

Table of Contents

1 Category:Android.....	1
2 Android.....	2
3 The Swivel Android Client Overview.....	3
4 Prerequisites.....	4
5 Swivel Configuration.....	5
5.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance.....	5
5.2 Configuring the Swivel Authentication.....	5
6 Android Installation and Configuration.....	6
6.1 Installing the Android Client.....	6
6.2 Configuring the Android Client App.....	6
6.3 Downloading Security Strings (Update Keys).....	8
6.4 Options.....	11
6.5 Using the Android Client to Authenticate.....	11
6.6 Using the Android Client with ChangePIN.....	12
6.7 Updating Keys.....	14
7 Testing.....	15
8 Known Issues and limitations.....	16
9 Troubleshooting.....	17
9.1 Error Messages.....	17
10 Tested Mobile Phones.....	22
11 Android 2.0.....	23
12 Swivel Android 2.x App Overview.....	24
13 Requirements.....	25
14 Versions.....	26
14.1 Which version do I need?.....	26
15 Swivel Server Configuration.....	27
15.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance.....	27
15.2 Configuring the Swivel Authentication.....	27
16 Swivel Mobile Application Installation.....	28
17 Swivel Mobile Application Configuration.....	29
17.1 URL Provisioning.....	29
17.2 QR Code Provisioning.....	29
17.3 Get Server Settings.....	29
17.4 Manual Configuration.....	29
18 Downloading Security Strings or OTC.....	30
19 Swivel Client Policies.....	31
19.1 Authenticating with Swivel Mobile Phone Clients.....	31
19.2 Updating Keys.....	31
20 Known Issues.....	32
20.1 Android version 4.4.4.....	32
21 Troubleshooting.....	33
21.1 Error Messages.....	33
22 Tested Mobile Phones.....	34
23 Category:Blackberry.....	35
24 Blackberry.....	36
25 Overview.....	37
26 Prerequisites.....	38
27 Versions.....	39
28 Swivel Configuration.....	40
28.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance.....	40
28.2 Configuring the Swivel Authentication.....	40
29 Installing the Client.....	41
29.1 Via Blackberry App World.....	41
29.2 Over the air.....	41
29.3 Blackberry Desktop.....	41
29.4 Blackberry Enterprise Server.....	41

Table of Contents

30 Navigation.....	42
31 Configuration.....	43
32 Provisioning.....	44
33 Downloading Strings.....	45
34 Authentication.....	46
35 Troubleshooting.....	47
35.1 Error Messages.....	47
36 Known Issues.....	48
37 Tested Mobile Phones.....	49
38 Blackberry 2.0.....	50
39 The Swivel Blackberry 2.0 App Overview.....	51
40 Requirements.....	52
41 Versions.....	53
41.1 Which version do I need?.....	53
42 Swivel Configuration.....	54
42.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance.....	54
42.2 Configuring the Swivel Authentication.....	54
42.3 Mobile Provisioning.....	54
43 Swivel Mobile Application Installation.....	55
44 Swivel Mobile Application Configuration.....	56
44.1 URL Provisioning.....	56
44.2 QR Code Provisioning.....	56
44.3 Get Server Settings.....	56
44.4 Manual Configuration.....	56
44.5 Downloading Security Strings.....	56
44.6 Options.....	57
44.7 Authenticating with app.....	57
44.8 Authenticating with app and Swivel.....	58
44.9 Updating Keys.....	59
45 Known Issues.....	60
46 Troubleshooting.....	61
46.1 Error Messages.....	61
47 Tested Mobile Phones.....	62
48 Legacy.....	63
49 Citrix Receiver.....	64
50 Introduction.....	65
51 Prerequisites.....	66
52 iPhone / Android Citrix receiver.....	67
53 Citrix Netscaler RADIUS authentication for Receiver.....	68
54 Citrix Access Standard Edition Gateway RADIUS authentication for Receiver.....	69
55 Citrix Access Advanced Edition Gateway RADIUS authentication for receiver.....	70
56 Known Issues and Limitations.....	71
57 2.0 Mobile Clients Administration.....	72
58 The Swivel iPhone App v2 Overview.....	73
59 Requirements.....	74
60 Versions.....	75
60.1 Which version do I need?.....	75
61 Swivel Configuration.....	76
61.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance.....	76
61.2 Configuring the Swivel Authentication.....	76
61.3 Mobile Provisioning.....	76

Table of Contents

62 iPhone Installation and Configuration.....	77
62.1 Download compatible with Swivel 3.8 onwards.....	77
62.2 Configuring the app.....	77
62.3 Mobile Provision Code.....	78
62.4 Downloading Security Strings.....	78
62.5 Options.....	78
62.6 Authenticating with app and PINsafe.....	78
62.7 Updating Keys.....	79
63 Troubleshooting.....	80
63.1 Error Messages.....	80
64 Tested Mobile Phones.....	81
65 Known Issues and Limitations.....	82
66 Legacy.....	83
67 iPhone.....	84
68 The Swivel iPhone App Overview.....	85
69 Requirements.....	86
70 Versions.....	87
70.1 Which version do I need?.....	87
71 Swivel Configuration.....	88
71.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance.....	88
71.2 Configuring the Swivel Authentication.....	88
71.3 Mobile Provisioning.....	88
72 iPhone Installation and Configuration.....	89
72.1 Download compatible with Swivel 3.8 to 3.9.....	89
72.2 Configuring the app.....	89
72.3 Mobile Provision Code.....	90
72.4 Downloading Security Strings.....	90
72.5 Options.....	90
72.6 Authenticating with app and PINsafe.....	90
72.7 Updating Keys.....	91
73 Troubleshooting.....	92
73.1 Error Messages.....	92
74 Tested Mobile Phones.....	93
75 Known Issues and Limitations.....	94
76 Legacy.....	95
77 Category: iPhone.....	96
78 iPhone 2.0.....	97
79 The Swivel iPhone 2.0 App Overview.....	98
80 Requirements.....	99
81 Versions.....	100
81.1 Which version do I need?.....	100
82 Swivel Configuration.....	101
82.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance.....	101
82.2 Configuring the Swivel Authentication.....	101
82.3 Mobile Provisioning.....	101
83 User Experience with 'Quick Provisioning'.....	102
84 iPhone Installation and Configuration.....	103
84.1 Download compatible with Swivel 3.10 onwards.....	103
84.2 Configuring the app.....	103
84.3 Mobile Provision Code.....	104
84.4 Downloading Security Strings.....	104
84.5 Options.....	104
84.6 Authenticating with app.....	105
84.7 Authenticating with app and Swivel.....	105
84.8 Updating Keys.....	106
85 Troubleshooting.....	107
85.1 Error Messages.....	107
86 Known Issues and Limitations.....	108

Table of Contents

87 Legacy.....	109
88 Mobile Phone Client.....	110
89 Mobile Phone Client 2.x.....	111
89.1 Overview.....	111
89.2 Integrating with the Mobile App.....	111
90 Mobile Phone Client 1.0.....	112
90.1 Overview.....	112
90.2 Integrating with the Mobile App.....	112
91 iPad Citrix Receiver.....	113
92 Category:Java.....	114
93 Java Mobile Phone Client.....	115
93.1 Swivlet How To Guide.....	115
93.2 Overview.....	115
93.3 Prerequisites.....	115
93.4 Swivel Server Configuration.....	115
93.5 Swivlet Installation on Phone.....	115
93.6 Swivlet Configuration on Phone.....	115
93.7 Testing.....	116
93.8 Options.....	116
93.9 Troubleshooting.....	116
93.10 Error Messages.....	116
93.11 Known Issues and Limitations.....	117
93.12 Tested Mobile Phones.....	117
93.13 RADIUS Considerations.....	117
94 Mobile App Privacy Policy.....	118
95 Notes.....	119
96 Privacy Policy.....	120
97 Need more help?.....	121
98 QR Code Provision.....	122
99 Overview.....	123
100 Prerequisites.....	124
101 QR Code Setup.....	125
101.1 Transport Configuration.....	125
102 Testing.....	126
102.1 Provisioning a Mobile Client.....	126
103 Known Issues.....	127
104 Troubleshooting.....	128
104.1 Error Messages.....	128
105 How To Configure Local Mode Mobile.....	129
105.1 Overview.....	129
105.2 Prerequisites.....	129
105.3 Swivel core configuration.....	129
105.4 Configuring Local Mode policy settings.....	129
105.5 Testing.....	130
105.6 Troubleshooting.....	130
106 How To Configure OATH Mobile.....	132
106.1 Overview.....	132
106.2 Prerequisites.....	132
106.3 Swivel core configuration.....	132
106.4 Configuring OATH policy settings.....	132
106.5 Define a group of Mobile OATH users.....	134
106.6 Testing.....	134
106.7 Troubleshooting.....	134
107 How To Configure Push Mobile.....	136
107.1 Overview.....	136
107.2 Prerequisites.....	136
107.3 Swivel core configuration.....	136
107.4 Configuring Dual Channel settings.....	136
107.5 Define a group of Push Users.....	136
107.6 Define a Push Transport.....	137
107.7 PNA configuration.....	138
107.8 PNA V5 Configuration.....	139
107.9 iOS Users.....	140
107.10 Android Users.....	140
107.11 Testing.....	140

Table of Contents

107 How To Configure Push Mobile	
107.12 Troubleshooting.....	140
108 How To Provision Mobile Apps.....	142
108.1 Provisioning Mobile Apps.....	142
108.2 How it works.....	142
108.3 Site ID.....	142
108.4 Provision URLs.....	142
108.5 Quick Provision Link.....	143
108.6 QR Code.....	143
108.7 Policies.....	143
108.8 Troubleshooting.....	145
109 Mobile Client Policies.....	146
110 Mobile Client Policy Overview.....	147
111 Requirements.....	148
112 Swivel Configuration.....	149
112.1 Mobile Provisioning.....	149
113 Error Messages.....	150
114 Mobile Client Policies 2.0.....	151
115 Mobile Client Policy Overview.....	152
116 Requirements.....	153
117 Swivel Configuration.....	154
117.1 Mobile Provisioning.....	154
118 Messages.....	155
119 Mobile Phone Client RADIUS Authentication.....	156
119.1 Overview.....	156
119.2 Prerequisites.....	156
119.3 Symptoms.....	156
119.4 Solution.....	156
120 Mobile Provision Code.....	157
121 Mobile Provision Code Overview.....	158
121.1 Swivel Core Verion information.....	158
122 Requirements.....	159
122.1 Swivel Configuration.....	159
122.2 Mobile Self Provisioning.....	159
122.3 Obtaining a Provision code using the Self Provisioning feature.....	159
122.4 Mobile Client Configuration.....	159
123 Verify Device Provisioning.....	162
124 Error Messages.....	163
125 Category:Swivel Policy Mobile.....	164
126 Category:Windows.....	165
127 Windows Mobile How To Guide.....	166
128 Windows Mobile How To Guide.....	167
129 Overview.....	168
130 Prerequisites.....	169
130.1 Mobile App Store versions.....	169
131 Swivel Configuration.....	170
131.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance.....	170
131.2 Configuring the Swivel Authentication.....	170
132 Windows Mobile Installation.....	171
133 Testing.....	172
134 Troubleshooting.....	173
134.1 Known Issues.....	173
134.2 Error Messages.....	173
135 Tested Mobile Phones.....	174

Table of Contents

136 RADIUS Considerations.....	175
137 Windows Phone 7 How To Guide.....	176
138 Overview.....	177
139 Prerequisites.....	178
139.1 Mobile App Store versions.....	178
140 Swivel Configuration.....	179
140.1 Configuring Mobile Client user access on the Swivel appliance.....	179
140.2 Configuring the Swivel Authentication.....	179
141 Getting the Application.....	180
142 Using the Application.....	181
143 Configuration.....	183
144 Provisioning.....	185
145 Top Up.....	187
146 Authentication.....	189
146.1 Change PIN.....	190
147 Known Issues.....	191
148 Troubleshooting.....	192
149 Windows Phone(8) 2.0 How To Guide.....	193
150 The Swivel Windows Phone 8 2.0 App Overview.....	194
151 Requirements.....	195
152 Versions.....	196
152.1 Which version do I need?.....	196
152.2 Mobile App Store versions.....	196
153 Swivel Configuration.....	197
153.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance.....	197
153.2 Configuring the Swivel Authentication.....	197
153.3 Mobile Provisioning.....	197
154 Windows Phone 8 Installation and Configuration.....	198
154.1 Download compatible with Swivel 3.10 onwards.....	198
154.2 Configuring the app.....	198
154.3 Mobile Provision Code.....	199
154.4 Downloading Security Strings.....	199
154.5 Options.....	199
154.6 Authenticating with app.....	199
154.7 Authenticating with app and PINsafe.....	200
154.8 Updating Keys.....	201
155 Troubleshooting.....	202
155.1 Device fails to Quick Provision.....	202
155.2 Error Messages.....	202
156 Tested Mobile Phones.....	203
157 Legacy.....	204

1 Category:Android

2 Android

3 The Swivel Android Client Overview

For version 2 of the Swivel Android client see [Android 2.0](#)

Swivel Secure now offers an Android client for use with the Swivel platform. This article explains how to download, configure and use this client. For the Java Applet version see [Swivlet How To Guide](#), for the Windows Mobile version see [Windows Mobile How To Guide](#), for the iPhone client see [iPhone](#). For the BlackBerry Client see [Blackberry](#).

4 Prerequisites

Android Phone

The Swivel virtual or hardware appliance must be reachable from the mobile phone to receive security strings

Access device for authentication

The index is required to be entered as nn on the end example: 292401, Swivel versions earlier than 3.10 require ,nn example: 2924,01 otherwise it will see it as a dual channel authentication.

