	S		Help For this Page 🚯	Alexandra Conscioned
<ul> <li>By Personal Information</li> <li>Email</li> <li>Insport</li> <li>Desisting Integration</li> <li>My Charlter Bellings</li> </ul>	Configure single sign-on in order to author	ticale users in salesforce, com from external environm je sign on method that uses a Web service call sent from s je sign on method that user SAAL assertions sent to a sal Bilk BAAL Assertion V	erls. Your organization has the following options available f alestrone.com to an endpoint. electore.com endpoint. filetor Deumbant Metadata	tr single sign-on:	
App Setup 8: Custonia	Collegated authoritication Delegated Galeway URL		Face Delegated Author Scalina Collect	D	
E Create	Poderated single sign on using SAUL				
2 Deploy	SMIL Erabled	1	SAUL Version	2.0	
View Installed Packages	SAM, Useril) Type	Faderation ID	lssuer	http://83.105.30.12.8080/SAMLSalesForce	
Critical Updates	SAM, User ID Location	Subject	Identity Provider Certificate	CN+Andy, OU+Dex, O+Solivel Secure, L+Relbarby, C+UK Explication: II Apr 2011 11:51:51 GMT	
	Mentily Provider Login URL	https://deme.savive/secure.com/hallestorce/		24 8.	·
Administration Setup	Kentity Provider Logost URL	hipscilleme swivelsecure.com/saleslovce/			
Manage Users	Curiça Emer UR	Mipscildeme.swivelsecure.com/halleslovce/error/himi			
Company Profile	Sales/arce.com Lagin URL	htps://ogin.soles/krce.com?isani=02HKPoin4nQspKPI	InSomusOmsKIM, pSWrNisBCwhCBicS2m87/yICNvOp		
Security Controls	GAuth 20 Taken Endpoint	https://ogin.sales/arce.com/sen/ces/coult/3/toker/hom/-	02HXPoin4nOspXPHoScruciOnsXULqPXn/NSBCmb06/052	nðiýt Citiv Op	
Sharing Sellings	Entity ki	https://band.salesforce.com			
Field Accessibility Passward Palities Sension Solitions	Salesforce.com Single Logout URL	Nipsologin aslesiona comisantilogosi-request jasrham Bill: Billi: Jassefan V	<ul> <li>Markin Landary NPH Astronomy Constraint (NASSCONE ON CONSTRAINT)</li> <li>Markin Landary Markinia</li> </ul>	2n54ptCHuOp	and a state of the
Metrorit Access Package Support Access Certificate and Kay Management Single Sign-On Settings					

Click on Edit. At this point you should get something similar to the screen below:

ersonal Setup Ny Personal Information	Single Sign-On Setting	\$			Help for this Plage (1)
Enal		Sure Canoel			
Desktop Integration	Bulogated authradication				8
My Challer Sellings	Delogated Gateway URL		Force Delegated Authentication Co	iket Di	5
ip Setup Customize Create Develop Deptoy View Installed Packages Critical Updates	Podaratod singto algo-con using BAU SAM, Brabled BMM, Version Monthly Provider Continuate Intentity Provider Login UTL	s a) b) b) b) b) b) b) b) b) b) b	lssuer Current Certificate Identity Provider Logont URL	https://83.105.30.12.0080/5A CN=Andy, CU=Dev, C=Svivel Secure, L=Weiherby, C=UK Explosion: 6 Apr 2011 11:51:51 GW https://demo.swivelsecure.(	and
dministration Setup Manage Users Company Postle Security Controls Sharing Settings Field Accessibility Password Policies	Conton Error URL SANIL User 10 Type SANIL User 10 Location Entity Id	https://demo.swivelsecure.e Assertion contains User's salesforce.com usemane Assertion contains the Podention ID from the User object User ID is in the Namekteniller element of the Subjectstatement User ID is in an Abitwise element User ID is in an Abitwise element https://swinelsecure-developer-edition.my.salesforce.com			SALAS KARANA MANANA
Session Settings		Saue Cancel			

#### a) upload the certificate and set the issuer

b) set the login URL and logout URL to point to the instance of salesforce-pinsafe you will have running (pointing to the instance is fine as it will re-direct to the logon page automatically)

c) set the remaining settings as above

Entity ID The issuer in SAML requests generated by Salesforce, and is also the expected audience of any inbound SAML Responses. If you don?t have domains deployed, this value is always Entity ID https://saml.salesforce.com. If you have domains deployed, Salesforce recommends that you use your custom domain name.

Ensure the users that you wish to use SSO are using a profile that has SSO enabled. Click Manage Users->Users. The profile assigned to each user is on the right hand side.

salesforce	Mariana e Mariana e Mariana e	
Anne Challer Start Hare & Personal Solup 3 My Personal Information 3 Email 3 Impart 3 Depicture Internation	All Users Verx: All Users Verx: All Users All Code Ver View All Code (Code Ver View All Code (Code Ver View)	Market and a second sec
🗵 Ny Chalter Ballings	Rend Password() Add Multiple Users	
App Schip © Contoniae © Create © Devolop	Autor Pull Same P     Altar     Discreme     Lastlagin     Pole     Autor     Polle     Manager       Ener Cash.David     Cask     darahlan/discretesumman     28/00/00111330     Casterer Susset.International     If Standard Zhahan.User       Ener Davidan.Andre     Allow     andre davidandibarbana.com     28/00/00111430     Casterer Susset.International     If Standard Zhahan.User       Ener Davidan.Andre     Allow     andre davidandibarbana.com     28/00/00111430     If National Andre       Han User     Road Passocol(d)     Md Hallple Boars     If National Andre	
Deploy View Installed Packages Critical Updates	A   B   C   D   E   F   G   W   1   X   L   M   W   C   P   Q   R   S   T   U   V   W   X   Y   2   Offer   30	41103-003
Administration Setup & Manage Users Users		

Click on the profile and find the SSO option as shown below, ensure it is enabled. If it isn't then click edit and enable it.

Administrativo Pormissions														
AP	Enabled	1						Nanoge Public List Views						
Edit HTML T	emplates							Nanoge Public Reports						
IP Restrict	Requests							Manage Public Templates						
Nanage Business Hours	Holidays							Password Never Expires						
Manage Dat	shboards							Sand Outbound Messages	1					
Manage Dynamic Dat	shboards							Transfer Record						
Manage Lei	lterheads							View Setup and Configuration	1					
Manage Public Do	cuments													
Ganaral Usar Parmissions														
Create and Customize	e Reports	1						Is Single Sign-On Enabled	1					
Create Wo	rkspaces							Manage Content Permissions						
Deliver Uploaded Files and Personal	Content	1						Nass Edits from Lists	1					
Drog-and-Drop Dashboar	d Builder							Mass Email	1					
Ed	IR Events	1						Run Reports	1					
8	dit Tasks	1						Send Email	1					
Export	Reports	1						Show Custom Sidebar On All Pages						
Import Personal	Contacts	1						Wew My Team's Dashboards						
Standard Object Permissions														
The permissions defined here cont groups of permissions for individual	rol access I contribute	al the object l vis, managers	evel. Access s, and admini	lo individu strators. <u>He</u>	al records w eu do 1 chos	ihin hatobjec 2897.7	t type is controlled by	y the sharing model. Set access levels base	d an <mark>the lunc</mark>	ional require	manis for O	te profile. Fi	or example, cre	ale dif <mark>e</mark> rent
		Basic Acc	ess			Data Adminis	éalon 👘		Basic Acc	es			Data Adminis	//afiot
		Raad	Greate	Bar	Daleka	Maw All	Nedily All		Read	Greate	Bill	Dalata	Maw All	Nedily All 1
	Accounts	1	1	1	4			Documents	1	4	1	1		
	Contacts	1	1	1	4			kleas	1	1				
Cashlop Integration Clients														
Choose whether users with this p	rolle can i	use o cliant, i	ușdate o elle	at, see alla	at update o	lerts, or be for	read to update to the	e lateat version. To set permissions for Se	laaforca for	Guillock, use	the Manes	je Emall CB	ant Conligurat	ione permisale
and canna salitinga in Criterix con	Olline	n, ood	ades w/o a l	ents 7	1									
					1									

Ensure the users have a Federation ID which will map to their Swivel username. Click Manage Users->Users, select a user then enter the Federation ID

	Employee Numb	r
hilling Address		
Street	Equinor 1 Agg2y Lane Wetherby	Tool and the second
City		La Constante de la Constante d
State/Province		
Zip/Pestal Code	LS22 7RD	WE ARE STORED
Country	England	
Single Sign On Information		
Federation ID	testFederationID	
acula Bellinga		
Time Zaby	(GNT+C000) Billion Summer (fina Bungpeterson)	
Locale	Faulth (United Kladom)	
Language	Siglish i	
loprovar Baillinga		
Delegated Approver	00	
Manager	Q	
Receive Approval Request Emails	Only (1) a main approver 🦿	
Andrew and March Ser D. March	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
enssearen een vavaraan aasuda		and the second
Receive the salesfarce.com neuroletter	e namelaBar	
E reserve ha successor contraction	a reportation	- Constant
Ganerate new password and notify user	inenactiately	
	Parce & Marco - Parcel	

### 485.2 Configure The Swivel Server

Configure a Swivel Agent (For standard XML Authentication)

1. On the Swivel Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the IP address or hostname for the server where the salesforce.war is installed, if installed on the same server as the Swivel server use 127.0.0.1 or localhost, a default entry may already exist for this

4. Enter the shared secret to be used above on the below server configuration.

5. Click on Apply to save changes

Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	•••••	
	Group:	ANY	
	Authentication Modes:	ALL	Delete
	Name:	IIS	
	Name: Hostname/IP:	IIS 192.168.1.1	
	Name: Hostname/IP: Shared secret:	IIS 192.168.1.1	1
	Name: Hostname/IP: Shared secret: Group:	IIS 192.168.1.1 ANY	

### **Configure Single Channel Access**

- 1. On the Swivel Management Console select Server/Single Channel
- 2. Ensure ?Allow session request by username? is set to YES

Server>Single Channel @	
Please specify how single channel security strin	gs are delivered.
Image file:	turing.xml
Rotate letters:	No 💌
Allow session request by username:	Yes
Only use one font per image:	Yes 💌
Jiggle characters within slot:	No 💌
Add blank trailer frame to animated images:	Yes 💌
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static 💌
Multiple AUthentications per String:	No 💌
Generate animated images:	No 💌
Random glyph order when animating:	No 💌
No. Characters Visible:	1
	Apply Reset

## 485.3 Access Device or Application Integration

**Client Side Installation** 

1. The SAML-salesforce war (salesforce.war) should be placed near a Swivel installation on a webserver. This could be a Swivel virtual or hardware appliance. On a Swivel virtual or hardware appliance this would need to be copied to the /usr/local/tomcat/webapps2 folder.