Virtual or hardware appliances using Swivel 3.8 may require an upgrade on their proxy to provision a mobile device, see [Appliance Proxy Server Upgrade](#)

RADIUS authentications made against Swivel must use PAP RADIUS authentication since with other RADIUS protocols such as CHAP and MSCHAP the access device requests the OTC from Swivel.

5 Swivel Configuration

5.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance

To allow a user to authenticate using a One Time Code from the Mobile Phone Client, the user must have the Mobile Client authentication enabled. To do this on the Swivel Administration console ensure that the group they are part of has access to the Mobile Client under Repository Groups.

5.2 Configuring the Swivel Authentication

Swivel can authenticate users using the mobile client to authenticate by RADIUS or Agent-XML authentication

- For RADIUS authentication see [RADIUS Configuration](#) Note: The access device connecting to the Swivel RADIUS must be configured to use PAP for authentication.
- For Agent-XML authentication see [XML Authentication Configuration](#)
- To display to the user a the number of the Security String or One Time Code to use, see [Mobile Security String Index](#)

5.2.1 Mobile Provisioning

Swivel 3.8 and higher requires each mobile phone to be provisioned so it can be uniquely identified. Ensure that all Mobile Client users have suitable Transports configured to receive their Provision Code. To provision the mobile client select the user and click Re-provision. Earlier versions of Swivel do not need to use a Mobile Provision Code. See [Mobile Provision Code](#).

5.2.2 Mobile Client Policies

For the Server based policies see [Mobile Client Policies](#)

6 Android Installation and Configuration

6.1 Installing the Android Client

The Swivel Android client is available from the [Android Market place](#) and can be downloaded directly onto the mobile phone.

Alternatively to find the application go the Android Marketplace <https://play.google.com> and search for "swivel secure".

The pinsafe.apk file may also be uploaded by various utilities such as Droid Explorer, the Android Marketplace is the preferred method of deployment. A Swivel version for testing is available here [Swivel Android Client](#)

6.2 Configuring the Android Client App

When you launch the Android Client select Settings on the main screen, the option to select a 3.8 and Above server can be made.



6.2.1 Get Server Settings

If a [SSD](#) server is being used, then select **Get Server Settings** and enter the Server ID, otherwise the settings can be manually entered with information from the Swivel System administrator.

6.2.2 Manual entry of Server Settings

The settings are

1. PINsafe Version The Version of the Swivel server. Default pre 3.8, Options pre 3.8 or 3.8 and above
2. User Your username that you use when you authenticate via Swivel
3. Webservice URL The URL from where the client can download security strings (or keys)
4. Webservice Port The port number used by the webservice. For a virtual or hardware appliance this is **8443**, for a software install this is **8080**
5. Webservice Context The context used by the webservice. For a virtual or hardware appliance this is **proxy**, for a software install this is usually **pinsafe**

Once you have entered the settings return to the main Swivel screen.

3G 3:16 PM

PINsafe Client

SWIVEL®

PINsafe Version

Pre 3.8

User

Web service URL

https://

Web service Port

0

Web service Context

Authentication Solutions

3G 3:18 PM

glatiani

Web service URL

https://pinsafe.swivelsecure.com

Web service Port

8443

Web service Context

pinsafe

q w e r t y u i o p

a s d f g h j k l

↑ z x c v b n m DEL

?123 , _ . Done

3G 6:34 PM

PINsafe Client

SWIVEL®

Pre 3.8

User

graham

Webservice URL

http://10.40.10.220

Webservice Port

8080

Webservice Context

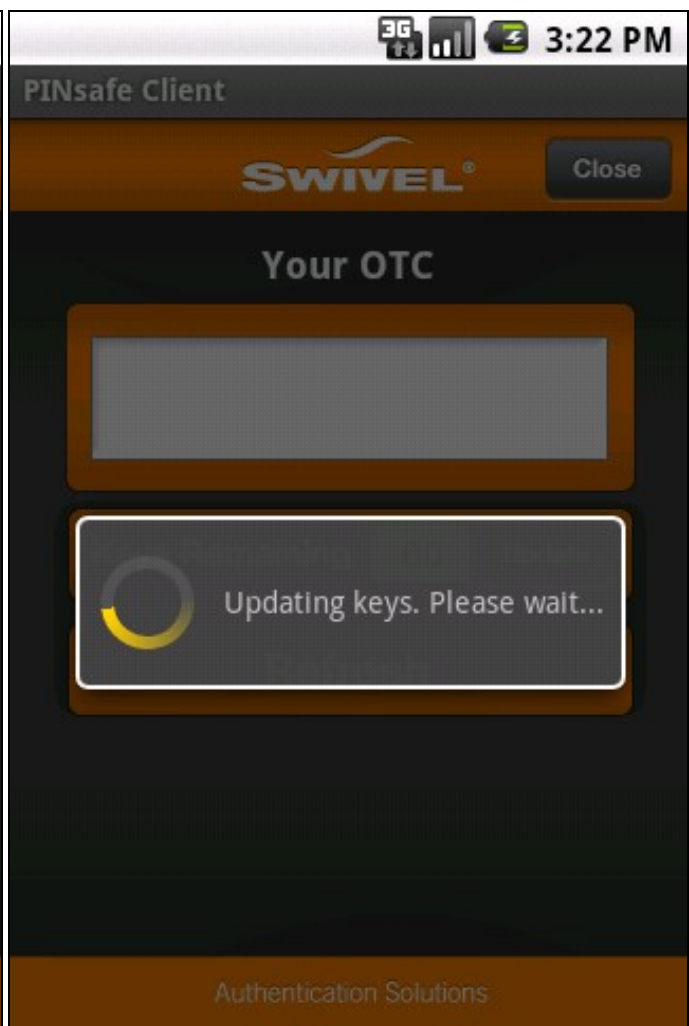
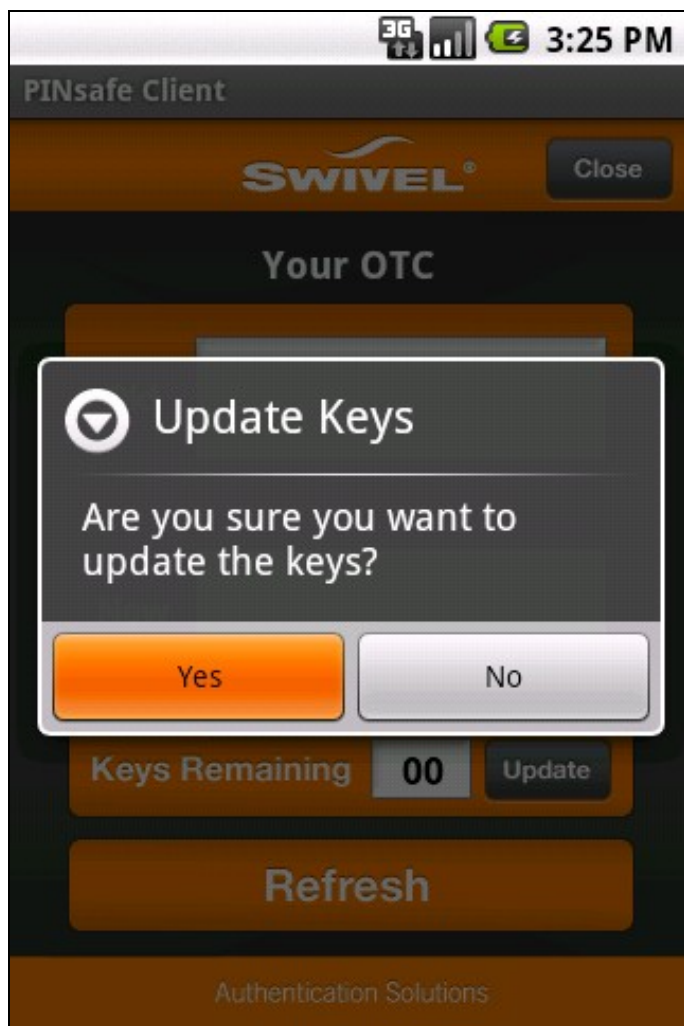
proxy

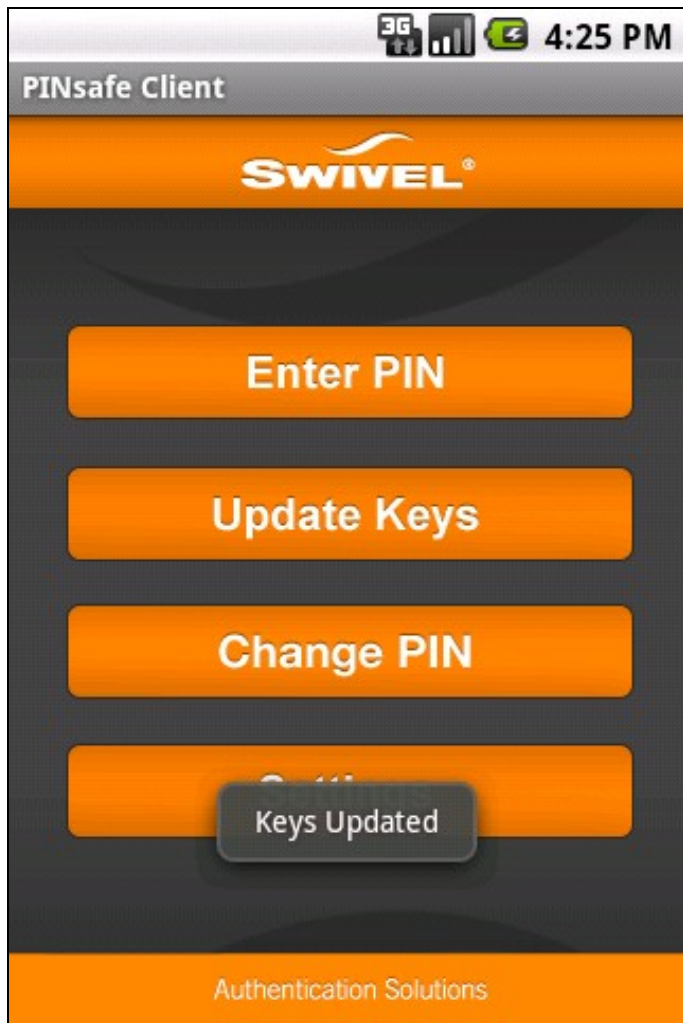
Authentication Solutions

6.3 Downloading Security Strings (Update Keys)

At the main menu, test the settings by Selecting the Update Keys option, at the prompt select Yes to confirm to update the keys. This will attempt to retrieve Security Strings from the Swivel virtual or hardware appliance.

You will see a brief message stating Updated Keys and then if all is well the display will return to the main menu.

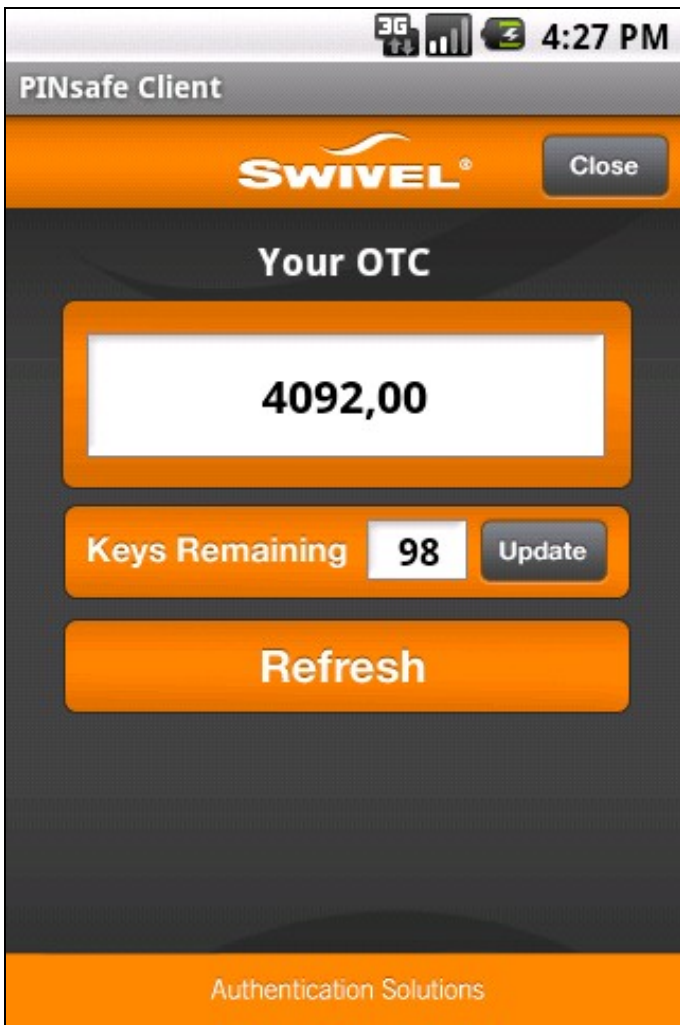




If there are any problems an error message will be displayed.

You can confirm that keys have been downloaded by going to the Enter PIN screen and Entering you PIN. (Note: Version 2 does not ask for PIN entry but for additional security provides an OTC). Once you have entered your PIN you will see you extracted one-time code and the number of Security Strings (Keys) you have remaining. The Swivel virtual or hardware appliance will display the following log message **Security strings fetched for user: username**

The first time you do this after downloading keys, the Keys Remaining will show as 98.



6.4 Options

The following options are available:

Auto extract OTC, Prompt for PIN Number to auto-extract OTC, Options, enable/disable. This option may be turned off on the Swivel server. When enabled this allows the user to enter their PIN number and a One Time Code will be displayed. Note that there is no error checking of the PIN, so if an incorrect PIN is entered an incorrect One Time Code will be displayed.

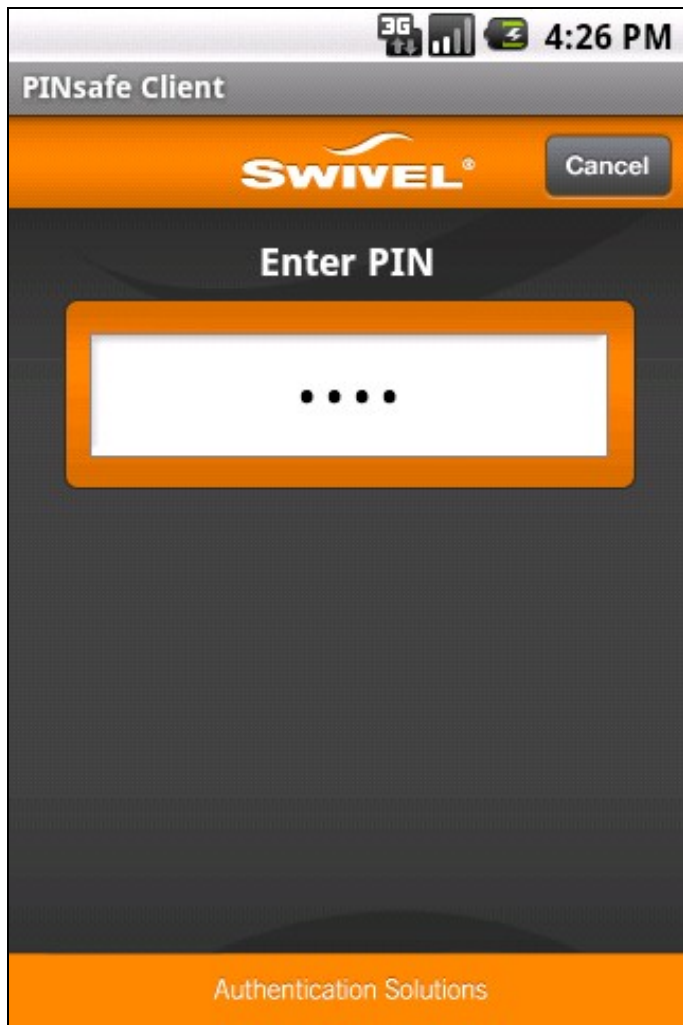
Allow String Browsing, This is a Swivel server controlled option, which if enabled will allow the user to browse through security strings on the mobile app.

6.5 Using the Android Client to Authenticate

To use the Swivel Android Client to authenticate is very simple.

1. Open the application on your Android
2. Select the Enter PIN Option (Note: Version 2 does not ask for PIN entry but for additional security provides an OTC)
3. Enter your PIN using the Android keypad displayed.
4. The client will show the OTC that you need to enter, (as shown above)
5. Enter the OTC into the authentication dialogue, including the ',' and the following 2 digits. e.g. 0947,00

If you need to authenticate again you can select the refresh option



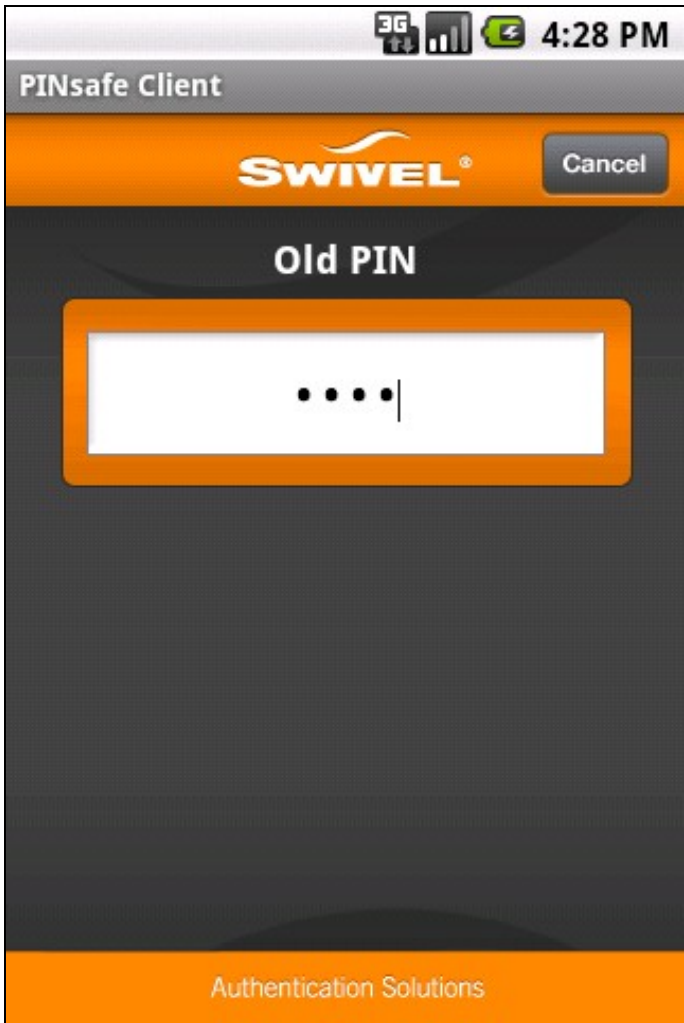
6.6 Using the Android Client with ChangePIN

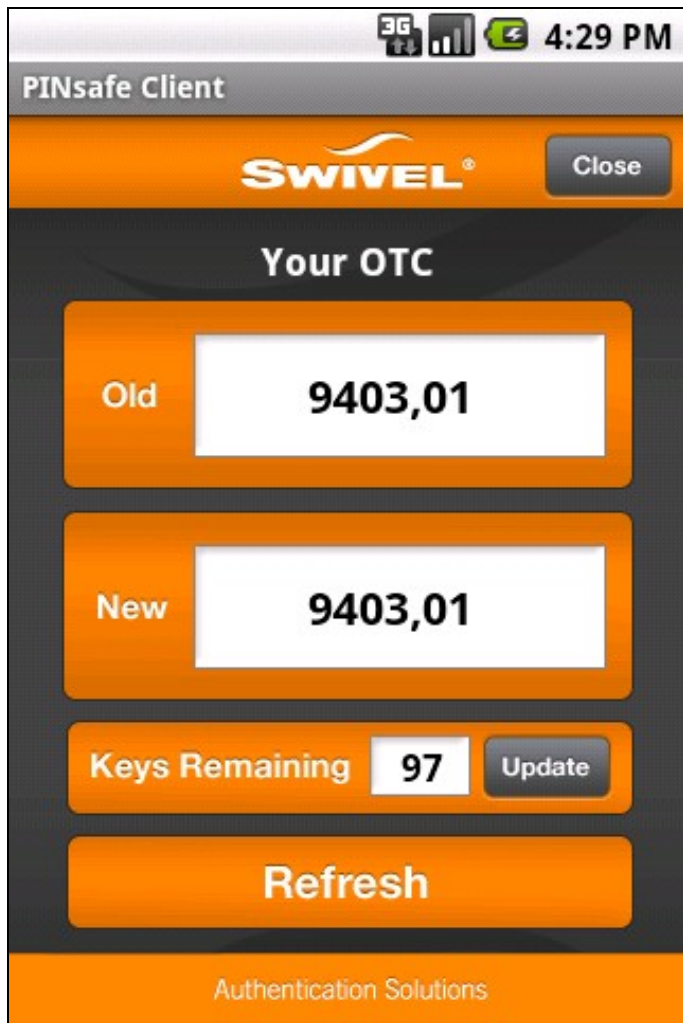
The client can be used in conjunction with the Swivel changePIN application to allow a user to change their PIN.

For the Swivel version 2 Android Client, the ChangePIN feature is deprecated. To use ChangePIN, view a security string and use the details to obtain an OTC and generate a new OTC.

For the version 1 client the user first accesses the change pin application in their computer browser then selects the Change PIN option on the Android Client

On the Swivel client page you first enter your current PIN, then on the next screen you enter your New PIN.





The next screen then displays the two OTCs you need to enter within the Change PIN dialogue in your browser.

6.7 Updating Keys

The client downloads 99 keys at a time and these keys are used one at a time until there are none left. However a new set of 99 keys can be downloaded at any time by using the Update Keys. Downloading keys requires network connectivity so it is recommended that you download a new set of keys before the Android Client is likely to be without network connectivity for any length of time.

7 Testing

When downloading security strings, the following messages should be seen **Security strings fetched for user:**

8 Known Issues and limitations

The current version only supports one device per user.

Older versions of the Android client only supports numbers for the authentication string rather than letters. If letters are set on the Swivel virtual or hardware appliance then a security string of -1,-1,-1,-1,00 is displayed. The current version supports numbers and letters.

PIN numbers may be from 4 to 8 digits in length

Version 2.0 of the client has a changePIN button, but pressing it has no effect. The ChangePIN button has been deprecated, see ChangePIN above.

9 Troubleshooting

Is the Swivel virtual or hardware appliance accessible on the internet

Check the connection settings to the Swivel virtual or hardware appliance

Check the Swivel logs for any error messages

Can the phone access the internet

If a RADIUS connection is seen from the access device to the Swivel virtual or hardware appliance but authentication fails, try using PAP

Download new security strings to the phone and retest

Is the OTC being entered with the comma and last two digits. E.g. 7329,62

If the proxy port (8443) on the virtual or hardware appliance is being used, ensure that it supports the proxy request of the key retrieval using AgentXML. If this is the case then contact Support for an updated version of the Proxy.

The PIN cannot be entered, version 2 of the client. For security the option to enter the PIN has been removed, instead a security string is displayed.

Login fails and User receives a security string or One Time Code by SMS or email at each login attempt. The index is required to be entered as nn or ,nn example 2924,01 otherwise it will see it as a dual channel authentication.

9.1 Error Messages

Incorrect settings - please check your settings

The settings for downloading the security strings are incorrect. Verify what has been entered, and check what the values should be.

Timed Out

The settings for connecting to the Swivel virtual or hardware appliance may be incorrect or the port is being blocked.

Failure Please check your settings or try again later. Message: At line 1, column 0: no element found

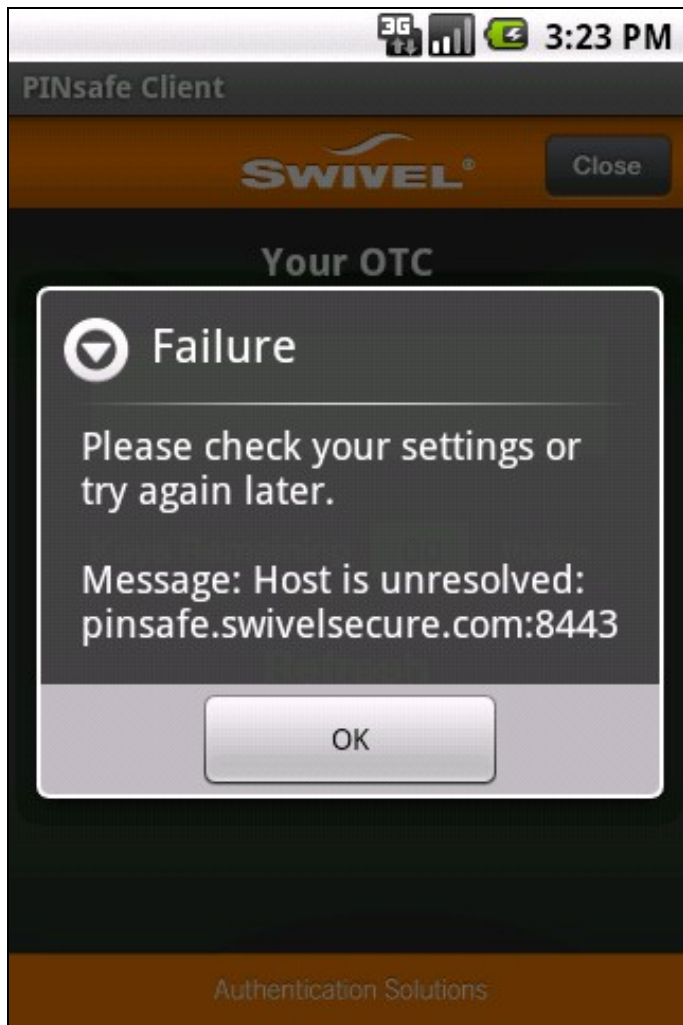
Mobile Client cannot connect to the Swivel server. Check network setting and that client has network access.

Error occurred whilst fetching security strings for user: graham, error: The user does not belong in the correct group within the user repository to continue the authentication attempt.

The user does not have permissions to use the Mobile client or Swivlet.