2.Inside the saleforce war exists a properties file (WEB-INF->settings.xml). Initially this will look something like:

xml version="1.0" encoding="UTF-8"? properties SYSTEM "http://java.sun.com/dtd/properties.dtd"
<properties></properties>
<pre><entry key="ssl">false</entry></pre>
<entry key="server">localhost</entry>
<pre><entry key="port">8080</entry></pre>
<entry key="context">pinsafe</entry>
<entry key="imagessl">true</entry>
<pre><entry key="imageserver">demo.swivelsecure.com</entry></pre>
<entry key="imagecontext">proxy</entry>
<pre><entry key="imageport">8443</entry></pre>
<pre><entry key="secret">secret</entry></pre>
<pre><entry key="selfsigned">true</entry></pre>
<pre><entry key="salesforceURL">https://login.salesforce.com/?saml=02HKiPoin4nQspKPHoScmudQmsKtM.qRKnViSBCmh05IC52m5VptCNw0.p</entry></pre>
<pre><entry key="audience">https://saml.salesforce.com</entry></pre>

```
<entry key="certificateIssuer">http://83.105.30.12:8080/SAMLSalesForce</entry>
<entry key="publicKeyFilePath">./keys/pinsafe/ssl/dsapubkey.der</entry>
<entry key="privateKeyFilePath">./keys/pinsafe/ssl/dsapubkey.der</entry>
<entry key="certificate">./keys/pinsafe/ssl/dsaputkey.der</entry>
</properties>
```

These settings should be changed to match, additional field values may need to be created as above:

#### The settings for the local Swivel server

For a Swivel virtual or hardware appliance the settings may be:

<entry key="ssl">false</entry>
<entry key="server">localhost</entry>
<entry key="context">pinsafe</entry>
<entry key="imagessl">true</entry>
<entry key="imagessl">true</entry>
<entry key="imagecontext">proxy</entry>
<entry key="imagecontext">proxy</entry>
<entry key="imagecontext">entry key="imagecontext">false

#### For a Swivel software install the settings may be:

<entry key="ssl">false</entry>
<entry key="server">localhost/entry>
<entry key="context">pinsafe</entry>
<entry key="imagessl">false</entry>
<entry key="imagessl">false</entry>
<entry key="imagesorver">demo.swivelsecure.com</entry>
<entry key="imagecontext">pinsafe</entry>
<entry key="secret"><entry key="imagecontext">pinsafe</entry>
<entry key="secret"><entry key="imagecontext">pinsafe</entry>
<entry key="secret"><entry key="secret"></entry></entry key="secret"><entry key="secret"><entry key="secret"</entry></entry></entry key="secret"></entry></entry key="secret"></entry></entry key="secret"></entry></entry key="secret"></entry></entry key="secret"></entry></entry</entry></entry</entry></entry</entry></entry</entry></entry</entry></entry</entry></entry</entry></entry</entry></entry</entry></entry</entry</entry></entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</entry</

The settings as per the salesforce setup (Setup->Administrative Setup->Security Controls->Single Sign-On Settings)
The location of the keys (which must match the certificate installed in salesforce)

<entry key="publicKeyFilePath">./keys/pinsafe/ssl/dsapubkey.der</entry>
<entry key="privateKeyFilePath">./keys/pinsafe/ssl/dsaprivkey.der</entry>

### 485.4 Key and Certificate Generation

see Key and Certificate Generation

#### **485.5 Additional Installation Options**

# 486 Verifying the Installation

In a browser, go to the root URL for the saml-salesforce client. This will redirect to the logon page. Logging in as a user will send a saml assertion for the username you logged in as. If this username matches to a FederationID for a user in Saleforce (see above) then you will be logged in as that user

# 487 Uninstalling the Swivel Integration

# 488 Troubleshooting

# 489 Known Issues and Limitations

# 490 Additional Information

# 491 SonicWall NSA Integration

### 491.1 SonicWall NSA PINsafe integration with SMS

The SonicWALL Network Security Appliance (NSA) Series applies next-generation Unified Threat Management (UTM) against a comprehensive array of attacks, combining intrusion prevention, anti-virus and antispyware with the application-level control of SonicWALL Application Firewall.

The appliances have SSL VPN capability with which PINsafe can provide Two Factor Authentication using SMS with RADIUS authentication.

If Strong authentication is required using TURing, then the image needs to be displayed to the user such as the use of a Taskbar, Web page etc. The use of TURing is not covered in this document.

### 491.2 Overview

#### 491.2.1 Prerequisites

Swivel 3.x configured with users and SMS gateway

SonicWALL Network Security Appliance configured for local authentication. Tested with 5.2 and 5.8

#### 491.2.2 Baseline

PINsafe 3.x NSA 240, SonicOS Enhanced 5.2.0.1-210

#### 491.2.3 Architecture

The NSA appliance was the firewall/SSL VPN device with the PINsafe server located within the DMZ.

#### 491.3 Installation

#### 491.3.1 Configuring the PINsafe server

Configure PINsafe as a RADIUS server, from the RADIUS/server menu, enter the RADIUS server details and then select Enable RADIUS server. From the RADIUS/NAS menu enter a name for the SonicWALL NAS appliance and its IP address and a shared secret key.

#### 491.3.2 Configuring the SonicWALL NSA Appliance User Settings

Select Users, then Settings, and on the menu for Authentication Method for Login: select RADIUS

SONICWALL NO	etwork Security Appliance	
<ul> <li>System</li> <li>Setwork</li> <li>PC Card</li> <li>SonicPoint</li> <li>Firewall</li> </ul>	Users / Settings	
VoIP	User Login Settings	
Application Firewall     O     VPN	Authentication method for login:	RADIUS
SSLVPN     SSLVPN     Users     Statue	Single-sign-on method:	None
Settings	Show authentication page for (minutes):	1
Local Users Local Groups Guest Services	Case-sensitive user names	
Guest Accounts Guest Status	IM Redirect users from HTTPS to HTTP on completion of login	
High Availability     Security Services	User Session Settings	

### 491.3.3 Configuring the SonicWALL NSA Appliance RADIUS settings

From the Users\Settings menu click on Configure button next to the RADIUS option, then select the Settings tab and in the Primary Server IP Address field, enter the IP address of the PINsafe server and the shared secret key, and the required port.

and a second s	rk security Applianci	0		
Settings	RADIUS Users	Test	1	
obal RADIUS Settin	gs			
ADIUS Server Timeout	(seconds): 5	Retries: 3		
ADIUS Servers				
rimary Server:				
Name or IP Address:	192.168.168.22			
Shared Secret:	•••••			
Port Number:	1812			
econdary Server:				
Name or IP Address:				
	[	8		
Shared Secret:	1			

Select the RADIUS Users tab, and ensure there is no tick in the allow only users listed locally box. Enter any other required information.

#### 491.3.4 Testing SonicWALL NSA Appliance RADIUS configuration

Select the Test tab, and enter a Username and a One Time Code in the password field from the users SMS, click on the Test button (Once only), and the returned attributes will verify if the test has worked, or alternatively, enter 1234, and check for a Authentication Rejected message.

<u>Settings</u>		RADIUS Users	Test		
	California				
To test the Ri		nas enter a valid R&D	IIIS login name a	and nassword ar	nd click the
Test button. I	Note that t	nis will apply any chang	es that have be	en made.	
User:	graham				
Password:	••••			Test	
Password:	••••	udauthastication C	CHAD C MEC		
Password:   Test:	•••• • Passwo	ord authentication C	CHAP C MSC	Test CHAP C MSCHA	Pv2
Password: Test:	••••	ord authentication C	CHAP C MSC	Test	Pv2
Password: Test: Test Status: Radius Cl Returned Us	Passwe ient Aut	ord authentication C	CHAP C MSC	Test	Pv2
Password: Test: Test Status: Radius Cl Returned Use	Passwe ient Aut ar Attribute	ord authentication C hentication Succe	CHAP C MSC	Test CHAP C MSCHA	Pv2 *
Password: Test: Test Status: Radius Cl Returned Use	•••• Passwo ient Aut	ord authentication C hentication Succe	CHAP C MSC	Test Chap C MSCHA	Pv2
Password: Test: Test Status: Radius Cl Returned Use	•••• Passwo ient Aut	ord authentication C hentication Succe	CHAP C MSC	Test CHAP C MSCHA	Pv2
Password: Test: Test Status: Radius Cl Returned Use	•••• Passwo ient Aut	ord authentication C hentication Succe	CHAP C MSC	Test Chap C MSCHA	Pv2
Password: Test: Test Status: Radius Cl Returned Use	•••• Passwo ient Aut er Attribute	ord authentication C hentication Succes	CHAP C MSC	Test	Pv2
Password: Test: Test Status: Radius Cl Returned Use	•••• Passwo ient Aut er Attribute	ord authentication C hentication Succe	CHAP C MSC	Test	Pv2

#### 491.3.5 Known Issues and Limitations

It is not currently possible to embed the Turing image into the login page, however other options such as the Taskbar utility or a web page can be used.

#### 491.3.6 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 or the local SonicWALL office http://www.sonicwall.com/emea/Support.html.

# 492 SonicWall SMA Appliances

For Integration with the SonicWall SMA Appliances see SonicWall SSL VPN Integration

# 493 SonicWall SRA EX appliances

For Integration with the SonicWall SRA EX appliances see SonicWall SSL VPN Integration

# 494 SonicWall SSL VPN Integration

### 494.1 Introduction

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

If Strong authentication is required using Single Channel such as TURing, Pinpad then the image can be displayed in the login page or in the Taskbar. The image is served from the PINsafe server to the client.

This document will use the following steps:

- · Configuring the PINsafe server
- Configuring the SonicWall login page
  Configuing the SonicWall authentication

To use the Single Channel Image such as the Turing Image, the PINsafe server must be made accessible. The client requests the images from the PINsafe server, and is usually configured using Network Address Translation, often with a proxy server. The PINsafe virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection.

### 494.2 Prerequisites

Swivel 3.x configured with users and SMS gateway

SonicWALL SSL VPN

Swivel login script for the SonicWall SSL VPN

The customisation script can be downloaded from here

A customisation script that also includes refresh for the TURing is [1] here

Swivel server must be accessible by client when using Single Channel Images, such as the TURing Image.

### 494.3 Baseline

SonicWALL SMA

SonicWALL SRA

SonicWALL SSL VPN 200 and 4200 and Firmware 3.5 onwards

SonicOS SSL-VPN 7.5.0.6-23sv

#### 494.4 Architecture

The SSL VPN appliance and the Swivel server are usually located within the DMZ. Authentication requests are made from the SonicWall SSL VPN using RADIUS.

#### 494.5 Swivel Configuration

#### 494.5.1 Configuring the RADIUS server

Configure the RADIUS settings using the RADIUS configuration page in the Swivel Administration console. In this example (see diagram below) the RADIUS Mode is set to ?Enabled? and the HOST IP (the Swivel 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 appliance VIP should not be used as the server IP address, see VIP on PINsafe Appliances

RADIUS>Server	0
Please enter the details for th	ne RADIUS server.
Server enabled:	Yes 💌
IP address:	0.0.0.0
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No 💌
Filter ID:	No 💌
Additional RADIUS logging:	Both 💌
Enable debug:	Yes 💌
Radius Groups:	Yes 💌
Radius Group Keyword:	POLICY
	Apply Reset

#### 494.5.2 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 SonicWall SSL VPN server. The IP address has been set to the IP of the VPN virtual or hardware appliance, and the secret that will be used on both the Swivel appliance and VPN RADIUS configuration.

# RADIUS>NAS 🕑

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther via the RADIUS interface.

NAS:	Identifier:	Device Name
	Hostname/IP:	192.168.0.1
	Secret:	•••••
	EAP protocol:	None
	Group:	ANY
	Authentication Mode:	All
	Change PIN warning:	No 💌
		Apply Reset

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.

#### 494.5.3 Enabling Session creation with username

The Swivel appliance can be configured so that it returns an image stream containing a TURing image by presenting the username via the XML API or the SCIMage servlet. It is this mechanism that is used to return the TURing image to the VPN sign in page.

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

#### 494.5.4 Setting up Swivel Dual Channel Transports

See Transport Configuration

#### 494.5.5 Using AD Password Authentication

This is an option to enter the AD password of users for authentication

See Check Password With Repository

#### 494.6 SonicWall SSL VPN Configuration

#### 494.6.1 Login Page Customisation

On the SonicWall SSL VPN select Portals, then click on Add Portal to open the add portal page.

•	System	Portals > Portals		
- 🏠	Portals	Portal Settings		
	Portals	Portal Name ▼	Description	Virtual H
	Application Offloading Domains	User	Secure Remote Access	N/A
	Custom Logos	VIP	Secure Remote Access	N/A
•	Services	VirtualOffice	Secure Remote Access	N/A
. 🦿	Virtual Assist	Add Portal	Offload Web Application	
•	Web Application Firewall			
•	Users			
•	Log			
	Virtual Office			

Enter the following information:

Portal Name: Name for the Portal, Example, PINsafe

Portal Site Title: Name for Portal Site, Example Virtual Office

Portal Banner Title: Name for Page, Example Virtual Office

Login Message: optional login message. If the Single channel TURing image is to be used then the login script needs to be pasted into this section. Ensure the relevant scripts are modified with the External IP NAT address of the PINsafe server:

\$('#psImage').attr('src', 'https://192.168.0.35:8443/proxy/SCImage?username=' + encodeURIComponent(username));

For a PINsafe virtual or hardware appliances this would need to be:

https://192.168.0.35:8443/proxy/SCImage?username=

For a software only install see Software Only Installation

Portal URL: The name of the login portal

Display custom login page: Ensure this is ticked

Display login message on custom login page: Ensure this is ticked

Enable HTTP meta tags for cache control (recommended): Usually selected

Enable ActiveX web cache cleaner: Optional

Enforce login uniqueness: Ensure this is ticked

Click OK to save the settings.

General	Home Page	Virtual Assist	Virtual Host	Logo
Portal Settings				
Portal Name:	Pins	afe		
Portal Site Title:	Virtu	al Office		
Portal Banner Title:	Virtu	al Office		1
Login Message:	<h1 Son Off Off</h1 	>Welcome to the icWALL Virtual ice The SonicWALL V ice provides ea	virtual	
Portal URL:	https	://192.168.200.1/por	tal/Pinsafe	
Display custom l	ogin page			
🗹 Display login	message on custom	n login page		
🗵 Enable HTTP me	ta tags for cache co	ntrol (recommended)		
Enable ActiveX v	veb cache cleaner			
I Enforce login un	queness			
		ок	СІ	ose

### 494.6.2 Configuring SonicWall SSL VPN Domain Settings

On the SonicWall SSL VPN select Portals then domains and click on Add Domain.
•	System Network	Portals > Domains				
- 🏠	Portals	Domain Settings				
	Application Offlanding	Domain Name 🔻	Authentication			
	Domains	AD	Active Directory			
1000	Custom Logos	LocalDomain	Local User Database			
> % > 🕅	Services NetExtender	Radius	Radius			
• 🧟	Virtual Assist	Add Domain				
•	Web Application Firewall	1				
•	Users					
•	Log					
	Virtual Office					

On the Add Domain page configure the Authentication server

Authentication type: select RADIUS

Domain name: Name for the domain

Authentication Type: Select the required authentication

RADIUS server address: Hostname or IP address of the PINsafe server

RADIUS server port: Usually 1812

Secret password: Enter a shared secret that needs to be also entered on the PINsafe server NAS entry

Portal Name: Select the Portal Name created above.

Click OK to save the settings.

Add Domain		
Authentication type:	Radius	
Domain name:	pin	
Authentication Protocol:	MSCHAP	11
Primary Radius server		$\langle \rangle$
adius server address:	192.168.168.3	1
Radius server port:	1812	1.
Secret password:	•••••	
Radius Timeout (Seconds):	5	
Max Retries:	2	
Backup Radius server		
Radius server address:		
Radius server port:	1812	
Secret password:		
Use Filter-ID For RADIUS	Groups	
Portal name:	VirtualOffice User VIP	•
	Pinsafe 🛛 🗲	e.M.
Enable client certificate er	nforcement	
Delete external user acco	unts on logout	
One-time passwords	raam, C 1997 <b>8</b> 7 File	
		Cancel

### 494.7 Additional Configuration Options

### 494.8 Testing

Browse to the login page and verify the login

Login page showing the TURing image where OTC is entered as the Password

# SONICWALL Virtual Office

# Welcome to the SonicWALL Virtual Office

The SonicWALL Virtual Office provides easy and secure remote access to your corporate network from anywhere on the Internet.

Username: graham	
Fetch Image	
1 2 3 4 5 6 7 8 9 0 4 8 1 6 5 0 9 2 7 3	
Password:	
Domain: PinSafe	
Login	

Login page showing the TURing image with where OTC is entered as Passsword and a Refresh Image button

# SONICWALL Virtual Office

## Welcome to the SonicWALL Virtual Office

The SonicWALL Virtual Office provides easy and secure remote access to your corporate network from anywhere on the Internet.

Username: graham	
1 2 3 4 5 6 7 8 9 0 3 5 0 7 9 1 9 2 6 8	
Refresh	
Password:	
Domain: pin 👻	

#### 494.9 Troubleshooting

Check the PINsafe logs for Turing images and RADIUS requests.

#### Users can bypass Swivel authentication

When a user authenticates using RADIUS, a local account may be created on the SonicWall. With some SSO policies the user may then not be required to sign in using RADIUS authentication. Verify the SSO policy and adjust as required.

#### 494.10 Known Issues and Limitations

None

#### 494.11 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

# 495 Stonesoft Integration

### **496 Introduction**

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

Swivel integration is made using RADIUS authentication protocol with an option to configure the login page. Depending on your needs, you can modify the default customization object or create a new customization object. There are many ways to configure it to work with Swivel.

To use the Single Channel Image such as the TURing Image and PINpad, 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.

# **497 Prerequisites**

Stonesoft Firewall Swivel 3.x Modified login page for TURing Modified login page for PINpad

### 498 Baseline

Stonesoft 4.9.9|1050

Swivel 3.9

### **499 Architecture**

Stonesoft makes authentication requests against the Swivel server by RADIUS.

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

### **500 Swivel Configuration**

### 500.1 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

RADIUS>Server	0				
Please enter the details for the RADIUS server.					
Server enabled:	Yes				
IP address:	0.0.0.0				
Authentication port:	1812				
Accounting port:	1813				
Maximum no. sessions:	50				
Permit empty attributes:	No 💌				
Filter ID:	No				
Additional RADIUS logging:	Both 💌				
Enable debug:	Yes				
Radius Groups:	Yes				
Radius Group Keyword:	POLICY				
	Apply Reset				

### 500.2 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.

# RADIUS>NAS 🥑

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther via the RADIUS interface.

NAS:	Identifier:	Device Name
	Hostname/IP:	192.168.0.1
	Secret:	•••••
	EAP protocol:	None
	Group:	ANY
	Authentication Mode:	All
	Change PIN warning:	No 💌
		Apply Reset

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.

#### 500.3 Enabling Session creation with username

The Swivel server can be configured to return an image 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 Swivel username:

Appliance

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

For a software only install see Software Only Installation

# 501 Stonesoft Configuration

### 501.1 Create a Radius Authentication Method

On the Stonesoft management console select the Manage System tab and then Authentication Methods, select Add Authentication Method...

STONESOF	T					
			Help	Brows	se Restor	e Publist
Monitor System	Manage Accounts and Storage	Manage Resou	Irce Acce	SS	Manage	System
Manage System						
Authentication Methods	Manage Authentication Methods	5				[
Certificates	Overview					
Abolishment	You can view, add, edit, and delet	te authentication m	ethods. R	egistered	d methods are	listed below
Assessment	To edit or delete an authenticatio	n method, click the	appropria	ite link in	the list.	
RADIUS Configuration	Add Authentication Method					
Notification Settings						
Device Definitions	Registered Authentication Meth	ods				
Access Points	Display Name Stonesoft Web					Status
Policy Services	Stonesoft Password					Enabled
Authentication Services						
Administration Service						
Directory Service						
OATH Configuration						
Log Off						

Select the General RADIUS authentication method



Ensure the following are checked:

- Enable authentication method
  Visible in authentication menu

Enter a Display Name, then click on Next.

Add Authentication	Method		?
General Settings			
Enter the following se one authentication m you add are listed be in the list.	ettings for the auther ethod server to the low. To edit or delete	ntication method General RADIUS authentication method. The auther e an authentication method server,	. You need to add at leas ntication method servers , click the appropriate lin
Enable authentica	tion method		
Visible in authenti	cation menu		
Display Name	SwivelRa	a	
Template Name	RADIUSI	Default	
	Manage I	Default Template Specification	
Registered Authentic	cation Method Serv	ers	
Host	Port	Timeout	
Add Authentication I	Method Server		
< Previous			Next >

Enter the following information and when complete click Next:

Host: Hostname/IP address of the Swivel server

**Port**: RADIUS authentication port, 1812 is the default for Swivel

Time-out: default 15000 milliseconds

Shared Secret: The shared secret entered on the Swivel NAS entry for the Stonesoft server

Add Authentication Meth	od Server		?
General Settings			
Enter the following setting authentication method.	gs for the authe	ntication method server and click Next to	add it to the
Host	172.16.2	05.235	
Port	1812		
Time-out	15000	milliseconds	
Shared Secret	•••••		
< Previous			Next >

Leave the RADIUS Reply settings as default unless a specific RADIUS configuration is required

Add Authentication	Method	?
General Settings		
Enter the following so one authentication m you add are listed be in the list.	ettings for the auti lethod server to th low. To edit or del	entication method General RADIUS. You need to add at leas e authentication method. The authentication method servers ete an authentication method server, click the appropriate lin
Enable authentica	ation method	
Visible in authenti	cation menu	
Display Name	Swive	Radius
Template Name	RADIL	SDefault
	Manag	e Default Template Specification
Registered Authenti	cation Method Se	rvers
Host	Port	Timeout
172.16.205.235	1812	15000
Add Authentication I	Method Server	
< Previous		Next >

On the Extended Properties page click on Add Extended Property then select *Allow user not listed in any User Storage* and set it to *true* The *Reveal RADIUS reject reason* can be used for troubleshooting if set to true.

Edit Authentication I	Method SwivelRadius	?
Add Extended Prope	erty	
Enter the following info	ormation for the extended property.	
Maria		
кеу	Lock user ID to session	
Value	Lock user ID to session	
value	Save credentials for SSO domain	
	Allow user not listed in any User Storage	
	Force create user	
	Create user on failed logon	
< Browieue	ActiveSync DeviceID Locking	Add

possibly not use: Stonesoft Authentication Method RADIUS Extended Properties.jpg

The configured RADIUS authentication method will appear under the list of Registered Authentication Methods.