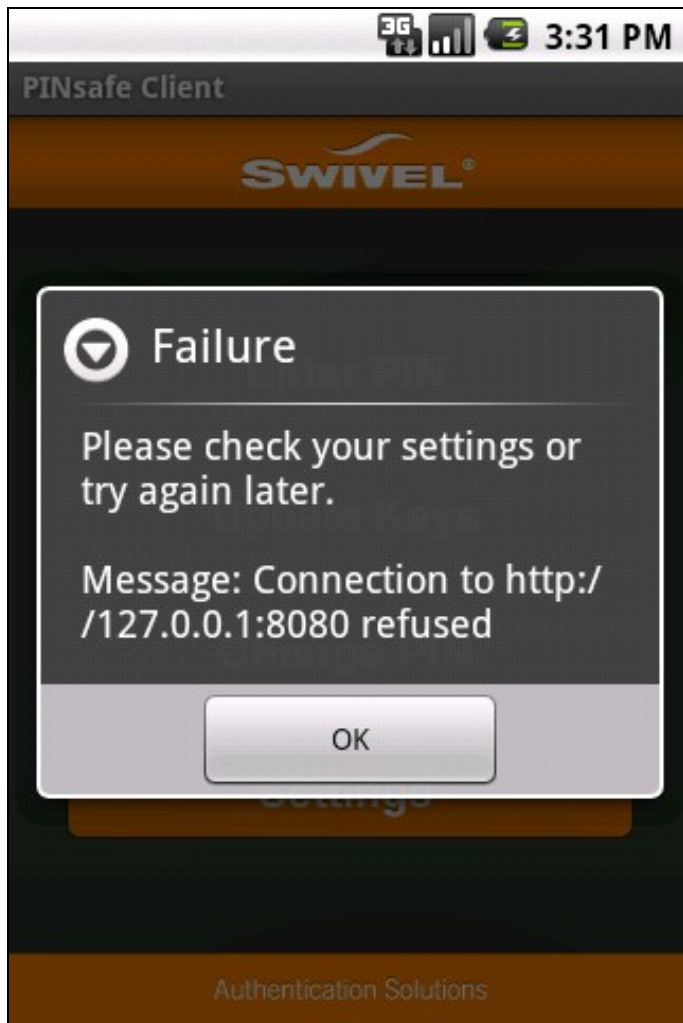
Host is unresolved

Hostname cannot be found, check the settings



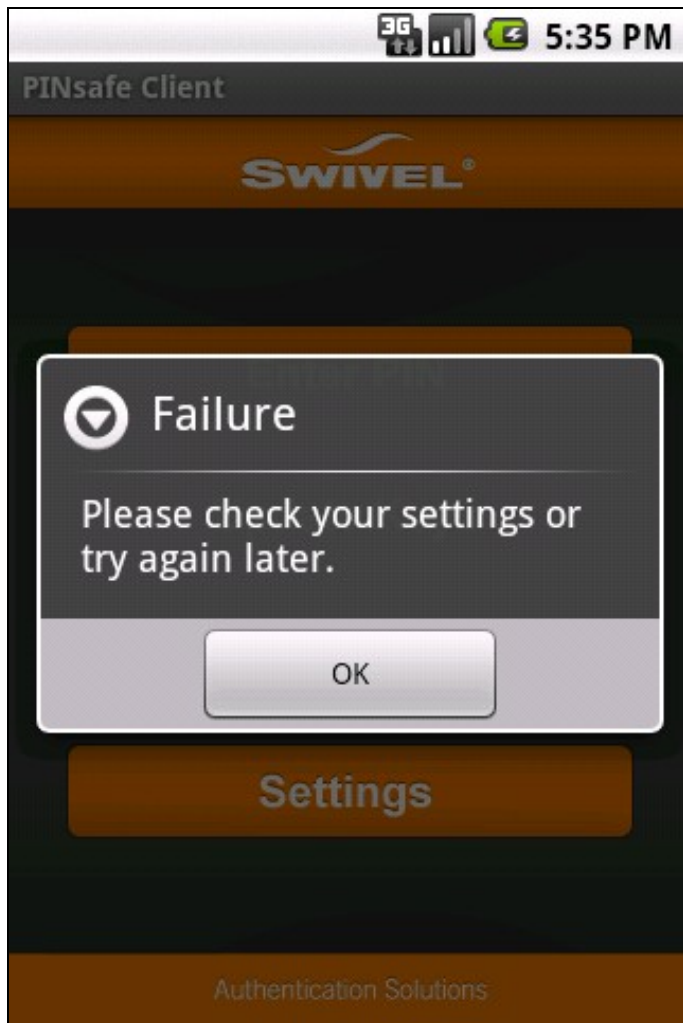
Message Connection to http://IP_or_Hostname:8080 refused

The IP address, hostname, or port may be incorrect and the server has refused to allow a connection from the client



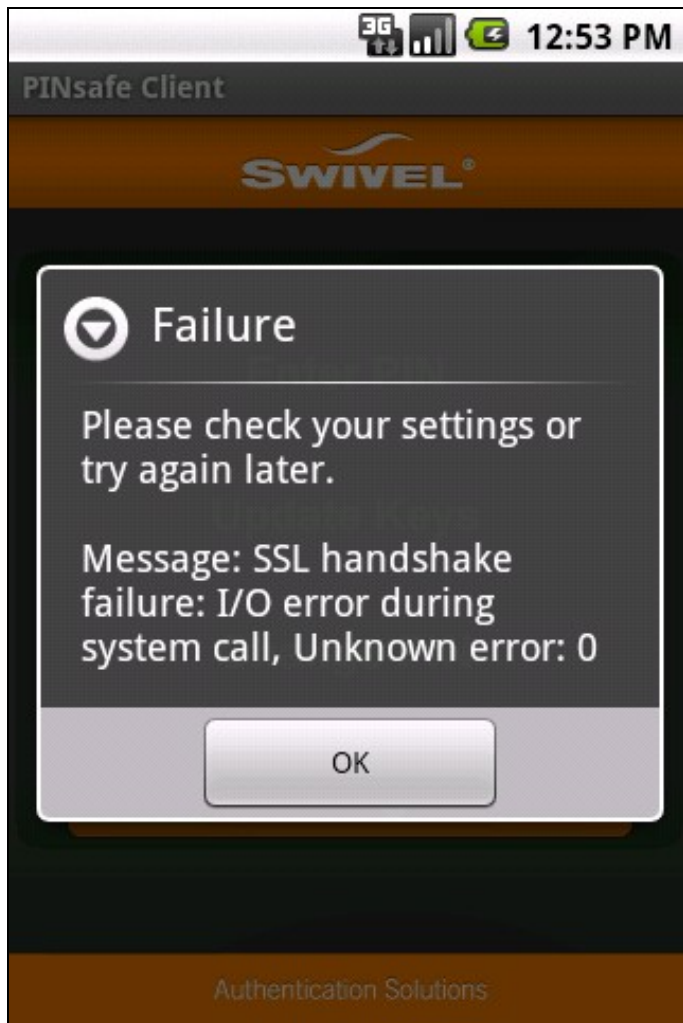
Failure Please check your settings or try again later

This can be caused by a Swivel Android Client configured to use Swivel 3.7 accessing Swivel version 3.8.



Message: SSL handshake failure: I/O error during system call, Unknown error: 0

This is caused by an SSL request being made against a non SSL server, check the Swivel Android Client Settings.



Failure Please check your settings or try again later Message: com.android.org.bouncycastle.jce.exception.ExtCertPathValidatorException: Could not validate certificate: current time: Tue Jun 19 11:54:52 GMT+01:00 2012, expiration time: Thu Mar 03 23:59:59 GMT 2011

SSL Certificate has expired. Install a valid certificate on the Swivel server.

AGENT_ERROR_NO_SECURITY_STRINGS, AGENT ERROR NO SECURITY STRINGS

See [AGENT ERROR NO SECURITY STRINGS](#)

10 Tested Mobile Phones

The following phones have been tested

Mobile Phone Compatibility

Manufacturer	Model	Version	OS Version	Operator	Compatible Y/N	Applet Version
Samsung	Galaxy	i9100	Android 2.3.3	O2	Y	1
Samsung	Galaxy	i9100	Android 2.3.3	O2	Y	2
Samsung	Galaxy	i9100	Android 4.0.3	O2	Y	2
Samsung	Galaxy	Note GF-7000	Android Ice Cream Sandwich 4.0.2	-	Y	2
Samsung	Galaxy	Mega GT - I9205	Android 4.2.2	O2	Y	-
Samsung	Galaxy	GT - I9195	Android 4.2.2	EE	Y	-

Keywords: Android, Client, Swivlet, App, marketplace

11 Android 2.0

12 Swivel Android 2.x App Overview

Swivel Secure now offers a Android mobile client for use with the Swivel platform. This article explains how to download, configure and use this client. For other phones see [Mobile Phone Client](#) for earlier versions.

13 Requirements

Swivel 3.10 or later

Android OS

The Swivel virtual or hardware appliance must be reachable from the mobile phone to receive security strings

The index is required to be entered as nn on the end example: 292401, Swivel versions earlier than 3.10 require ,nn example: 2924,01 otherwise it will see it as a dual channel authentication.

Valid certificate on the Swivel server or non SSL, but not a self signed certificate

14 Versions

Swivel Mobile Version 2.1.2 released: 05/02/2014

Version 2.1.1 released: 05/01/2014

- QR Code Provision
- Push Authentication Support
- Fix for Android 4.4.4

Version 2.0 released (Swivel 3.10 or later)

- Simple User Interface
- Extra Mobile Policies
- Help Section
- Citrix Receiver VPN Client support (iPhone Only)
- Removal of comma from OTC

14.1 Which version do I need?

Swivel version 3.10 or later,

Android Mobile Client 2.1

15 Swivel Server Configuration

15.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance

To allow a user to authenticate using a One Time Code from a mobile app, the user must have Mobile app authentication enabled. To do this on the Swivel Administration console ensure that the group they are part of has access to the Mobile Client under Repository Groups.

15.2 Configuring the Swivel Authentication

Swivel can authenticate users using the mobile client to authenticate by RADIUS or Agent-XML authentication

- For RADIUS authentication see [RADIUS Configuration](#) Note: The access device must be configured to use PAP for authentication.
- For Agent-XML authentication see [XML Authentication Configuration](#)

Allow user to browse strings: Options Yes/No, Default No. Version 3.9.6 onwards. This option allows the Mobile Phone App user to browse through the security strings. Availability to this feature is server controlled.

15.2.1 Mobile Client Policies

For the Server based policies see [Mobile Client Policies 2.0](#) for previous versions see [Mobile Client Policies](#)

16 Swivel Mobile Application Installation

The Swivel Mobile Phone Client 2 is available from the App store (see versions above). You can click the link to the and install from a web browser, or follow the instructions in this article to navigate to the App within the App Store.

17 Swivel Mobile Application Configuration

A user may use one of the following methods to provision a mobile device:

17.1 URL Provisioning

Provision URL Swivel 3.10 onwards

17.2 QR Code Provisioning

QR Code Provision Swivel 3.10.4 onwards

17.3 Get Server Settings

If an SSD server is being used, select **Get Server Settings** and enter the Server ID.

17.4 Manual Configuration

Manual entry may not be possible depending upon Swivel server policy

The settings are:

1. Username: Your username that you use when you authenticate via Swivel
1. Server: The URL from where the client can download security strings (or keys)
1. Context: The context used by the web service. For a virtual or hardware appliance this is **proxy**, for a software install this is usually **pinsafe**
1. Port: The port number used by the web service. For an virtual or hardware appliance this is **8443**, for a software install this is **8080**
1. SSL: SSL settings

Once you have entered the settings you can select Submit in the header location of that page.

Saving screenshot...

Back Settings Submit

Automatic Setting >

Username: username

Server: server

Context: context

Port: port

SSL: OFF

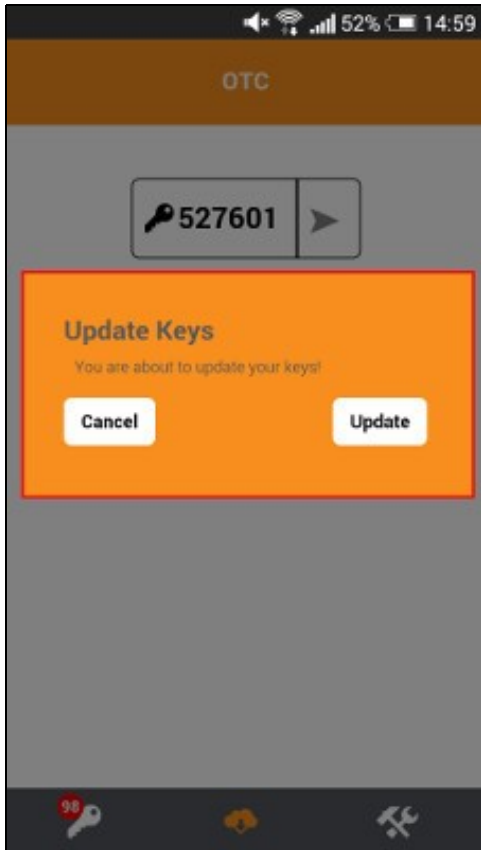
18 Downloading Security Strings or OTC

From the bottom menu there is a update keys button, pressing this will get you a new set of 99 security strings. This will attempt to retrieve **Security Strings** or **OTC** from the Swivel server.

If there are any problems and error message will be displayed

You can confirm that keys have been downloaded by checking the Swivel server logs

The Swivel server will display the following log message **Security strings fetched for user: username**



19 Swivel Client Policies

Policies may be hidden from view by the Swivel server settings.

The following options are available:

PIN Entry Whether the PIN can be entered or not to auto extract the OTC

Select String Allow String Browsing, This is a Swivel server controlled option, which if enabled will allow the user to browse through security strings on the mobile app.

Number Pad A number pad is displayed for the PIN entry

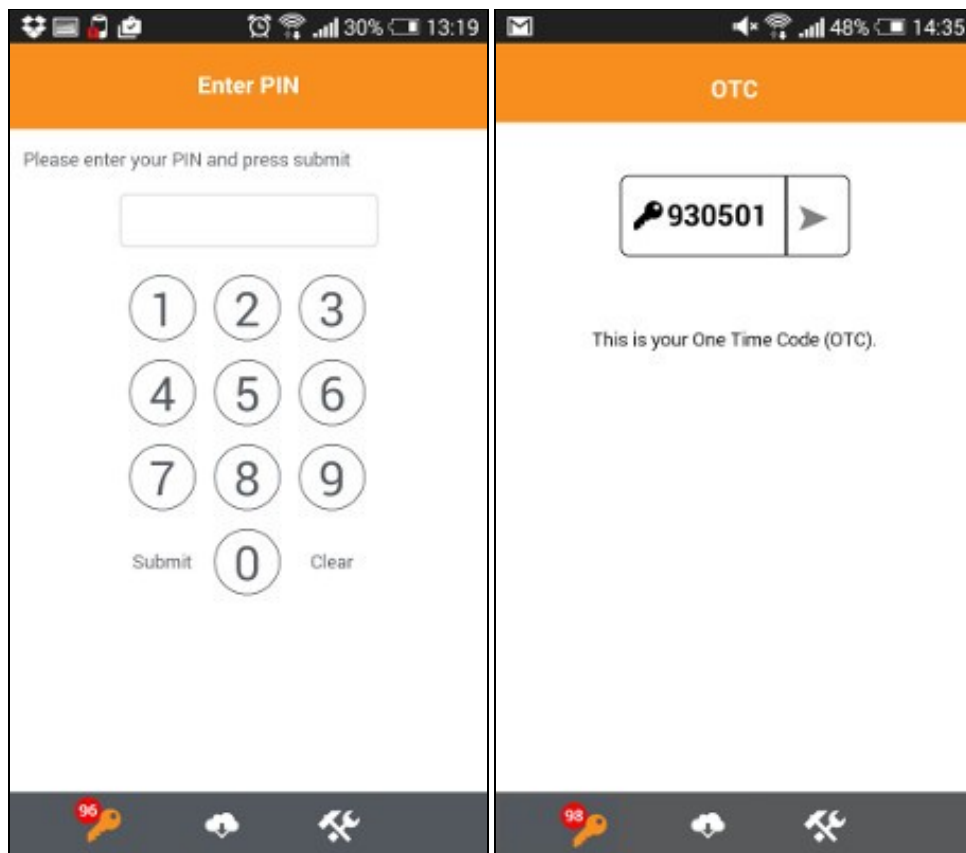
Notifications Support Used for the [OneTouch](#) Mobile.