Manage Authentication Methods	?
Added Authentication Method SwivelRadius	
Overview	
You can view, add, edit, and delete authentication methods. Registered To edit or delete an authentication method, click the appropriate link in t	I methods are listed below. the list.
Add Authentication Method	
Registered Authentication Methods	
Display Name	Status
Stonesoft Web	Enabled
Stonesoft Password	Enabled
SwivelRadius	Enabled

#### Select Authentication Services then Add Authentication Service

Monitor System	Manage Accounts and Storage	Manage Resource Access	Manage System	
Manage System	Authentication Services			
Authentication Methods	Manage Authentication Service	s		
Certificates	Overview			
Abolishment	You can view, add, edit, and dele	te Authentication Services, as well as	manage global RADIU	
Assessment	authentication and password/PI	N settings.		
RADIUS Configuration	Registered Authentication Servic	es are listed below. To edit or delete a	n Authentication Servic	
Notification Settings	Service Settings.	<ul> <li>click the appropriate link in the list. To manage global settings, click Manage Global Authention Service Settings.</li> </ul>		
Device Definitions	Add Authentication Convice			
Access Points	Add Addientication Service			
Policy Services	Registered Authentication Serv	ices		
Authentication Services	Service ID	Display Name	Internal Hos	
Administration Service	4	Authentication Service	127.0.0.1	
Directory Service				
OATH Configuration	Manage Global Authentication S	Service Settings		
Log Off				

On the RADIUS Authentication tab, ensure that Proxy unknown users is checked.

nage orobal riachone	cation berries settings		
ADIUS Authentication	Password/PIN Settings	E-mail Messages	SMS/Screen Messages
lanage RADIUS Auth	entication		
dd or edit global setti	ngs for RADIUS authentic	ation here.	
Vhen both "Drop unkr recedence over the fo	own users" and "Proxy ur ormer.	nknown users" are s	elected, the latter takes
Drop unknown ses	sions		
Drop unknown use	rs		
Proxy unknown use	rs		
Reveal reject reaso	n		
ession time-out	180 seco	nds	
ADIUS encoding	UTF-8		

#### When the configuration is complete then select publish

		Н	elp Brow	/se Restore	Put
Monitor System	Manage Accounts and Storage	Manage Resource	Access	Manage Sy	stem
	Publish Version				
Log Off	Configuration Published When the configuration has been Stonesoft network. For detailed in Published content - All files synch	I published successfull Iformation, please view Ironized.	y, it is distribu the system l	ited to all servers og.	in the
	Access Points				
	Display Name	Host		Status	
	Access Point	127.0.0.1		Successfu	ıl publi
	Policy Services				
	Display Name	Host		Status	
	Policy Service	127.0.0.1		Successfu	ul publi
	Authentication Services				
	Display Name	Host		Status	
	Authentication Se	127.0.0.1		Successfu	ul publi

### 501.2 Optional: Create a Secondary Authentication Server

These modifications are used only if some of the single channel features are required. The prerequisites section contains login pages for TURing and PINpad.

### 501.3 Login Page Customisation

The login page, GenericForm.html can be modified to allow a variety of different login methods.

To select a different login page browse to the files in:

select browse to select the source file, then click on Upload

Name	Size	Туре
[]		
Applet.html	1.93 KB	.html
Dialog.html	1.97 KB	.html
Dialog.pda.html	1.10 KB	.html
Dialog.wml	541 bytes	.wml
GenericForm.html	2.92 KB	.html
GenericForm.pda.html	2.09 KB	.html
GenericForm.wml	1.34 KB	.wml
SelfServiceForm.html	5.80 KB	.html
SelfServiceFormPIN.html	5.55 KB	.html
SelfServiceUserChallenge.html	3.05 KB	.html
setFocus.js	733 bytes	.js
setFocus.pda.js	660 bytes	.js
Web.jar	30.95 KB	.jar
Web.js	5.45 KB	.js
WebActiveX.cab	216.27 KB	.cab
WebSkin.zip	14.13 KB	.zip

Select all

Download selected files as zip Delete selected files

Create D	ir	Creat	e File	Rename File
 Browse	U	pload		

# 502 Testing

Browse to the login page and view the login page for the required configuration.

Stonesoft login page with Dual Channel using SMS, Mobile Client

SSL	Stonesoft SSL VPN
SwivelRadius	
User Name	
Password	
	Submit Clear

Stonesoft login page with Single Channel TURing image

Stonesoft SSL VPN SwivelRadius
User Name i.ivanov Password
Get OTC
1 2 3 4 5 6 7 8 9 0 4 2 7 8 0 5 1 5 5 3
Submit Clear

SSL	Stonesof SSL V	PN	
User Name Password Submi	iet OTC t Clear		)

# **503 Additional Configuration Options**

### 503.1 Two Stage Authentication

Swivel can be configured under the RADIUS/NAS settings to use Two Stage Authentication, whereby a password is entered and if correct the user is then prompted for a One Time Code, either from a graphical TURing image, mobile phone client or a Challenge and Response SMS sent to the user.

# 504 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

# 505 Known Issues and Limitations

None

# **506 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

# **507 Swivel Windows Credential Provider**

### 508 Introduction

Version 5 of the Credential Provider is now released. Documentation on it can be found at Windows Credential Provider. This documentation is out of date, and is not being maintained

This version has been tested on Windows 8, Windows 10 and Windows Server 2012 R2

The current version only works for 64 bit operating systems.

Swivel Windows Credential Provider is used in the desktop operating systems Windows 8 and 10 and the server operating system Windows Server 2012. For integration with Windows Vista and 7 and Server 2008, see Microsoft Windows Credential Provider Integration.

Users can authenticate using the Swivel Credential Provider allowing 2FA (Two Factor Authentication), or strong authentication at the Windows Logon. Offline authentication is also supported for single Channel authentication, following at least one successful authentication against the Swivel server with Third Party Authentication configured.

Supported methods are:

- **TURing** Lets the user sign into windows by using TURing. **PINpad** Lets the user sign into windows by using PINpad.
- On Demand Lets the user sign into windows by requesting a security string to their preferred method (SMS or email). More information.
- Other Two Factor Lets the user sign into windows by entering a one-time code based on a security string received previously or OATH token.

NOTE: One Touch is not currently supported.

#### 508.1 Downloads

Swivel Windows Credential Provider 64 bit (version 5.1.0)

### 508.2 Swivel Credential Provider FAQ

Q). Does the Credential provider support offline authentication? A). Offline authentication is permissible for Swivel users who have previously authenticated to the device. Offline local authentication is always single channel, even if single channel is normally disabled.

Q). Do all users have to authenticate using Swivel? A). Swivel has the option to Allow Unknown Users, users known to Swivel will be prompted for authentication in this instance. There is also a "Trusted Users" list where specific users can be added.

Q). Is it possible to define users who do not have Swivel authentication? A). Yes either by the Allow Unknown Users for non Swivel user authentication or by adding the user to the "Trusted Users" list

Q). Is it possible to login without AD password, A). No the AD password is required.

### **509 Prerequisites**

Swivel version 3.11.3 or later.

Connectivity to Swivel server during installation (with Third Party Authentication for GINA enabled).

Microsoft Windows 8 (including 8.1) and 10 or Windows Server 2012.

Microsoft.Net Framework version 4.

Swivel Windows Credential Provider 64 bit (version 5.1.0)

A separate Swivel Credential Provider license is not required, but the users authenticating to Swivel must be licensed.

User with AD account and valid password.

# 510 Baseline

Swivel 3.10.4 Windows 8, 10, Server 2012 R2.

### 511 Installation

#### 511.1 Basic Installation

To install the Swivel Windows Credential Provider run the installer and follow the on-screen instructions. At the end of the on-screen instructions you will be given the option to launch the configuration program to customise the Credential Provider. This can normally be found in the start menu under "Swivel Secure" and in "C:\Program Files\Swivel Secure\Swivel Credential Provider".

After installation and configuration:

- On Windows 8, 8.1 and 10 the computer must be restarted.
  On Windows Server 2012 R2 the Administration account can be signed out rather than doing a full restart.

### 511.2 Multiple Installation

If a configured Swivel Windows Credential Provider has been set up then the settings can be imported automatically on new installations.

- Extract the settings using the existing Credential Provider from the "File > Export Settings" option, keeping the default name.
   Copy this file and the installation file onto the new computer, they must be in the same location (example both files on the desktop).
   Run the installation as described above and the settings will be automatically loaded during installation.

### 512 Architecture

Swivel is installed as a Windows Credential Provider, and when a Windows login is made, AD username and password is checked against AD and the username and Swivel OTC is sent to the Swivel server using XML authentication, or locally if offline authentication is enabled.

### **512.1 Offline Authentication**

Swivel allows offline authentication using single channel but not dual channel authentication. For offline authentication the user attempting to authenticate must have made at least one successful authentication against the Swivel server while Offline Authentication has been enabled. Swivel caches a limited number of strings for authentication, when one is shown then it's classed as used and will not be re-shown, if the user makes a successful offline authentication then the number of strings will be replenished however if the user runs out of strings then they will need to authenticate online to get some more. Swivel Account lockout is disabled for Swivel offline authentication. ChangePIN will not function when the Swivel server is not contactable. Local authentication is always single channel, even if single channel is normally disabled.

Update: from version 5.4 onwards, offline is also supported for OATH tokens and for mobile app in OATH mode. This requires Sentry version 4.0.5 or later.

## **513 Swivel Integration Configuration**

#### 513.1 Configure a Swivel Agent

- 1. On the Swivel Management Console select Server/Agent.
- On the Swivel Management Console select Server/Agent.
   Enter a name for the Agent.
   Enter the Credential Provider IP address. You can limit the Agent IP to an IP address range like: 192.168.0.0/255.255.0.0 where the mask of 255 requires an exact match and 0 allows any value, so the previous example would allow any Agent in the range 192.168, or you can use an individual IP address for the Credential Provider.
   Enter the shared secret used above on the Credential Provider.
   Enter a group, (Note in this instance ANY is not a valid group and will cause authentication to fail).
   Click on Apply to save changes.

Agents:	Name:	local	
	Hostname/IP:	127.0.0.1	
	Shared secret:	•••••	
	Group:	ANY	
	Authentication Modes:	ALL	Delete
	Name:	IIS	
	Hostname/IP:	192.168.1.1	
	Shared secret:	•••••	
	Group:	ANY	
	Authentication Modes:	ALL	Delete

Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

#### 513.2 Configure Single Channel Access

- On the Swivel Management Console select Server/Single Channel.
   Ensure ?Allow session request by username? is set to YES.

Server>Single Channel 🛛	
Please specify how single channel security stri	ngs are delivered.
Image file:	turing.xml
Rotate letters:	No 💌
Allow session request by username:	Yes 🗖
Only use one font per image:	Yes 💌
Jiggle characters within slot:	No 💌
Add blank trailer frame to animated images:	Yes
Text Alpha Value:	80
Number of complete display cycles per image	: 10
Inter-frame delay (1/100s):	40
Image Rendering:	Static 💌
Multiple AUthentications per String:	No 💌
Generate animated images:	No 💌
Random glyph order when animating:	No 💌
No. Characters Visible:	1
	Apply Reset

### 513.3 Create a Third Party Authentication

If offline authentication is to be allowed, a third party authentication must be created with an Identifier of WindowsGINA. (Even though the GINA is not part of Credential Provider the third party authentication module is still used and must be configured).

- On the Swivel Management Console select Server/Third Party Authentication.
   For the Identifier Name enter: WindowsGINA (Even though the GINA is not used, this must be entered as WindowsGINA).
   For the Class enter: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA.
   For the License Key, leave this empty as it is not required.
   For the Group select a group of users (Note: the option Any cannot be selected).
   Click Apply to save the settings.

To allow offline authentication to be made a successful authentication must be made with the third party authentication in place.

Identifier:	WindowsGINA
Class:	com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA
License key:	
Group:	PINsafeUsers 🔹

### **514 Microsoft Windows Swivel Credential Provider Installation**

The Credential Provider is provided as a Microsoft Installer .msi file. You must run this as an administrator.

Double-click the .msi file to run it. Alternatively, you can install from the command line, using the msiexec command. The first page is the licence agreement:

👑 AuthControl Credential Provider 5.4.2.1 Setup — 🗌	X	
End-User License Agreement		A CONTRACTOR OF A CONTRACTOR OF A CONTRACTOR OF A CONTRACTOR A CONTRAC
THIS LEGAL DOCUMENT IS A LICENCE AGREEMENT ("LICENCE") BETWEEN YOU, THE CUSTOMER ("CUSTOMER") AND SWIVEL SECURE LTD. ("SWIVEL"). BY DOWNLOADING AND/OR INSTALLING THE ACCOMPANYING SOFTWARE PRODUCTS (THE "LICENSED SOFTWARE"), YOU, CUSTOMER, AGREE TO BE BOUND BY THE TERMS OF THIS LICENCE. ACTIVATION OF LICENSED SOFTWARE. Where relevant, Swivel shall provide Customer with an activation key or registration on		
Print Back Next Cancel		

Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

When the install has completed, the following dialog is shown:

Completed the Swivel Credential Provider 5.0.3.0 Setup Wizard Click the Finish button to exit the Setup Wizard.	
Svivel Credential Provider Configuration	
Back Finish Cancel	

### 514.1 Windows Swivel Credential Provider configuration

#### 514.1.1 Server

Sizin File Advanced Opt	rel WinCows V ons About	Declaritisi Provi	der Configurat	01	میں استیں ا میں میں مقامین میں استیں ا
Server Authentication					
Swivel Server					
Swivel Port	8080				193 WESTAANSS
Swivel Context					Malestan and Malestan Statements
Swivel Secret					
SSL 🔲 Ignore certificate errors 📝					
One Touch Timeout 60					
Test Connection					CONTRACTOR AND
	OX	Cancel	Apply	]	

Server: The Swivel virtual or hardware appliance or server IP or hostname. To add resilience, use the VIP on a swivel virtual or hardware appliance. See VIP on PINsafe Appliances.

NOTE: it has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name in this section.

Port: The Swivel virtual or hardware appliance or server port.

Context: The Swivel virtual or hardware appliance or server installation instance.

Secret: and Confirm Secret: A shared secret which must be entered onto the Swivel virtual or hardware appliance or server.

Use SSL The Swivel server or virtual or hardware appliance uses SSL communications.

Accept self signed SSL certificates Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts). You should also check this box if you are using IP address rather than host name, as recommended above.

Test Connection Tests link to Swivel server. A correct configuration should produce a dialogue box with Swivel Connection settings are correct.



Incorrect settings will produce a dialogue box with **Either the Swivel agent has not been defined, or the secret is wrong**, Please check that the machine can contact Swivel and that the entered settings are correct.



514.1.2 Authentication
Suivel Window File Advanced Options About	s Gredeniki, Provider Config	untion	The second s
Server Authentication			CINER OF STREET, STREE
Method	PINpad	v	
Test Mode			
Ignore Domain Prefix	2		
Ignore Domain Suffix	2		All and a second
Allow Unknown Users Online			
Allow Unknown Users Offline			
Require for Unlock Screen			
Remote Only			
-If Swivel Server unavailable:			derivers, since sizes
Fail authentication	0		STATES TO STRUCT
Use standard authentication	0		Contraction of the second second second
Use Offline authentication	0		
OX	Cancel Apply		

Method Select the method of authenticating with Swivel, see above.

Test Mode With test mode the user can switch to a standard authentication, see below.

Ignore Domain Prefix Swivel will Remove any domain prefix (domain\username) before matching username. This does not affect Windows authentication usernames.

Ignore Domain Suffix Swivel will Remove any domain suffix (username@domain) before matching username. This does not affect Windows authentication usernames.

Allow Unknown Users Online If the username is not recognized by Swivel, the user can authenticate using Windows credentials only. Any Swivel OTC entered will be ignored. If the user is known then they must authenticate using Swivel authentication.

Allow Unknown Users Offline If Swivel is not found and the user has not authenticated with Swivel before then the user can authenticate using Windows credentials only.

Require for Unlock Screen Shows the selected authentication method on the unlock screen.

Remote Only The selected authentication method will only be shown for users logging into the machine remotely.

If Swivel unavailable, Fail authentication lf the Swivel server cannot be contacted then authentication will fail.

If Swivel unavailable, Use standard authentication If the Swivel server is unavailable use standard authentication, the OTC field is displayed but ignored.

If Swivel unavailable, Use offline authentication If the Swivel server cannot be contacted a locally generated Turing image can be used for authentication. If this option is enabled, users will be able to force offline mode using a checkbox on the login dialog. (Only works for single channel authentication methods)

### 514.1.3 File menu



Export Settings Export settings as an XML file. These can be used to import settings elsewhere.

Import Settings Import settings from an XML file exported elsewhere.

### 514.1.4 Advanced Options

File A	Staivel Windows Cr dvanced Options About	
Sen.	Scale TURing Image	12
Meth	Irusted Users	
Test	Logging	

#### 514.1.4.1 Scale TURing Image

Scale TURing Image... Opens a dialog to let you scale the size of the TURing shown.

If Keep Aspect Ratio is selected then select the scale (%) of the TURing.



If its not selected then you can select the width and hight independently.

🕩 Scale fußing image – IM.	
Keep Aspect Ratio 📃	
TURing Width (%) 100	
TURing Height (%) 100	
OX Cancal Apply	

### 514.1.4.2 Trusted Users

""Trusted Users"" Lets listed users Authenticate without Swivel.

×	Delete	Apply
TrusteetUsers	Save	Cancel
<u>.</u>	Add	OK

To add a trusted user you must first click ""Add"" then enter the username in the text-box and click ""Save"", repeat these sets to add more users.

To edit a username select the username from the list, change the name in the text-box and click ""Save"".

To delete a username select the username from the list and press delete.

Make sure that the ""Apply"" or ""OK"" button to save these settings.

### 514.1.4.3 Logging

""Logging"" change settings relating to logging, recommended to be turned off unless problem are found.

ф.	logging		(	10 100 10 10 10 10 10 10 10 10 10 10 10
Logging Level	None		V 200	arrea and
Logging Location	C:\Users\Public\Docum	ents\Swivel <mark>(</mark> Brow	ISE Association	nanific (1999), 2 (* 18 - 1999) Rai - J. State (1999), 2 (* 18 - 1997) Tanana Tanana
OX	Cancel	Apply	- <b>Mai</b> i	ana an

""Logging Level"" The account of message that will be logged.

""Logging Location"" The location the logs will be created, this must be somewhere any account has access to.

## 514.2 Test Mode

With Test Mode enabled the user will be able to select how they will authenticate



# Administrator



The Sign-in options button is shown to let users select from the list which method they would like to use.

€	Administrator
	Password → Sign-in options
	PinPad

The last successful authentication method will be selected by default when the credential is loaded.

## **514.3 Importing Configurations**

You can import credentials exported from other installations using the Import Settings menu item.

# 515 Verifying the Installation

This will be an example of one of the credentials.

At the windows login screen a password and OTC login field should be available with a "Show PINpad" Button.

<b>(</b>	Administrator
$\bigcirc$	PINPad
	Password text
	OTC ->
	Show PINpad

Pressing the "Show PINpad" button will generate a PINpad image for authentication. The Swivel log should show a session request message: Session started for user: username.



A successful login should appear in the Swivel log: Login successful for user: username.

A failed login should not allow a login, and the following message should be displayed in the Swivel log: Login failed for user: username.

## 516 ChangePIN

A user is usually able to change the password by using the Ctrl-Alt-Del keys (Ctrl-Alt-End for remote sessions). With the Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the "Sign-in options" button and selecting the Swivel credential. This will not function for Offline authentication.

With Swivel authentication a user never changes enters PIN and this is true for ChangePIN. A user enters their current OTC, and then enters an OTC for what they wish their new PIN to be. PIN enforcement may be in place to the Swivel server to prevent the choosing of poor PIN numbers.

A user may use a single channel image or a dual channel security string to change their PIN.

¢	Change a password
	Administrator
	OTC
	New OTC
	Confirm New OTC
	Show PINpad
	Sign-in options

A successful Change PIN will show the message Your PIN was changed successfully, the Swivel server will also display in the logs a change PIN message Change PIN successful for user: username.



Other Changes to PINpad are that the PINpad dialog has buttons to select which text-box the numbers will be entered and text to show which text-box is currently selected.

## 517 Uninstalling the Swivel Integration

Use the Uninstall option from the Program menu, right click on the Windows Credentials provider and click on Uninstall. Note that uninstalling and reinstalling the Credential Provider will remove the settings, so if you need to reinstall at any point, make sure you have an exported settings file saved.

## 517.1 Disabling the Credential Provider

If the Credential Provider needs to be disabled temporarily, use the following procedure:

If the credential provider is preventing the machine starting normally, boot the machine into safe mode and log in as an administrator.

Try each of the following in turn. Only one of the following is required, so use the first one that works.

- Run the Swivel Login Configuration and edit the settings to disable the provider.
  Using regedit.exe, edit the following registry keys. Add a DWORD value named "disabled" to each one, set to 1. To re-enable it, you can set disabled to 0, rather than deleting the value.

  - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
     "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
- Uninstall the Credential Provider.
- Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}
  - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"

  - "HKEY` CLASSES ROOT \CLSID\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"

## **518 Known Issues and Limitations**

- The Swivel Windows Credential Provider does not support the use of Animated gifs for Single Channel authentication.
  It has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name for the Swivel server.
- Local authentication only works in single channel and OATH modes: the dual channel strings are not available offline.
  If the user gets an online TURing with a different scale then gets an offline TURing, the TURing is broken, the fix is to close the dialog and request an new TURing.
- If Allow Unknown Users Offline is enabled then users that have not previously authenticated to Swivel online can bypass Swivel by
- On Windows server 2012 R2 there is an update from Microsoft to fix an issue where dialogues will not be displayed, please ensure that windows update 2919355 is installed.
- Local authentication does not know if a users PIN has expired or even if the account is locked or deleted. Once a user has successfully authenticated they are allowed offline until their offline strings are deleted or the offline option is deselected.

## 519 VMware View (Horizon)

## **519.1 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.

## 519.2 Credits

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

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

### **519.3 Prerequisites**

VMware View 5.1 or higher VMware View documentation Swivel 3.x,

### 519.4 Baseline

VMware View 5.1 Swivel 3.8

### 519.5 Architecture

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

### **519.6 Swivel Configuration**

### 519.6.1 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

RADIUS>Server	0
Please enter the details for th	ne RADIUS server.
Server enabled:	Yes 💌
IP address:	0.0.0
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No 💌
Filter ID:	No 💌
Additional RADIUS logging:	Both 💌
Enable debug:	Yes
Radius Groups:	Yes
Radius Group Keyword:	POLICY
	Apply Reset

## 519.6.2 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.

# RADIUS>NAS 🥑

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther via the RADIUS interface.

NAS:	Identifier:	Device Name
	Hostname/IP:	192.168.0.1
	Secret:	•••••
	EAP protocol:	None
	Group:	ANY
	Authentication Mode:	All
	Change PIN warning:	No 💌
		Apply Reset

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.