19.1 Authenticating with Swivel Mobile Phone Clients

To use the Swivel Mobile Phone Clients to authenticate is very simple.

1. Open the Swivel Mobile Phone Client.
2. Select the key icon on the bottom menu.
3. Depending on your policy settings you will either be prompted for a PIN or immediately shown a One-Time-Code [OTC](#).
4. If you are asked for a PIN, enter the PIN number previously sent during the enrolment phase.
5. Enter the OTC into the authentication dialogue, make sure you enter all the characters.

If you need to authenticate again you can select the '<' or '>' button and a new string will be displayed (you may have to enter your PIN again).



19.2 Updating Keys

The Swivel Mobile Phone Client downloads 99 keys at a time and these keys are used one at a time until there are none left. However a new set of 99 keys can be downloaded at any time by selecting Update Keys. Downloading keys requires network connectivity so it is recommended that you download a new set of keys before the Android is likely to be without network connectivity for any length of time.

20 Known Issues

20.1 Android version 4.4.4

The 4.4.4 Operating System of Android has functionality issues with the Swivel Mobile Client 2.0 upgrade to the Swivel Mobile Client 2.10 overcome this.

A work around exists if it is not possible to upgrade:

In order to install the file [SwivelMobile-debug.apk](#) please connect your mobile via usb to your computer to place the attached file onto your phones file system, then use a file manager application <https://play.google.com/store/apps/details?id=com.mobisystems.fileman&hl=en> - Once you have the file loaded onto your phone on the internal storage then just navigate to it using file manager application and then double click and it will launch.

21 Troubleshooting

- Is the Swivel server accessible on the internet
- Check the connection settings to the Swivel server
- Check the Swivel logs for any error messages
- Can the phone access the internet
- If a RADIUS connection is seen from the access device to the Swivel server but authentication fails, try using PAP
- Download new security strings to the phone and retest
- Is the pin 6 characters when you only entered a 4 digit pin? If yes then enter all of the numbers you see on screen (the extra 2 are used as an index).
- Login fails and User receives a security string or One Time Code by SMS or email at each login attempt. Again make sure you are entering all of the numbers shown on screen.
- If the proxy port (8443) on the virtual or hardware appliance is being used, ensure that it supports the proxy request of the key retrieval using AgentXML. If this is the case then contact Support for an updated version of the Proxy.

21.1 Error Messages

Incorrect settings - please check your settings

The settings for downloading the security strings are incorrect. Verify what has been entered, and check what the values should be.

Timed Out

The settings for connecting to the Swivel server may be incorrect or the port is being blocked.

AGENT_ERROR_NO_SECURITY_STRINGS, AGENT ERROR NO SECURITY STRINGS

See [AGENT ERROR NO SECURITY STRINGS](#)

22 Tested Mobile Phones

The following phones have been tested

Mobile Phone Compatibility

Manufacturer	Phone Model	Kernel Version	Android Version	Operator	Compatible Y/N
Android	Galaxy S5 SM-G900F	3.4.0-3624618 +	5.0	O2	Y
Android	Galaxy S4 GT-I9505	3.4.0-481100 +	4.4.4	O2	Y
Android	Galaxy S4 GT-I9505	3.4.0-481100 +	4.4.2	O2	Y
Android	-	3.2 +	-	Orange	Y
Android	-	3.2 +	-	O2	Y
Android	-	3.2 +	-	Vodafone	Y

- The current version only supports one device per user.

Keywords: Android, Security, Tokens, Android App,

23 Category:Blackberry

24 Blackberry

25 Overview

For Verion 2 of the Swivel Blackberry App see [Blackberry 2.0](#).

The Swivel Mobile Phone Client allows 99 security strings or One Time Codes for PINless authentication to be stored on the Blackberry. These can be updated at any time from the client.

For Blackberry Devices of OS Version 4.5 and later a Blackberry Client app exists as described below. For earlier devices the Swivel app can be installed; please refer to the [Swivlet How To Guide](#)

There are two versions of the Blackberry Mobile Phone client one for Versions 3.8 and later and one for earlier versions.

This article covers the Blackberry client for Swivel, for other phones see [Mobile Phone Client](#).

26 Prerequisites

- On the Swivel Administration Console the user must have Swivlet or Mobile Client enabled to use the Java Applet (or other Mobile Client App)
- The Swivel server must be reachable from the mobile phone to receive security strings
- The index is required to be entered as nn on the end example: 292401, Swivel versions earlier than 3.10 require ,nn example: 2924,01 otherwise it will see it as a dual channel authentication.
- Where SSL communications are used the server must have a valid certificate for the hostname. If a self signed certificate is used it would need to be installed on the handset.
- RADIUS authentications made against Swivel must use PAP RADIUS authentication since with other RADIUS protocols such as CHAP and MSCHAP the access device requests the OTC from Swivel.
- Virtual or hardware appliances using Swivel 3.8 may require an upgrade on their proxy to provision a mobile device, see [Appliance Proxy Server Upgrade](#)
- Swivel 3.8 requires the mobile phone to be provisioned before use, see [Mobile Provision Code](#)

27 Versions

Swivel Blackberry Mobile Client 1.7.1 (Awaiting App Store release, available for the Blackberry Enterprise Server as file download (see below))
23/02/2015

- Supports Quick provision
- Requires Swivel 3.8 to 3.10

Swivel Blackberry Mobile Client 1.6 release 05/12/2013 (please note this is labelled as version 3.0)

- You can now "Get Server Settings" and provision the device using a URL from a text message
- It is possible for the server to allow users to navigate through the security strings backwards as well as forwards
- Several UI/UX improvements

Swivel Blackberry Mobile Client 1.6

- Added a "Get Server Settings" screen where users can use a 10-digit code they have been given to download the server settings
- Added server configurable ability to automatically extract otc prompting user for PIN

28 Swivel Configuration

28.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance

To allow a user to authenticate using a One Time Code from the Mobile Phone Client, the user must have the Mobile Client authentication enabled. To do this on the Swivel Administration console ensure that the group they are part of has access to the Mobile Client under Repository Groups.

28.2 Configuring the Swivel Authentication

Swivel can authenticate users using the mobile client to authenticate by RADIUS or Agent-XML authentication

- For RADIUS authentication see [RADIUS Configuration](#) Note: The access device must be configured to use PAP for authentication.
- For Agent-XML authentication see [XML Authentication Configuration](#)

28.2.1 Mobile Provisioning

Swivel 3.8 and higher requires each mobile phone to be provisioned so it can be uniquely identified. Ensure that all Mobile Client users have suitable Transports configured to receive their Provision Code. To provision the mobile client select the user and click Re-provision. Earlier versions of Swivel do not need to use a Mobile Provision Code. See [Mobile Provision Code](#).

28.2.2 Mobile Client Policies

For the Server based policies see [Mobile Client Policies](#)

29 Installing the Client

There are a number of ways to install the client. Via Blackberry App World is the recommended approach.

All the files required for either method are available here [Blackberry Software](#)

29.1 Via Blackberry App World

After logging into the Blackberry App World search for Swivel. The version of the app created by Swivel Secure Ltd is the correct version. Install this. Updates should be managed through the App World application.

29.2 Over the air

To install the client over-the-air you need to use the browser on your blackberry device and navigate to the location of the client .jad file.

This will instigate the download and installation of the client.

You may be prompted to allow the application "trusted status". You should respond Yes to this. You do not need to edit the applications permissions.

You can place the files required to perform OTA provision on a web-server of your choosing or you can install the client from the demo site.

<https://demo.swivelsecure.com/Rim/PinsafeClient.jad>

If you wish to use the client with Swivel 3.7 or older, you can use a version that is backward compatible.

<https://demo.swivelsecure.com/Rim/pre38/PinsafeClient.jad>

When used in conjunction with pre 3.8 versions, there is no requirement to provision the client

29.3 Blackberry Desktop

It is also possible to install the application via the Blackberry Desktop software.

For this you need to extract the application. From the desktop software select import and then select the .alx file.

However the .alx file may need to be edited to reflect your device Java and OS version.

29.4 Blackberry Enterprise Server

The software for the Blackberry Enterprise can be downloaded here | [Swivel BB Mobile Client 1.7.1.zip](#)

30 Navigation

You can navigate either using the selectable buttons on the user-interface or the menus. Certain devices lend themselves to different methods.

To get back to the main screen from any other screen use the cancel option.



31 Configuration



Before you can provision the client you need to configure it.

If a **SSD** server is being used, then select **Get Server Settings** and enter the Server ID, otherwise the settings can be manually entered with information from the Swivel System administrator.

The manual configuration screen has the following entries:

Debug This is a message field that shows the last error encountered or action completed relating to the client attempting to connect to the Swivel server. It is a read-only field

Username As recognised by the Swivel Authentication Platform

Server The host name of the Swivel Authentication Platform as accessible by the client. **nb** No http:// or https:// prefix required.

Context The context or path the client should use on the host to be able to communicate with the platform. For virtual or hardware appliances this would be proxy by default.

Port The port the client should use on the host to be able to communicate with the platform. For virtual or hardware appliances this would be 8443 by default.

SSL Is SSL communication required. Default is yes for virtual or hardware appliances.

PINless Is the user a PINless user.

Once these settings are complete the client can be provisioned.

If using in pre version 3.8 client there will be no debug field but there will be a pre38 setting which must be selected to use the client with a pre 3.8 version.

If pre38 is set then there is no need to provision the client.

32 Provisioning

In order to provision the client you need to obtain a provision code. This will usually be sent to you by the administrator of your Swivel Platform or you maybe able to request one to be sent. A provision code is a 10 character code that you enter on the provision screen. Once you enter the code and select provision, the client will contact the platform and if the code is valid you device will be provisioned. See also [Mobile Provision Code](#).

33 Downloading Strings

To download security strings select the refresh option.

34 Authentication

To authenticate using the client select the authenticate option. This will then display the security string you need to use to authenticate. Note the actual format you need to enter into the login-form is 1234nn or Swivel version prior to 3.10 1234,nn where 1234 represents your one-time code and nn represents the string index.

35 Troubleshooting

Login fails and User receives a security string or One Time Code by SMS or email at each login attempt. The index is required to be entered as nn or ,nn example 2924,01 otherwise it will see it as a dual channel authentication.

If the login continues to fail, try subtracting 1 from the security string index, example for 7432,32 try 7432,31.

35.1 Error Messages

AGENT_ERROR_NO_SECURITY_STRINGS, AGENT ERROR NO SECURITY STRINGS

See [AGENT ERROR NO SECURITY STRINGS](#)

net.rim.device.cldc.io.ssl.TLSIOException (net.rim.device.api.crypto.tls.TLSAlertException

When configuring the Blackberry App with an SSL connection, the hostname for the Swivel servers public IP should be used rather than the IP address.

HTTP error 0 ()

Ensure that the option to use SSL is enabled if HTTPS is being used.

36 Known Issues

Blackberry only support HTTP and not HTTPS for the [Provision URL](#).

37 Tested Mobile Phones

The following phones have been tested

Mobile Phone Compatibility

Manufacturer	Model	Version	Operator	Compatible Y/N	Client Version
Blackberry	Curve 8520	v4.2.0.135	O2	Y	1.0.1
Blackberry	Curve 8900	(Emulator)	N/A	Y	1.0.1
Blackberry	9300	v6.6.0.195	Not Known	Y	Not Known
Blackberry	9300	v6.6.0.207	Not Known	Y	Not Known
Blackberry	Torch 9810	v6	O2	Y	1.0.1
Blackberry	Q10	-	-	Y	2.0.x
Blackberry	Z10	-	-	Y	2.0.x

38 Blackberry 2.0

39 The Swivel Blackberry 2.0 App Overview

Swivel Secure now offers a Blackberry mobile client for use with the Swivel platform. This article explains how to download, configure and use this client. For other phones see [Mobile Phone Client](#) for earlier versions.

40 Requirements

Swivel 3.10 or higher

Blackberry 10 OS. (For older Blackberry versions see [Blackberry](#))

The Swivel virtual or hardware appliance must be reachable from the mobile phone to receive security strings

The index is required to be entered as nn on the end example: 292401, Swivel versions earlier than 3.10 require ,nn example: 2924,01 otherwise it will see it as a dual channel authentication.

Valid certificate on the Swivel server or non SSL, but not a self signed certificate

41 Versions

Swivel Mobile version 2.1.3.1 released 17/02/2015

Swivel Beta version 2.1.1 released: 05/02/2014

- **QR Code Provision**
- Push Authentication Support

version 2.0 released

- Simple User Interface
- Extra Mobile Policies
- Help Section
- Citrix Receiver VPN Client support (iPhone Only)
- Removal of comma from OTC,

41.1 Which version do I need?

Pinsafe version 3.10 or later, Mobile Client 2.0

Blackberry Mobile Client 2.0 version 2.0

42 Swivel Configuration

42.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance

To allow a user to authenticate using a One Time Code from a mobile app, the user must have Mobile app authentication enabled. To do this on the Swivel Administration console ensure that the group they are part of has access to the Mobile Client under Repository Groups.