#### 519.6.3 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

### 519.7 VMware View Configuration

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

#### 519.7.1 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.

t View Connection Serve	r Settings	
General Local Mode	Authentication Backup	
Changes to authentication Smart card authentication Disconnect user se	n settings will take effect on next user logir n: Optional 🛛 💌 ssions on smart card removal	n
Advanced Authentica 2-factor authentication	Disabled	
	Disabled	
	RSA SecurID	
	RADIUS	
	6	
		OK Cano

Edit View Connection	Server Settings	0
General Local	Mode Authentication Backup	
Changes to authen Smart card authen	tication settings will take effect on next user login tication: Optional 🔍	
Advanced Authe	ntication	
2-factor authentica	tion RADIUS -	
Enforce 2-fac	tor and Windows user name matching	
Use the same	user name and password for RADIUS and Windows	authentication
Authenticator:	Select Suthenticator	
	Manage Authenticators	
		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

environment.				
abel:	Swivel		Enter a shown to	label that will be o clients
Description:				
mary Authenticatio	on Server			
Hostname/Address:	swivel			
Authentication port:	1812	Accountin	ig port:	1813
Authentication type:	PAP	-		
Shared secret:	340 340 340 340 340 340 34	= 34= 34= 34= 34= 34=		
Server timeout:	3	seconds		
Max retries:	5			
Realm prefix:				
Realm suffix:				

Clicking OK returns to to the Authentication tab.

t View Coni	nection Server S	ettings		
General	Local Mode	Authentication	Backup	
Changes to Smart card	authentication authentication:	settings will take ef Optional •	fect on next user login removal	
Advanced 2-factor au	I Authenticatio	n ADIUS 🗸 🔻	e matching	
Use t	he same user na cator: Swivel	ame and password	or RADIUS and Windows authentication	1
	Manage	Authenticators		
				OK Cano

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.

## **519.8 Additional Configuration Options**

#### 519.8.1 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.

### 519.9 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.

A VMware Vie	w Client	
	ware ⊡ncom Mware View™	
Enter your Swi User name:	vel user name and passcode. barryc	
Passcode: Support Inform	••••••	
	OK Cancel	Help

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

VMware View Client						
	<b>n</b> ware					
Enter your use User name:	er name and password. barryc					
Password:	•••••					
Domain: <u>Support Inform</u>	SYSTEM. mation Login Cancel Help	•				

## 519.10 Troubleshooting

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

## 519.11 Known Issues and Limitations

None

### 519.12 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

## **520 WatchGuard Firebox**

## 521 Overview

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

## **522 Windows Credential Provider**

## 523 Introduction

Swivel Secure AuthControl Desktop (formerly Windows Credential Provider) is used in the desktop operating systems Windows 8, 10 and 11 and the server operating system Windows Server 2012 and 2019. For integration with Windows Vista and 7 and Server 2008, use version 5.3 or later, or see Microsoft Windows Credential Provider Integration (Legacy OS).

Users can authenticate using the Swivel Credential Provider allowing 2FA (Two Factor Authentication), or strong authentication at the Windows Logon. Offline authentication is also supported for single Channel authentication, following at least one successful authentication against the Swivel server with Third Party Authentication configured.

Supported methods are:

- TURing Lets the user sign into windows by using TURing.
- PINpad Lets the user sign into windows by using PINpad.
   On Demand Lets the user sign into windows by requesting a security string to their preferred method (SMS or email). More information.
- Other Two Factor Lets the user sign into windows by entering a one-time code based on a security string received previously or OATH token.
   Push for Windows 8 and Server 2012 R2 onwards.
- Fingerprint (From v5.4.2 onwards and requires AuthControl Sentry v4.0.5) Lets the user sign into windows using Biometric Fingerprint.

### 523.1 Downloads

Latest Release Versions:

Swivel AuthControl Desktop 64-bit version MSI 5.7.42.1 NOTE: this is the latest release. Documentation has not yet been updated to reflect the changes in this version.

Swivel AuthControl Desktop 64-bit version MSI 5.7.31.1

Swivel AuthControl Desktop 64-bit version executable 5.7.31.1

Swivel AuthControl Desktop 32-bit version MSI 5.7.31.1

If you have difficulties downloading these files, please contact teamsupport@swivelsecure.com for an alternative method.

The two versions install identical products. The difference is that the executable will copy the current settings from version 5.x and reapply them after installation. The MSI will always overwrite the settings with either blank settings or the contents of acd.xml or scps.xml if provided (see later). As of 5.7, old settings are no longer removed on upgrade, but that only applies to the version that is uninstalled, so upgrading to 5.7 from an earlier version will still remove the old settings.

Settings from versions earlier than 5 cannot be imported automatically on upgrade: you will need to export the settings, uninstall the version 4 credential provider and then install the new version and import the settings.

Important: the Credential Provider requires Microsoft Visual Studio C++ redistributable to work. Recent operating systems already include this, but it will need to be installed on older operating systems if it has not already been installed. You can retrieve it from here. If you have already installed the credential provider, it is not necessary to uninstall it before installing the redistributable.

Note that this article has not yet been fully updated to reflect the changes in version 5.6 or 5.7. See below for release notes.

Older Versions:

Swivel AuthControl Desktop 64-bit version executable 5.6.10.1

NOTE: we discovered a bug in version 5.6.3.1 whereby the stored secret fails to be decrypted at unpredictable times. We therefore recommend using the following version, 5.6.10.1, which stores the secret unencrypted. This version also fixes a problem with Push authentication, which did not work in 5.6.3.1 or 5.6.9.1.

Swivel AuthControl Desktop 64-bit version MSI 5.6.10.1

Swivel AuthControl Desktop 64-bit version executable 5.5.11.1

Swivel AuthControl Desktop 64-bit version MSI 5.5.11.1

Swivel AuthControl Credential Provider 64 bit version 5.4.4.2

Swivel AuthControl Credential Provider 64 bit version 5.4.3.2

Swivel AuthControl Credential Provider 64 bit version 5.4.2.1

Swivel AuthControl Credential Provider 64 bit version 5.3.1.5

Swivel Windows Credential Provider 64 bit version 5.1.1

Swivel Windows Credential Provider 64 bits version 5.3.0.1

### 523.2 Swivel Credential Provider FAQ

Q). Does the Credential provider support offline authentication?

A). Offline authentication is permissible for Swivel users who have previously authenticated to the device. Offline local authentication is a

Do all users have to authenticate using Swivel? A). Swivel has the option to Allow Unknown Users. Users known to Swivel will be prompted for authentication in this instance. There is also a

Is it possible to define users who do not have Swivel authentication?

A). Yes either by the Allow Unknown Users for non Swivel user authentication or by adding the user to the "Trusted Users" list

. Is it possible to login without AD password?

A). Yes, there is an option to log in without the AD password, but you must previously have logged in with the AD password.

## **524 Prerequisites**

Swivel version 3.11.3 or later. For password caching, version 4.0.4 or later is required.

Connectivity to Swivel server during installation (with Third Party Authentication for GINA enabled).

Microsoft Windows 8 (including 8.1), 10 and 11 or Windows Server 2012 (including R2) and Windows Server 2019. Version 5.3 and later have backward support for Windows Vista or later, and Windows Server 2008 or later.

Microsoft.Net Framework version 4.5.

AuthControl Windows Credential Provider 64-bit - see above for links.

A separate Swivel Credential Provider license is not required, but the users authenticating to Swivel must be licensed.

User with AD account and valid password.

## 525 Baseline

Swivel 3.11.3

Windows 8, 10, 11 Server 2012 R2, Server 2019.

## 526 Installation

## 526.1 Basic Installation

To install the Swivel Windows Credential Provider run the installer and follow the on-screen instructions. At the end of the on-screen instructions you will be given the option to launch the configuration program to customise the Credential Provider. This can normally be found in the start menu under "Swivel Secure" and in "C:\Program Files\Swivel Secure\Swivel Credential Provider".

After installation and configuration:

- On Desktop Windows versions the computer must be restarted.
- On Windows Server versions the Administration account can be signed out rather than doing a full restart.

## 526.2 Multiple Installation

If a configured Swivel Windows Credential Provider has been set up then the settings can be imported automatically on new installations.

- 1. Extract the settings using the existing Credential Provider from the "File > Export Settings" option, naming the output file either "acd.xml" or "scps.xml". Alternatively, you can export the settings as encrypted and name the file "acd.enc". Note that for the file to be imported automatically you must not specify a password (the default password will be used). 2. Copy this file and the installation file onto the new computer. They must be in the same location (for example both files on the desktop).
- 3. Run the installation as described above and the settings will be automatically loaded during installation.

NOTE: in version 5.6.9.1 and later builds, the configuration file can be named "acd.xml" instead of "scps.xml". The latter will be used by preference if both files exist.

Alternatively, you can build an pre-configured installer executable. Please contact Swivel Secure support to get the necessary build script.

- Extract the files from the zip link above into a folder
   Extract the settings using the existing Credential Provider from the "File > Export Settings" option, naming the output file "acd_in.xml".
   Replace acd_in.xml in the extracted folder with your customised one
   Compile the executable using ACDInstall.nsi with Nullsoft installation system. If you don't have a copy of Nullsoft, it can be downloaded from here.

## **527 Release Notes**

## 527.1 AuthControl Desktop 5.7

#### 527.1.1 New Features

#### 527.1.1.1 Generate offline strings outside ACD

The credential manager application allows you to authenticate to Sentry and to download offline security strings. These strings can then be exported to another machine and used there to authenticate users offline

#### 527.1.1.2 All displayed text is customisable

The configuration program allows you to customise the text displayed in the Windows credential. Additionally, you can copy the customised text to the same folder as the ACD installer and it will be imported to the target machine on installation. Currently, only one set of strings is possible per installation, but it is hoped in the future to support multiple languages.

#### 527.1.1.3 Proxy for Sentry connections

You can optionally specify an HTTP proxy for connecting to the Sentry server.

#### 527.1.1.4 Enhancements to Import and Export Settings

Version 5.6 introduced encrypted settings files using a password. Version 5.7 expands on this by allowing for a fixed password, used automatically if encryption is selected but no password is given. Automatic import of settings on installation works with encrypted settings, provided the fixed password is used for encryption. Automatic import of settings will look for the following file names, in this order:

- scps.xml (previously the only name that worked)
- acd.xml
- scps.enc ? assumes the settings are encrypted using the default password
- acd.enc ? as above

Note that the MSI installation no longer deletes the old settings on uninstallation. However, this only applies to upgrading FROM 5.7 or reinstalling. Since the settings are deleted by uninstalling the old version, upgrading from a version older than 5.7 will still remove the old settings.

#### 527.1.1.5 Change PIN for locked users

Previously, if a user attempted to log in and the account was locked due to PIN expiry, authentication would fail. Now, the PIN change screen is shown. It should be noted that in order to change a PIN when the account is locked, you need Sentry version 4.1.4 or later.

#### 527.1.1.6 Optionally, OTC field is not shown initially for Other User

It is possible to specify that the OTC field is not initially shown for the ?Other User? credential. This is the credential that is shown with an empty username field. In the case where users unknown to Sentry are permitted to log on without MFA, it might be preferable not to show the OTC field, in case it is not required. If a user logs in with username and password, and it is subsequently discovered that an OTC is required, the login form is redisplayed with the OTC field.

#### 527.1.1.7 Offline OATH works with On Demand credential

Previously, offline OATH only worked if the authentication method was set to ?Other Two-Factor? (and that not reliably ? see bug fixes). Now it also works with ?On Demand?.

#### 527.1.2 Bug Fixes / Improvements

#### 527.1.2.1 Error messages displayed for PIN change errors

Previously, if an error occurred in the PIN change screen, no message was displayed. The screen was simply redisplayed with no additional information. Now, an error is displayed on the screen indicating why the PIN change failed.

#### 527.1.2.2 Improved configuration for Single Sign-On

In 5.6 and earlier, the use of Single Sign-On (SSO) to check if MFA is required was indicated simply by providing a port and context for SSO. This could result in the settings being entered when they were not really needed, just because the fields are there. Version 5.7 shows a check-box to indicate that SSO is active. Activating SSO will display a pop-up dialog requesting the SSO settings, which includes a host name as well as port and context, so the SSO server does not have to be the same as the Sentry Core.

#### 527.1.2.3 Push authentication not working

Version 5.6 (prior to 5.6.10.1) did not support Push authentication due to incompatible changes in the code. Version 5.7 now supports Push correctly.

#### 527.1.2.4 Offline OATH not working

Version 5.6 did not always work for OATH if the token details were stored locally. This was due to an error in the encryption code that affected several features. This has now been corrected.

#### 527.1.2.5 Fixed problems with Secret not encrypting/decrypting on occasions

This problem was caused by the same encryption issue as the previous one. As a workaround, versions 5.6.9.1 and 5.6.10.1 were released with the secret being stored unencrypted, as it was in version 5.5 and earlier. Now that the encryption issue has been resolved, the secret is once again stored in encrypted format, although the encryption is not backward-compatible with 5.6, so copying the secret registry entry from 5.6 to 5.7 will not work. Exporting and importing will work, provided the secret is not encrypted in the export file.

#### 527.1.2.6 Allow unknown users online

It was discovered that version 5.6 did not correctly handle the situation where users were not known to Sentry but could authenticate with password only. This has now been fixed.

## 528 Architecture

Swivel is installed as a Windows Credential Provider. When a Windows login is made, AD username and password is checked against AD and the username and Swivel OTC is sent to the Swivel server using XML authentication, or locally if offline authentication is enabled.

## 528.1 Offline Authentication

Swivel allows offline authentication using single channel or OATH, but not dual channel authentication. For offline authentication the user attempting to authenticate must have made at least one successful authentication against the Swivel server while Offline Authentication has been enabled. Swivel caches a limited number of strings for authentication: when one is shown then it's classed as used and will not be re-shown. If the user makes a successful offline authentication then the number of strings will be replenished: however if the user runs out of strings then they will need to authenticate online to get some more. Swivel Account lockout is disabled for Swivel offline authentication. ChangePIN will not function when the Swivel server is not contactable. Local authentication is always single channel, even if single channel is normally disabled. The exception is that OATH authentication is also supported offline, provided the user has previously authenticated online using the same token.

## **529 Swivel Integration Configuration**

## 529.1 Configure a Swivel Agent

- 1. On the Swivel Management Console select Server/Agent.
- 2. Enter a name for the Agent.
- 3. Enter the Credential Provider IP address. You can use an individual IP address for the Credential Provider, such as 192.168.0.99, or you can specify an IP address range like 192.168.0.0/24, which means the first 24 bits, or 3 numbers, are significant or you (i.e. 192.168.0.x).

- Enter the shared secret used above on the Credential Provider.
   Select a group, or leave it as "Any" to allow all users to authenticate.
   Click on Apply to save changes.

## Server>Agents @

Please enter the details for any Swivel agents below. Agents are permitted to access the authentication ser

Agents:

Name:	Network
Hostname/IP:	172.22.5.0/24
Shared secret:	•••••
Group:	ANY 🗸
Authentication Modes:	ALL 🗸
Check password with Repository:	Yes 🗸
Check password for non-user:	Yes 🗸
Username attribute for repository:	userPrincipalName
Allow alternative usernames:	Yes 🗸
Alternative username attributes:	altusername
Can act as Repository:	No 🗸
URL Check password:	
Encryption/Decryption key:	

Note that this creates a GINA menu item, but there are no configurable options, so is not selectable.

### 529.2 Create a Third Party Authentication

If offline authentication is to be allowed, a third party authentication must be created with an Identifier of WindowsGINA. The name must be exactly as shown. This entry should already exist, but check that the settings are as shown.

- 1. On the Swivel Management Console select Server/Third Party Authentication.
- 2. For the Identifier Name: WindowsGINA.
- 3. For the Class: com.swiveltechnologies.Swivel.server.thirdparty.WindowsGINA.
- 4. Ensure that Enabled is set to Yes.
- 5. For the Group select a group of users, or Any to allow any users to authenticate using this third party.
- For the License Key, leave this empty as it is not required.
   Click Apply to save the settings.

# Server>Third Party Authentication @

Please enter the details of any third party authentication methods to be used. Third party authentication al checking of additional credentials to take place on top of the standard Swivel traffic.

Third parties:	Ŧ	PositiveID	
	Ξ		
		Identifier:	WindowsGINA
		Class:	com.swiveltechnologies.pinsafe.server.thirdparty.WindowsGINA
		Enabled:	Yes 🗸
		Group:	ANY 🗸
		License key:	
	Ŧ	New Entry	
			App

## 530 Microsoft Windows AuthControl Credential Provider Installation

The Credential Provider is provided as a Microsoft Installer .msi file. You must run this as an administrator.

Double-click the .msi file to run it. Alternatively, you can install from the command line, using the msiexec command.

The first page is the licence agreement:

End-User License Agreement Please read the following Icense agreement carefully THIS LEGAL DOCUMENT IS A LICENCE AGREEMENT ("LICENCE")	and a second sec
THIS LEGAL DOCUMENT IS A LICENCE AGREEMENT ("LICENCE")	
BETWEEN YOU, THE CUSTOMER ("CUSTOMER") AND SWIVEL SECURE LTD. ("SWIVEL"). BY DOWNLOADING AND/OR INSTALLING THE ACCOMPANYING SOFTWARE PRODUCTS (THE "LICENSED SOFTWARE"), YOU, CUSTOMER, AGREE TO BE BOUND BY THE TERMS OF THIS LICENCE. ACTIVATION OF LICENSED SOFTWARE. Where relevant, Swivel shall provide Customer with an activation key or registration on	

Read the licence agreement (yeah, right!), and check the box to acknowledge it. Click Next to continue.

Select the neccessary addons:

AuthControl Direct Access Manager - for integration with Direct Access

Fingerprint Enrolment - for Biometric Fingerprint enrolment and use Biometric authentication

AuthControl Creder	ntial Provider 5.4.2.1 Setup		_		X	
Custom Setup Select the way you	vant features to be installed.					
Click the icons in the	e tree below to change the wa	y features	will be installed.			
K Z	hControl Direct Access Mane perprint Enrolment	This fea your he	iture requires 58 rd drive.	900 on		
				Browse		Andreas - They area
Reget	Disk Usage	ljadk	itext	Cancel		

The application will be installed to C:\Program Files\Swivel Secure\Swivel Credential Provider. If you have reconfigured the program files directory elsewhere, it will be installed there, but otherwise you cannot control where the application is installed.

When the install has completed, the following dialog is shown:

📲 AuthControl Credential Pro	vider 5.4.2.1 Setup — 🗆 🗙	· · · · · · · · · · · · · · · · · · ·
swivelsecure	Completed the AuthControl Credential Provider 5.4.2.1 Setup Wizard Ock the Finish button to exit the Setup Wizard.	
	AuthCantral Credential Provider Configuration	
	Back Finish Cancel	

530.1 AuthControl Credential Provider configuration

### 530.1.1 Server

AuthControl Cre	1131-11-11-11-11-11-11-11-11-11-11-11-11				
File Advanced Opti	Suman and a survey of the				
Server Authentic	in a start and a start of the s				
Swivel Server					and a start the start of the start
Swivel Port	8080				
Swivel Context	pinsafe				
Swivel Secret					
Swivel SSO Port					
Swivel SSO Contex	t				a maria addina any sian di dala.
SSL 🔲 Ignore ce	rtificate errors	5 📈			an a
Security Protocol	3				·····
TLS1.2					· · · · · · · · · · · · · · · · · · ·
TLS1.1					
TLS1.0					a the second
SSL3					
One Touch Timeou	it 60				
Test Connection	·····				
					· · · · · · · · · · · · · · · · · · ·
	OK	Cancel	Apply		and the second

Server: The Swivel virtual or hardware appliance or server IP or hostname. To add resilience, use the VIP on a swivel virtual or hardware appliance. See VIP on PINsafe Appliances.

NOTE: it has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name in this section.

Port: The Swivel virtual or hardware appliance or server port.

Context: The Swivel virtual or hardware appliance or server installation instance.

Secret: and Confirm Secret: A shared secret which must be entered onto the Swivel virtual or hardware appliance or server.

SSO Port: (Sentry v4.0.5 required) The AuthControl Sentry SSO port to allow RBA usage. (ex: 8443)

SSO Context: (Sentry v4.0.5 required) The AuthControl Sentry SSO context to allow RBA usage. (ex: sentry)

Use SSL The Swivel server or virtual or hardware appliance uses SSL communications.

Accept self signed SSL certificates Check this box if Use SSL is enabled, and you do not have a commercial certificate on your Swivel server (or a certificate signed by an authority that the client machine trusts). You should also check this box if you are using IP address rather than host name, as recommended above.

Test Connection Tests link to Swivel server. A correct configuration should produce a dialogue box with Swivel Connection settings are correct.



Incorrect settings will produce a dialogue box with Either the Swivel agent has not been defined, or the secret is wrong. Please check that the machine can contact Swivel and that the entered settings are correct.



### 530.1.2 Authentication

AuthControl Credential I	81.1818.8.611.614.6.1				
Cila Ashanzad Matiane A	and the preterior of the				
Server Authentication	Annotation from the same fully a pro-				
Method	TUR	ng		Ŷ	
Test Mode					
Ignore Domain Prefix	<b>S</b>				
Ignore Domain Suffix	1				
Allow Unknown Users On	line 🗌				The second s
Allow Unknown Users Of	fline 📃				
Require for Unlock Scree	n 🗌				
Remote Only					
Password Caching					
<b>Biometric Identification</b>					
Biometric Reader	Non	5	v		
- If Swivel Server unavaila	ble:				
Fail authentication	0				
Use standard authentica					
Use Offline authenticatio	on O				
0	<	Cancel	Apply		

Method Select the method of authenticating with Swivel, see above.

Test Mode With test mode the user can switch to a standard authentication, see below.

Ignore Domain Prefix Swivel will Remove any domain prefix (domain\username) before matching username. This does not affect Windows authentication usernames.

Ignore Domain Suffix Swivel will Remove any domain suffix (username@domain) before matching username. This does not affect Windows authentication usernames.

Allow Unknown Users Online If the username is not recognized by Swivel, the user can authenticate using Windows credentials only. Any Swivel OTC entered will be ignored. If the user is known then they must authenticate using Swivel authentication.

Allow Unknown Users Offline If Swivel is not found and the user has not authenticated with Swivel before then the user can authenticate using Windows credentials only.

Require for Unlock Screen Shows the selected authentication method on the unlock screen.

Remote Only The selected authentication method will only be shown for users logging into the machine remotely.