42.2 Configuring the Swivel Authentication

Swivel can authenticate users using the mobile client to authenticate by RADIUS or Agent-XML authentication

- For RADIUS authentication see [RADIUS Configuration](#) Note: The access device must be configured to use PAP for authentication.
- For Agent-XML authentication see [XML Authentication Configuration](#)

Allow user to browse strings: Options Yes/No, Default No. Version 3.9.6 onwards. This option allows the Mobile Phone App user to browse through the security strings. Availability to this feature is server controlled.

42.3 Mobile Provisioning

Swivel 3.8 and higher requires each mobile phone to be provisioned so it can be uniquely identified. Ensure that all Mobile Client users have suitable Transports configured to receive their Provision Code. To provision the mobile client select the user and click Re-provision. Earlier versions of Swivel do not need to use a Mobile Provision Code. See [Mobile Provision Code](#).

42.3.1 Mobile Client Policies

For the Server based policies see [Mobile Client Policies 2.0](#) for previous versions see [Mobile Client Policies](#)

43 Swivel Mobile Application Installation

The Swivel Mobile Phone Client 2 is available from the App store (see versions above). You can click the link to the and install from a web browser, or follow the instructions in this article to navigate to the App within the App Store.

44 Swivel Mobile Application Configuration

A user may use one of the following methods to provision a mobile device:

44.1 URL Provisioning

Provision URL Swivel 3.10 onwards

44.2 QR Code Provisioning

QR Code Provision Swivel 3.10.4 onwards

44.3 Get Server Settings

If an SSD server is being used, select **Get Server Settings** and enter the Server ID.

44.4 Manual Configuration

Manual entry may not be possible depending upon Swivel server policy

The settings are:

1. Username: Your username that you use when you authenticate via Swivel
1. Server: The URL from where the client can download security strings (or keys)
1. Context: The context used by the web service. For a virtual or hardware appliance this is **proxy**, for a software install this is usually **pinsafe**
1. Port: The port number used by the web service. For an virtual or hardware appliance this is **8443**, for a software install this is **8080**
1. SSL: SSL settings

Once you have entered the settings you can select Submit in the header location of that page.

Back Settings Submit

Username: syed

Server: 192.168.11.114

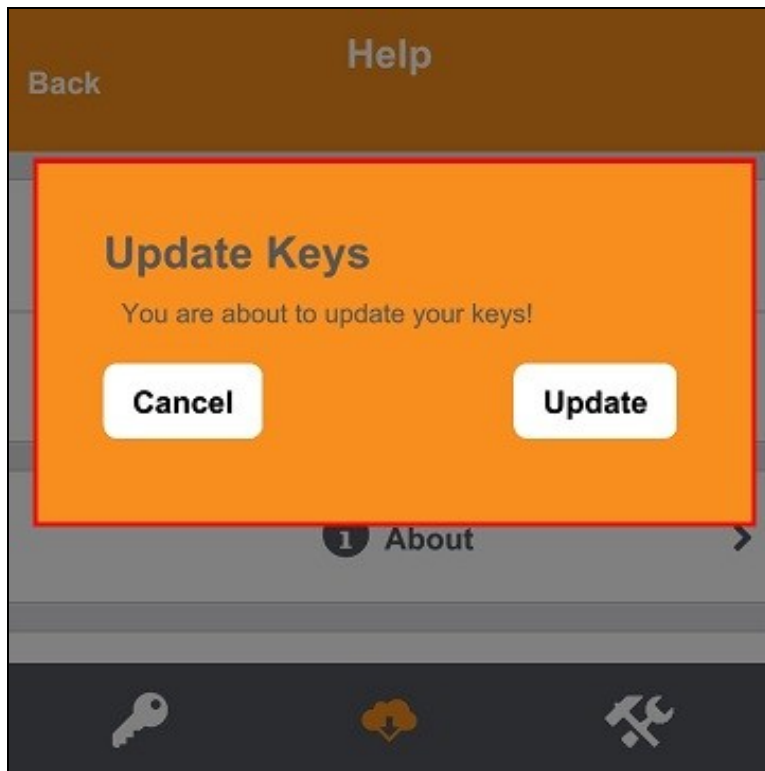
Context: pinsafe

Port: 8080

SSL OFF

44.5 Downloading Security Strings

From the bottom menu there is a update keys button, pressing this will get you a new set of 99 security strings. This will attempt to retrieve Security Strings from the Swivel server.



If there are any problems and error message will be displayed

You can confirm that keys have been downloaded by checking the server logs

The Swivel server will display the following log message **Security strings fetched for user: username**

44.6 Options

The following options are available:

Auto extract OTC, Prompt for PIN Number to auto-extract OTC, Options, enable/disable. This option may be turned off on the Swivel server. When enabled this allows the user to enter their PIN number and a One Time Code will be displayed. Note that there is no error checking of the PIN, so if an incorrect PIN is entered an incorrect One Time Code will be displayed.

Allow String Browsing, This is a Swivel server controlled option, which if enabled will allow the user to browse through security strings on the mobile app.

Provision is numeric, allows the keyboard type to be either alpha numeric of numeric depending on the users provision code type.

Set Support Email Address. Set Support Phone Number. Set VPN client URL.

44.7 Authenticating with app

To use the Swivel Blackberry app to authenticate is very simple.

1. Open the app. on your Blackberry.
2. Select the key icon on the bottom menu.
3. Depending on your policy settings you will either be prompted for a PIN or immediately shown a One-Time-Code (OTC).
4. If you are asked for a PIN, enter the PIN number previously sent during the enrollment phase.
5. Enter the OTC into the authentication dialogue, make sure you enter all the characters.

If you need to authenticate again you can select the '<' or '>' button and a new string will be displayed (you may have to enter your PIN again).

Enter PIN

ALT

Please enter your PIN and press submit

....|

Submit

Key icon, Cloud icon, Wrench icon

OTC

< 523905 >

This is your One Time Code (OTC).

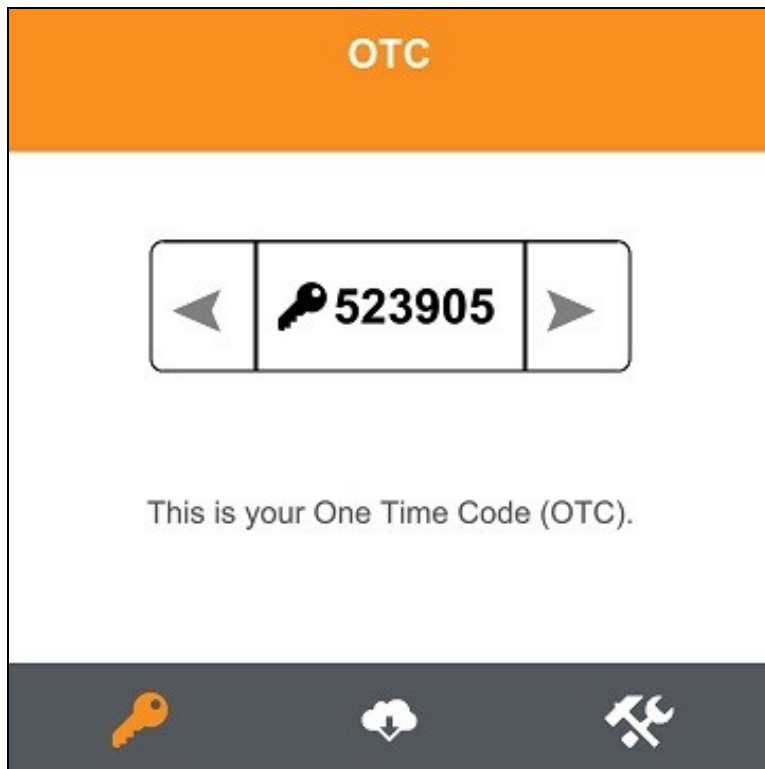
Key icon, Cloud icon, Wrench icon

44.8 Authenticating with app and Swivel

To use the Swivel Blackberry app to authenticate is very simple.

1. Open the app on your Blackberry.
2. Select the key icon on the bottom menu.
3. The client will show a security string with a row of placeholders 1234567890 below it.
4. Use your PIN to extract your One-Time-Code (OTC), eg if your PIN is 2468 take the 2nd 4th 6th and 8th characters of the security string.
5. In the example screen shoot the OTC would be: 1825.
6. After the OTC has been worked out, you will also need to ensure you type in the last two characters shown (the index).
7. Using the example screen shot you would type 182512.

If you need to authenticate again you can select the '<' or '>' button and a new string will be displayed.



44.9 Updating Keys

The client downloads 99 keys at a time and these keys are used one at a time until there are none left. However a new set of 99 keys can be downloaded at any time by selecting Update Keys. Downloading keys requires network connectivity so it is recommended that you download a new set of keys before the Blackberry is likely to be without network connectivity for any length of time.

45 Known Issues

The Blackberry App version 2.0 may incorrectly display its version as 3.0

When using PIN entry and the app is started, the key symbol should be pressed before entering the PIN, otherwise it will use the previous OTC, which will work on the first authentication but fail on subsequent authentications.

46 Troubleshooting

- Is the Swivel server accessible on the internet
- Check the connection settings to the Swivel server
- Check the Swivel logs for any error messages
- Can the phone access the internet
- If a RADIUS connection is seen from the access device to the Swivel server but authentication fails, try using PAP
- Download new security strings to the phone and retest
- Is the pin 6 characters when you only entered a 4 digit pin? If yes then enter all of the numbers you see on screen (the extra 2 are used as an index).
- Login fails and User receives a security string or One Time Code by SMS or email at each login attempt. Again make sure you are entering all of the numbers shown on screen.
- If the proxy port (8443) on the virtual or hardware appliance is being used, ensure that it supports the proxy request of the key retrieval using AgentXML. If this is the case then contact Support for an updated version of the Proxy.

46.1 Error Messages

Incorrect settings - please check your settings

The settings for downloading the security strings are incorrect. Verify what has been entered, and check what the values should be.

Timed Out

The settings for connecting to the Swivel server may be incorrect or the port is being blocked.

AGENT_ERROR_NO_SECURITY_STRINGS, AGENT ERROR NO SECURITY STRINGS

See [AGENT ERROR NO SECURITY STRINGS](#)

47 Tested Mobile Phones

The following phones have been tested

Mobile Phone Compatibility

Manufacturer	Model	Version	Operator	Compatible Y/N
Blackberry	Q10	-	Orange	Y
Blackberry	Q10	-	O2	Y
Blackberry	Q10	-	Vodafone	Y

- The current version only supports one device per user.

Keywords: Blackberry, Q10, BB World, Blackberry App, AppStore, Apple, iPad

48 Legacy

Download compatible with Swivel 3.10 and later.



49 Citrix Receiver

[[Category:android|A]]

50 Introduction

Citrix Receiver is a lightweight software client that allows access to virtual desktops and apps including Windows, Web or SaaS apps on any PC, Mac, netbook, tablet or smartphone.

For configuring Netscaler and Receiver to work with multiple authentication servers see [Citrix Netscaler configuration for Receiver](#)

51 Prerequisites

Citrix receiver Client

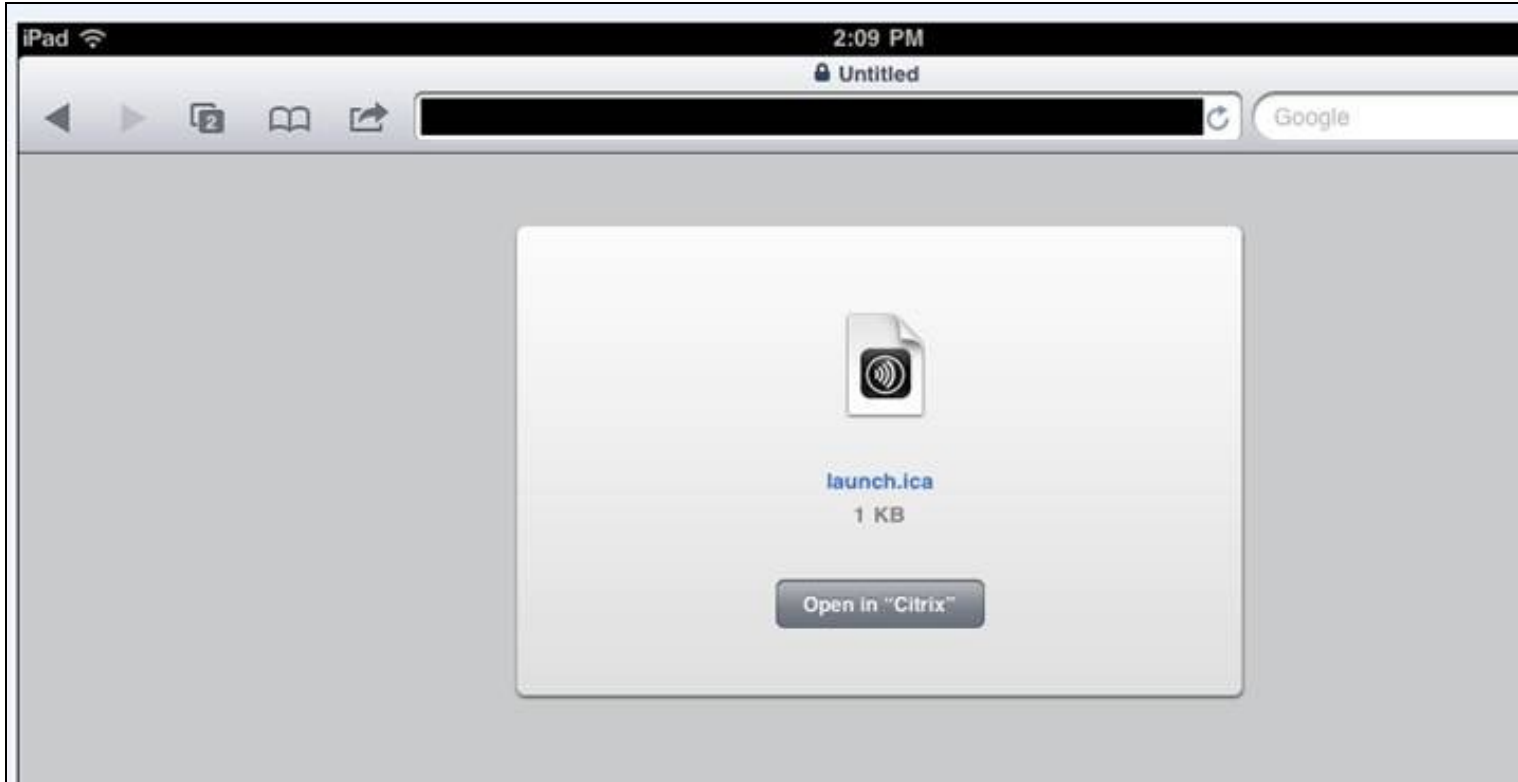
Swivel Appliance or Server

Citrix Gateway integrated with Swivel

52 iPhone / Android Citrix receiver

1. Open the **Safari** web browser on the iPad / **Mozilla Firefox** on Android Please see [Known Issues and Limitations](#)
2. Browse to the login page of the Citrix gateway
3. Enter username, password, and Swivel security string (Using TURING or SMS). Click login button.
4. Once the user is logged in go to the Citrix gateway, click on the Citrix application they want to launch (eg, the published desktop)
5. Here's where things are a little different from a PC. Instead of just launching the Citrix plug-in directly, the user will see the screen shot in the attachment. The user then clicks on the "Open in Citrix" button.
6. The Citrix receiver app will launch and allow the user to access the selected Citrix app