Password Caching Allows to cache the password and login using only 2fa. This option only works online.

Biometric Identification Allows to use the Biometric Reader to obtain the username.

Biometric Reader The type of Biometric Reader: Nitgen or Native Laptop.

If Swivel unavailable, Fail authentication If the Swivel server cannot be contacted then authentication will fail.

If Swivel unavailable, Use standard authentication If the Swivel server is unavailable use standard authentication, the OTC field is displayed but ignored.

If Swivel unavailable, Use offline authentication If the Swivel server cannot be contacted a locally generated Turing image can be used for authentication. If this option is enabled, users will be able to force offline mode using a checkbox on the login dialog. (Only works for single channel authentication methods)

#### 530.1.3 File menu



Export Settings Export settings as an XML file. These can be used to import settings elsewhere.

Import Settings Import settings from an XML file exported elsewhere.

### 530.1.4 Advanced Options



#### 530.1.4.1 Scale TURing Image

Scale TURing Image... Opens a dialog to let you scale the size of the TURing shown.

If Keep Aspect Ratio is selected then select the scale (%) of the TURing.

]](1 Scale FURing Image	
TURing Scale (%) 100	
OK Cancel Apply	

If its not selected then you can select the width and hight independently.

1)# Scale TURing Image	X
Keep Aspect Ratio	
TURing Width (%) 100	
TURing Height (%) 100	Constant Annual Working
OK Cancel Apply	

#### 530.1.4.2 Trusted Users

""Trusted Users"" Lets listed users Authenticate without Swivel.

))ia	TrusterUsers	X	a come title for
			WidPress so real
Àdd	Save	Delete	Paras sinadahan ang mananan sina ang sina
OK	Cancel	Apply	

To add a trusted user you must first click ""Add"" then enter the username in the text-box and click ""Save"", repeat these sets to add more users.

To edit a username select the username from the list, change the name in the text-box and click ""Save"".

To delete a username select the username from the list and press delete.

Make sure that the "Apply" or "OK" button to save these settings.

#### 530.1.4.3 Logging

""Logging"" change settings relating to logging, recommended to be turned off unless problem are found.
<u>1</u> 9	Logging	×	prosecution
Logging Level	None	v	212 x 75 12 1
Logging Location	C:\Users\Public\Docum	tents\Swivel( Browsi	
OX	Cancel	Apply	

""Logging Level"" The account of message that will be logged.

""Logging Location"" The location the logs will be created, this must be somewhere any account has access to.

### 530.2 Test Mode

With Test Mode enabled the user will be able to select how they will authenticate



The Sign-in options button is shown to let users select from the list which method they would like to use.



The last successful authentication method will be selected by default when the credential is loaded.

## 530.3 Importing Configurations

You can import credentials exported from other installations using the Import Settings menu item.

# 531 Verifying the Installation

This will be an example of one of the credentials.

At the windows login screen a password and OTC login field should be available with a "Show PINpad" Button.

( <del>c</del> )		Administrator
	PINPad	
		Password text
	OTC ->	
		Show PINpad

Pressing the "Show PINpad" button will generate a PINpad image for authentication. The Swivel log should show a session request message: Session started for user: username.



A successful login should appear in the Swivel log: Login successful for user: username.

A failed login should not allow a login, and the following message should be displayed in the Swivel log: Login failed for user: username.

## 532 ChangePIN

A user is usually able to change the password by using the Ctrl-Alt-Del keys (Ctrl-Alt-End for remote sessions). With the Swivel Credential Provider installed, an additional option exists when the Change Password is selected, by clicking on the "Sign-in options" button and selecting the Swivel credential. This will not function for Offline authentication.

With Swivel authentication a user never changes enters PIN and this is true for ChangePIN. A user enters their current OTC, and then enters an OTC for what they wish their new PIN to be. PIN enforcement may be in place to the Swivel server to prevent the choosing of poor PIN numbers.

A user may use a single channel image or a dual channel security string to change their PIN.

E		Change a password
	Administrator	
	OTC	
	New OTC	
		Confirm New OTC →
		Show PINpad
		Sign-in options
		PinPad 🖽

A successful Change PIN will show the message Your PIN was changed successfully, the Swivel server will also display in the logs a change PIN message Change PIN successful for user: username.



Other Changes to PINpad are that the PINpad dialog has buttons to select which text-box the numbers will be entered and text to show which text-box is currently selected.

### 533 Uninstalling the Swivel Integration

Use the Uninstall option from the Program menu, right click on the Windows Credentials provider and click on Uninstall. Note that uninstalling and reinstalling the Credential Provider will remove the settings, so if you need to reinstall at any point, make sure you have an exported settings file saved.

### 533.1 Disabling the Credential Provider

If the Credential Provider fails to load correctly it can be disabled using the following process:

Boot the machine into safe mode and log in as an administrator.

Try each of the following in turn. Only one of the following is required, so use the first one that works. Experience suggests that the first two options do not work in Windows 10.

- Run the Swivel Login Configuration and edit the settings to disable the provider.
- Uninstall the Credential Provider.
- Using regedit.exe add or alter the following registry values:

  - ٠
  - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}\Disabled=1" "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}\Disabled=1"
- - Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}
  - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
  - "HKEY` CLASSES ROOT \CLSID\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"

The third option disables the credential provider, whereas the others actually remove it.

### 533.2 Temporarily Disabling the Credential Provider Remotely

If there is a problem with the Swivel Secure appliance, and you need to disable the AuthControl Credential Provider on a number of machines temporarily, you can do this using a PowerShell script.

#### 533.2.1 Enabling Powershell Remoting

In order to be able to run PowerShell scripts on remote machines, you need to enable the WinRM service on both the target machines and the machine running the script. This article provides a step-by-step guide on setting up PowerShell remoting.

#### 533.2.2 Setting up a List of Computers

The first step is to get a list of computers that you want to disable. This article suggests three alternative methods: hard-code the list in your script, read it from a file, or query the Active Directory. The last is only useful if you want to run the script on every computer on your domain. We will use the second method in our example, so assume there is a list of computer names, one per line, in "CPComputers.txt". This also assumes that the list is in the directory from which you are running the script, so you might want to use a full path in your script.

#### 533.2.3 Setting up Credentials

For completeness, we will describe how to set up credentials to connect to the remote machines. If you are able simply to use the current logged-in user credentials on all remote PCs, then you can ignore this part.

To initialize a credential for use on the remote computers, use the following PowerShell command:

\$cred = Get-Credential domain\adminuser

Replace "domain\adminuser" with the qualified name of the user whose credentials you will be using: note that you must include the domain. You will be prompted for the user's password.

If you are using the current user's credentials, leave off -Credential \$cred from the Enter-PSSession command below.

#### 533.2.4 The Script

Here is an example script for disabling the Credential Provider on a number of remote computers:

```
$cred = Get-Credential domain\adminuser
$computers = Get-Content -Path ".\CPComputers.txt"
foreach ($pc in $computers) {
  bleach (specific second condition) {
    there PSSession - ComputerName $pc -Credential $cred
    $filterPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA
    if (Test-Path $filterPath) { Set-ItemProperty -Path $filterPath -Name Disabled -Value 1 }
    $credPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
    *credPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"

           (Test-Path $credPath) { Set-ItemProperty -Path $credPath -Name Disabled -Value 1 }
  Exit-PSSession
```

### 533.2.5 Known Limitations

Be aware that running this script may not immediately disable the Credential Provider. You may need to wait a few minutes, or restart the computer, for the change to take effect.

### 533.2.6 Re-enabling the Credential Provider

To re-enable the Credential Provider, use the same script, but change the Disabled Value to 0 in two lines. So the script between Enter-PSSession and Exit-PSSession becomes

\$filterPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{6AD69A51-00E9-4BE9-A3D6-9D26255DA

if (Test-Path \$filterPath) { Set-ItemProperty -Path \$filterPath -Name Disabled -Value 0 }
\$credPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6AD69A51-00E9-4BE9-A3D6-9D26255DA4E1}"
if (Test-Path \$credPath) { Set-ItemProperty -Path \$credPath -Name Disabled -Value 0 }

### 534 Known Issues and Limitations

- The Swivel Windows Credential Provider does not support the use of Animated gifs for Single Channel authentication.
  It has been observed in testing that DNS is not always available when logging on. It is therefore recommended that you use IP address, rather than host name for the Swivel server.
- Local (offline) authentication only works in single channel and OATH modes: the dual channel strings are not available offline. • If the user gets an online TURing with a different scale then gets an offline TURing, the TURing is broken, the fix is to close the dialog and
- request an new TURing.
- If Allow Unknown Users Offline is enabled then users that have not previously authenticated to Swivel online can bypass Swivel by
- On Windows server 2012 R2 there is an update from Microsoft to fix an issue where dialogues will not be displayed, please ensure that windows update 2919355 is installed.
- Local authentication does not know if a users PIN has expired or even if the account is locked or deleted. Once a user has successfully authenticated they are allowed offline until their offline strings are deleted or the offline option is deselected.

## 535 Windows Credential Provider with RBA

## **536 Introduction**

From AuthControl Sentry v4.0.5, you can use your RBA rules with AuthControl Credential Provider to disable 2fa in case the user has enough points.

# **537 Prerequisites**

AuthControl Credential Provider v5.4.2

AuthControl Sentry v4.0.5

## **538 Limitations**

Certificate rule does not work with WCP

# 539 RBA Configuration

In AuthControl Sentry SSO administration page you have a new application type WCP. Add a new application.

Start Page	Application Tupes
Rules	Application igpes
Applications	
Authentication Methods	RADIUS VPN - Cisco ASA
View IdP Metadata	
Keys	RADIUS VPN - Citrix Netscaler
Users Active Sessions	RADIUS VPN - Juniper
User History	
Log Viewer	RADIUS VPN - Other
General Configuration	
Application Images	SAML - ADES
	WCP

Select WCP.

Start Page	Windows Credential Provider Ap	
Rules		
Applications		
Authentication Methods	Note: The Endpoint URL is used only if it is	
View IdP Metadata		
Keys		
Users Active Sessions	Name	Windows Credential Provider
User History		
Log Viewer	Image	Windows.png
General Configuration		
Application Images		
	Points	100
	Entity ID	wcp

Enter a name, the required points for authentication without 2fa, the entity ID must be wcp and click Save.

If you haven't configure any rules, please look at Authcontrol v4 Sentry SSO and Adaptive Authentication.

# 540 WCP Configuration

Open AuthControl Credential Provider Configuration

AuthControl Credential Provider Configuration     X		
File Advanced Optio	ns About	Summer and a summer of the first
Server Authentica	tion	a and a strange of the second se
Swivel Server		and a statistic statistics and the
Swivel Port	8080	
Swivel Context	pinsafe	
Swivel Secret		
Swivel SSO Port		
Swivel SSO Context		stantic alteration of a line.
SSL Ignore ceri -Security Protocol: TLS1.2 TLS1.1 TLS1.1 TLS1.0 SSL3	tificate errors 📝	
One Touch Timeout Test Connection	60	
	OK Cancel Apply	A MARK AND AND A MARK A

enter the Swivel SSO Port as 8443 and Swivel SSO Context as sentry. This will enable the check for RBA rules in WCP.

# 541 Authenticating

When you try to login now it will check for the rules. If the user has enough points, it will allow authentication without using 2fa.

# 542 RBA with fingerprint

If you have Biometric Identification active, you can use this to give more points to RBA and disable 2fa.