The latest version of the Citrix Receiver supports Third-Party Authentication support for the iOS and Android platform allowing the configuration data to be retrieved from a Citrix gateway URL, so there is no Swivel configuration required on the directly within the Receiver app.



53 Citrix Netscaler RADIUS authentication for Receiver

For configuring Netscaler and Receiver to work with multiple authentication servers see [Citrix Netscaler configuration for Receiver](#)

54 Citrix Access Standard Edition Gateway RADIUS authentication for Receiver

The following article describes adding RADIUS authentication to the Citrix Access Standard Edition for Citrix Receiver. The RADIUS authentication needs to be set as the primary authentication and AD as the Secondary authentication.

<http://support.citrix.com/article/CTX121093>

55 Citrix Access Advanced Edition Gateway RADIUS authentication for receiver

The following article describes adding RADIUS authentication to the Citrix Access Advanced Edition for Citrix Receiver.

<http://cdn.ws.citrix.com/wp-content/uploads/2009/08/iphone-receiver-admin.pdf>

56 Known Issues and Limitations

It has been observed by our customers that the Citrix Receiver only launches successfully on the Android platform when accessing links via the Mozilla Firefox browser (at the time this article was written)

57 2.0 Mobile Clients Administration

58 The Swivel iPhone App v2 Overview

Swivel Secure now offers a new and improved iPhone and iPad client for use with the Swivel platform. This article explains how to download, configure and use this client. For other phones see [Mobile Phone Client](#).

59 Requirements

iPhone, 4S, 5, 5C and 5S

The Swivel virtual or hardware appliance must be reachable from the mobile phone to receive a [Security string](#)

Security strings must be entered as seen on the screen (previous versions had a comma to seperate the index and number, this has been removed from this version)

Virtual or hardware appliances using Swivel 3.10 may require an upgrade on their proxy to provision a mobile device, see [Appliance Proxy Server Upgrade](#)

60 Versions

version 2.0 BETA release around 1st May 2014

- Navigate back and forward through security strings
- URL provisioning

60.1 Which version do I need?

Swivel version 2.0, 1st May 2014. For Swivel version 3.10, iOS 5.0 or later

61 Swivel Configuration

61.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance

To allow a user to authenticate using a One Time Code from a mobile app, the user must have Mobile app authentication enabled. To do this on the Swivel Administration console ensure that the group they are part of has access to the Mobile Client under Repository Groups.

61.2 Configuring the Swivel Authentication

Swivel can authenticate users using the mobile client to authenticate by RADIUS or Agent-XML authentication

- For RADIUS authentication see [RADIUS Configuration](#) Note: The access device must be configured to use PAP for authentication.
- For Agent-XML authentication see [XML Authentication Configuration](#)

Allow user to browse strings: Options Yes/No, Default No. Version 3.9.6 onwards. This option allows the Mobile Phone App user to browse through the security strings. Availability to this feature is server controlled.

Provision Number Is Numeric: Options Yes/No, Default No. Version 3.10 onwards. This option allows the Mobile Phone App user to set the keyboard input type for the provision ID field. Availability to this feature is server controlled.

Sync Index: Options Yes/No, default No. Version 3.10.2. Version 3.10.2 onwards. When set to yes a check is made when the next [Security string](#) or [One Time Code](#) is requested from the App, if it has not been used, then it will not show the next available value. If set to No, the user can go to the next whether the previous has been used or not.

Support Email Address: Options String Data, Default "". Version 3.10 onwards. This option allows the Admin to set a support email address so that the mobile client can be pre-configured to email the support desk. Availability to this feature is server controlled.

Support Phone Number: Options String Data, Default "". Version 3.10 onwards. This option allows the Admin to set a support phone number so that the mobile client can be pre-configured to phone the support desk. Availability to this feature is server controlled.

VPN URL Scheme: Options String Data, Default "". Version 3.10 onwards. This option allows the Admin to set a vpn url so that the vpn client can be launched directly from the mobile app. Availability to this feature is server controlled.

61.3 Mobile Provisioning

Swivel 3.10 and higher requires each mobile phone to be provisioned so it can be uniquely identified. Ensure that all Mobile Client users have suitable Transports configured to receive their Provision Code. To provision the mobile client select the user and click Re-provision. Earlier versions of Swivel do not need to use a Mobile Provision Code. See [Mobile Provision Code](#).

61.3.1 Mobile Client Policies

For the Server based policies see [Mobile Client Policies](#)

62 iPhone Installation and Configuration

The Swivel iPhone iClient is available from the Apple App Store. You can click the icon below to open the App within iTunes, or follow the instructions in this article to navigate to the App within the App Store.

62.1 Download compatible with Swivel 3.8 onwards



62.2 Configuring the app

When you launch the app you will see the bottom navigation screen this will allow you to browse the menu options available, from here you can choose the server settings and enter the server ID you have been emailed.

62.2.1 Get Server Settings

If a **SSD** server is being used, then select **Server Settings** and enter the Server ID, otherwise the settings can be manually entered with information from the Swivel System administrator. You can reach the manual setting from the server settings page.



The settings are

1. User Your username that you use when you authenticate via Swivel
2. Webservice URL The URL from where the client can download security strings (or keys)
3. Webservice Port The port number used by the web service. For an virtual or hardware appliance this is **8443**, for a software install this is **8080**
4. Webservice Context The context used by the web service. For a virtual or hardware appliance this is **proxy**, for a software install this is usually **pinsafe**

Once you have entered the settings you can select Submit.

62.3 Mobile Provision Code

Swivel versions 3.10 and higher require each Mobile device to be Provisioned with a Code sent from the Swivel server. To provision a phone see [Mobile Provision Code](#).

62.4 Downloading Security Strings

From the main menu where you can test the settings by Selecting the Update Keys option. This will attempt to retrieve Security Strings from the Swivel server.



If there are any problems and error message will be displayed

You can confirm that keys have been downloaded by checking the server logs

The Swivel server will display the following log message **Security strings fetched for user: username**

62.5 Options

The following options are available:

Auto extract OTC, Prompt for PIN Number to auto-extract OTC, Options, enable/disable. This option may be turned off on the Swivel server. When enabled this allows the user to enter their PIN number and a One Time Code will be displayed. Note that there is no error checking of the PIN, so if an incorrect PIN is entered an incorrect One Time Code will be displayed.

Allow String Browsing, This is a Swivel server controlled option, which if enabled will allow the user to browse through security strings on the mobile app.

62.6 Authenticating with app and PINsafe

To use the Swivel iPhone app to authenticate is very simple.

1. Open the app on your iPhone
2. Select Authenticate
3. The client will show a security string with a row of placeholders 1234567890 above it.
4. Use your PIN to extract your one-time code, eg if your PIN is 2468 take the 2nd 4th 6th and 8th characters of the Security String, 1870 in the example.
5. Enter the OTC into the authentication dialogue, including the ',' and the following 2 digits. e.g. 1870,02

If you need to authenticate again you can select the 'Next' button and a new string will be displayed



62.7 Updating Keys

The client downloads 99 keys at a time and these keys are used one at a time until there are none left. However a new set of 99 keys can be downloaded at any time by selecting Update Keys. Downloading keys requires network connectivity so it is recommended that you download a new set of keys before the iPhone is likely to be without network connectivity for any length of time.

63 Troubleshooting

- Is the Swivel server accessible on the internet
- Check the connection settings to the Swivel server
- Check the Swivel logs for any error messages
- Can the phone access the internet
- If a RADIUS connection is seen from the access device to the Swivel server but authentication fails, try using PAP
- Download new security strings to the phone and retest
- Is the OTC being entered with the comma and last two digits. E.g. 7329,62
- Login fails and User receives a security string or One Time Code by SMS or email at each login attempt. The index is required to be entered as nn on the end example: 292401, Swivel versions earlier than 3.10 require ,nn example: 2924,01 otherwise it will see it as a dual channel authentication.
- If the proxy port (8443) on the virtual or hardware appliance is being used, ensure that it supports the proxy request of the key retrieval using AgentXML. If this is the case then contact Support for an updated version of the Proxy.
- If you fail to authenticate successfully using the security string provided by the iPhone app please see [iPhone authentication fails](#)

63.1 Error Messages

Incorrect settings - please check your settings

The settings for downloading the security strings are incorrect. Verify what has been entered, and check what the values should be.

Timed Out

The settings for connecting to the Swivel server may be incorrect or the port is being blocked.

AGENT_ERROR_NO_SECURITY_STRINGS, AGENT ERROR NO SECURITY STRINGS

See [AGENT ERROR NO SECURITY STRINGS](#)

64 Tested Mobile Phones

The following phones have been tested

Mobile Phone Compatibility

Manufacturer	Model	Version	Operator	Compatible Y/N
Apple	5	7	-	Y
Apple	5	6.1.4	O2	Y
Apple	4	4.3.3	Vodafone	Y
Apple	3GS	4.0	Not Known	Y
Apple	3G	4.0	Deutsche Telekom	Y

The iPhone applet will also work on the iPad

65 Known Issues and Limitations

- The current version only supports one device per user.
- Currently only 4 digit PIN numbers are supported within the iPhone iClient (3.7 and earlier). This limitation does not affect the iPhone app Swivel 1.1 which is compatible with Swivel 3.8 onwards.
- iPhone Client 1.1 selecting the settings option will cause the iPhone client to be re-provisioned.
- iPhone Client 1.0 and 1.1 only support the use of number in the security string.
- iPhone Update to iOS7 is incompatible with version 1.4 and below of the Swivel mobile app. The application should update automatically but if not then you can update through the app store. (This limitation does not apply to the older Swivel mobile app)

Keywords: iPhone, iClient, Swivel, App, AppStore, Apple, iPad

66 Legacy

Download compatible with Swivel 3.7 and earlier



67 iPhone

68 The Swivel iPhone App Overview

This document covers the Swivel iPhone Client version 1, for Swivel versions up to 3.9.x. For Swivel version 3.10 onwards see [iPhone 2.0](#)

Swivel Secure now offers a iPhone and iPad client for use with the Swivel platform. This article explains how to download, configure and use this client. For other phones see [Mobile Phone Client](#).

69 Requirements

iPhone, 3, 4, 4S, 5, 5C and 5S

The Swivel virtual or hardware appliance must be reachable from the mobile phone to receive security strings

The index is required to be entered as nn on the end example: 292401, Swivel versions earlier than 3.10 require ,nn example: 2924,01 otherwise it will see it as a dual channel authentication.

Virtual or hardware appliances using Swivel 3.8 may require an upgrade on their proxy to provision a mobile device, see [Appliance Proxy Server Upgrade](#)

70 Versions

version 1.6 released 10 December 2013

- Navigate back and forward through security strings
- URL provisioning

70.1 Which version do I need?

Fro Swivel version 3.10 or higher see [IPhone 2.0](#)

Swivel version 1.6, 10th December 2013. For Swivel version 3.8 to 3.9, iOS 5.0 or later

PINsafe 1.1 (version 1.3) 5th June 2013, For Swivel version 3.8 to 3.9, iOS 3.0 to iOS 7

PINsafe iClient version 1.0, 02 June 2010, For Swivel versions up to and including 3.7, iOS 3.0 or later

71 Swivel Configuration

71.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance

To allow a user to authenticate using a One Time Code from a mobile app, the user must have Mobile app authentication enabled. To do this on the Swivel Administration console ensure that the group they are part of has access to the Mobile Client under Repository Groups.

71.2 Configuring the Swivel Authentication

Swivel can authenticate users using the mobile client to authenticate by RADIUS or Agent-XML authentication

- For RADIUS authentication see [RADIUS Configuration](#) Note: The access device must be configured to use PAP for authentication.
- For Agent-XML authentication see [XML Authentication Configuration](#)

Allow user to browse strings: Options Yes/No, Default No. Version 3.9.6 onwards. This option allows the Mobile Phone App user to browse through the security strings. Availability to this feature is server controlled.

71.3 Mobile Provisioning

Swivel 3.8 and higher requires each mobile phone to be provisioned so it can be uniquely identified. Ensure that all Mobile Client users have suitable Transports configured to receive their Provision Code. To provision the mobile client select the user and click Re-provision. Earlier versions of Swivel do not need to use a Mobile Provision Code. See [Mobile Provision Code](#).

71.3.1 Mobile Client Policies

For the Server based policies see [Mobile Client Policies](#)

72 iPhone Installation and Configuration

The Swivel iPhone iClient is available from the Apple App Store. You can click the icon below to open the App within iTunes, or follow the instructions in this article to navigate to the App within the App Store.

72.1 Download compatible with Swivel 3.8 to 3.9



72.2 Configuring the app

When you launch the app you will see the Configuration option on the main screen.

72.2.1 Get Server Settings

If a [SSD](#) server is being used, then select **Get Server Settings** and enter the Server ID, otherwise the settings can be manually entered with information from the Swivel System administrator.



The settings are

1. User Your username that you use when you authenticate via Swivel
2. Webservice URL The URL from where the client can download security strings (or keys)
3. Webservice Port The port number used by the web service. For an virtual or hardware appliance this is **8443**, for a software only install see [Software Only Installation](#)
4. Webservice Context The context used by the web service. For a virtual or hardware appliance this is **proxy**, for a software install this is usually **pinsafe**

Once you have entered the settings you can select Done.

72.3 Mobile Provision Code

Swivel versions 3.8 and higher require each Mobile device to be Provisioned with a Code sent from the Swivel server. To provision a phone see [Mobile Provision Code](#).

72.4 Downloading Security Strings

From the main menu where you can test the settings by Selecting the Update Keys option. This will attempt to retrieve Security Strings from the Swivel server.



If there are any problems and error message will be displayed

You can confirm that keys have been downloaded by checking the server logs

The Swivel server will display the following log message **Security strings fetched for user: username**

72.5 Options

The following options are available:

Auto extract OTC, Prompt for PIN Number to auto-extract OTC, Options, enable/disable. This option may be turned off on the Swivel server. When enabled this allows the user to enter their PIN number and a One Time Code will be displayed. Note that there is no error checking of the PIN, so if an incorrect PIN is entered an incorrect One Time Code will be displayed.

Allow String Browsing, This is a Swivel server controlled option, which if enabled will allow the user to browse through security strings on the mobile app.

72.6 Authenticating with app and PINsafe

To use the Swivel iPhone app to authenticate is very simple.

1. Open the app on your iPhone
2. Select Authenticate
3. The client will show a security string with a row of placeholders 1234567890 above it.
4. Use your PIN to extract your one-time code, eg if your PIN is 2468 take the 2nd 4th 6th and 8th characters of the Security String, 1870 in the example.
5. Enter the OTC into the authentication dialogue, including the ',' and the following 2 digits. e.g. 1870,02

If you need to authenticate again you can select the 'Next' button and a new string will be displayed



72.7 Updating Keys

The client downloads 99 keys at a time and these keys are used one at a time until there are none left. However a new set of 99 keys can be downloaded at any time by selecting Update Keys. Downloading keys requires network connectivity so it is recommended that you download a new set of keys before the iPhone is likely to be without network connectivity for any length of time.

73 Troubleshooting

- Is the Swivel server accessible on the internet
- Check the connection settings to the Swivel server
- Check the Swivel logs for any error messages
- Can the phone access the internet
- If a RADIUS connection is seen from the access device to the Swivel server but authentication fails, try using PAP
- Download new security strings to the phone and retest
- Is the OTC being entered with the comma and last two digits. E.g. 7329,62
- Login fails and User receives a security string or One Time Code by SMS or email at each login attempt. The index is required to be entered as nn on the end example: 292401, Swivel versions earlier than 3.10 require ,nn example: 2924,01 otherwise it will see it as a dual channel authentication.
- If the proxy port (8443) on the virtual or hardware appliance is being used, ensure that it supports the proxy request of the key retrieval using AgentXML. If this is the case then contact Support for an updated version of the Proxy.
- If you fail to authenticate successfully using the security string provided by the iPhone app please see [iPhone authentication fails](#)

73.1 Error Messages

Incorrect settings - please check your settings

The settings for downloading the security strings are incorrect. Verify what has been entered, and check what the values should be.

Timed Out

The settings for connecting to the Swivel server may be incorrect or the port is being blocked.

AGENT_ERROR_NO_SECURITY_STRINGS, AGENT ERROR NO SECURITY STRINGS

See [AGENT ERROR NO SECURITY STRINGS](#)

Not a valid command

This error message can be displayed when a mobile client app is attempted to be activated but uses an older version of the app with a newer version of the Swivel core. Remove previous versions of the app.

74 Tested Mobile Phones

The following phones have been tested

Mobile Phone Compatibility

Manufacturer	Model	Version	Operator	Compatible Y/N
Apple	5	7	-	Y
Apple	5	6.1.4	O2	Y
Apple	4	4.3.3	Vodafone	Y
Apple	3GS	4.0	Not Known	Y
Apple	3G	4.0	Deutsche Telekom	Y

The iPhone applet will also work on the iPad

75 Known Issues and Limitations

- The current version only supports one device per user.
- Currently only 4 digit PIN numbers are supported within the iPhone iClient (3.7 and earlier). This limitation does not affect the iPhone app Swivel 1.1 which is compatible with Swivel 3.8 onwards.
- iPhone Client 1.1 selecting the settings option will cause the iPhone client to be re-provisioned.
- iPhone Client 1.0 and 1.1 only support the use of number in the security string.
- iPhone Update to iOS7 is incompatible with version 1.4 and below of the Swivel mobile app. The application should update automatically but if not then you can update through the app store. (This limitation does not apply to the older Swivel mobile app)
- iOS 8 requires the iPhone Mobile Client 1.6 or higher

76 Legacy

Download compatible with Swivel 3.7 and earlier



Keywords: iPhone, iClient, Swivel, App, AppStore, Apple, iPad

77 Category:IPhone

78 iPhone 2.0

79 The Swivel iPhone 2.0 App Overview

Swivel Secure now offers a iPhone and iPad client for use with the Swivel platform. This article explains how to download, configure and use this client. For other phones see [Mobile Phone Client](#) for earlier versions.

80 Requirements

Swivel 3.10 or higher

iPhone, 4, 4S, 5, 5C, 5S and 6.

The Swivel virtual or hardware appliance must be reachable from the mobile phone to receive security strings

The index is required to be entered as nn on the end example: 292401, Swivel versions earlier than 3.10 require ,nn example: 2924,01 otherwise it will see it as a dual channel authentication.

Valid certificate on the Swivel server or non SSL, but not a self signed certificate

Updating Transports [Transport HTML](#)

81 Versions

version 2.1.1 released: 21/02/2015

- QR Code Provision
- Push Authentication Support

version 2.0 released

- Simple User Interface
- Extra Mobile Policies
- Help Section
- Citrix Receiver VPN Client support (iPhone Only)
- Removal of comma from OTC,

81.1 Which version do I need?

Swivel Mobile version 3.10 or later, iOS 5.0 or later.

Swivel version 3.10, iOS 5.0 or later

iPhone Mobile Client 2.0 version 2.0, TBA, iOS 7.0 or later

82 Swivel Configuration

82.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance

To allow a user to authenticate using a One Time Code from a mobile app, the user must have Mobile app authentication enabled. To do this on the Swivel Administration console ensure that the group they are part of has access to the Mobile Client under Repository Groups.

82.2 Configuring the Swivel Authentication

Swivel can authenticate users using the mobile client to authenticate by RADIUS or Agent-XML authentication

- For RADIUS authentication see [RADIUS Configuration](#) Note: The access device must be configured to use PAP for authentication.
- For Agent-XML authentication see [XML Authentication Configuration](#)

Allow user to browse strings: Options Yes/No, Default No. Version 3.9.6 onwards. This option allows the Mobile Phone App user to browse through the security strings. Availability to this feature is server controlled.

82.3 Mobile Provisioning

Swivel 3.8 and higher requires each mobile phone to be provisioned so it can be uniquely identified. Ensure that all Mobile Client users have suitable Transports configured to receive their Provision Code. To provision the mobile client select the user and click Re-provision. Earlier versions of Swivel do not need to use a Mobile Provision Code. See [Mobile Provision Code](#).

82.3.1 Mobile Client Policies

For the Server based policies see [Mobile Client Policies 2.0](#) for previous versions see [Mobile Client Policies](#)

83 User Experience with 'Quick Provisioning'

iPhone app 2.0 deployment from [Swivel Secure](#).

Swivel deployment process for the Mobile App. 2.0. The video shows a user receiving an email, from the Swivel platform providing the links and process to use their smartphone with Swivel for 2FA access.

84 iPhone Installation and Configuration

The Swivel iPhone Client 2.0 is available from the Apple App Store. You can click the icon below to open the App within iTunes, or follow the instructions in this article to navigate to the App within the App Store.

84.1 Download compatible with Swivel 3.10 onwards

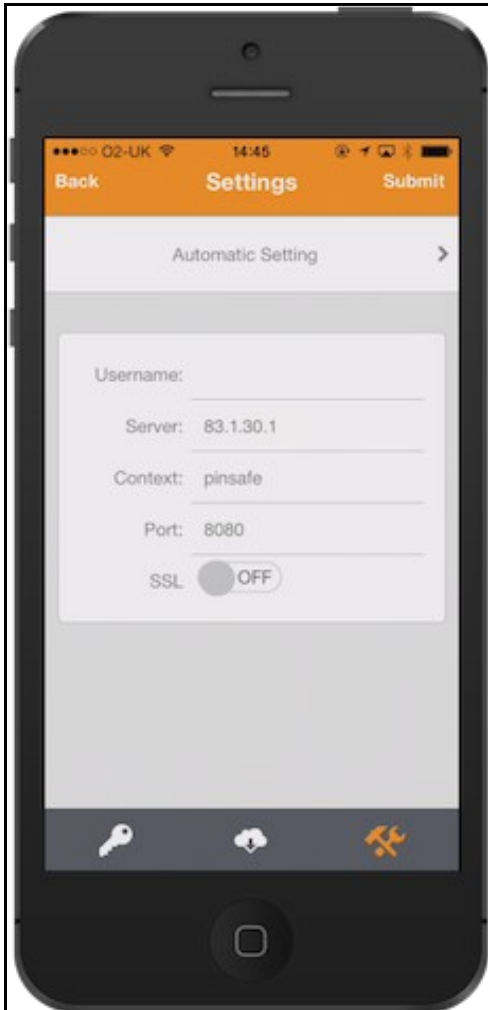


84.2 Configuring the app

When you launch the app you will see the helper wizard, at the bottom of the screen there will be menu icons to guide you through the mobile client options.

84.2.1 Get Server Settings

If an [SSD](#) server is being used, select **Get Server Settings** and enter the Server ID. Otherwise the settings can be manually entered with information from the Swivel System administrator.



The settings are

1. Username: Your username that you use when you authenticate via Swivel
2. Server: The URL from where the client can download security strings (or keys)
3. Context: The context used by the web service. For a virtual or hardware appliance this is **proxy**, for a software install this is usually **pinsafe**

4. Port: The port number used by the web service. For an virtual or hardware appliance this is **8443**, for a software only install see [Software Only Installation](#)

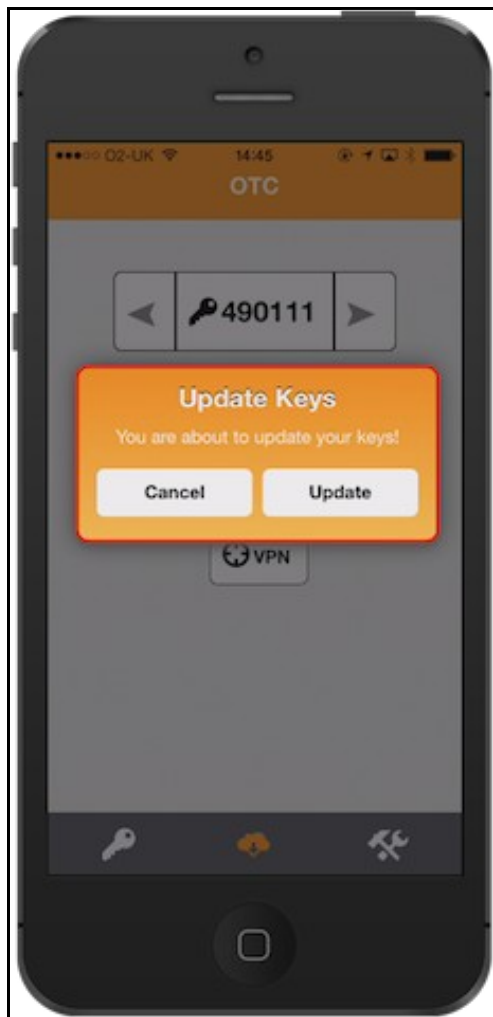
Once you have entered the settings you can select Submit in the header location of that page.

84.3 Mobile Provision Code

Swivel versions 3.10 and higher require each Mobile device to be Provisioned with a Code sent from the Swivel server. To provision a phone see [Mobile Provision Code](#).

84.4 Downloading Security Strings

From the bottom menu there is a update keys button, pressing this will get you a new set of 99 security strings. This will attempt to retrieve Security Strings from the Swivel server.



If there are any problems and error message will be displayed

You can confirm that keys have been downloaded by checking the server logs

The Swivel server will display the following log message **Security strings fetched for user: username**

84.5 Options

The following options are available:

Auto extract OTC, Prompt for PIN Number to auto-extract OTC, Options, enable/disable. This option may be turned off on the Swivel server. When enabled this allows the user to enter their PIN number and a One Time Code will be displayed. Note that there is no error checking of the PIN, so if an incorrect PIN is entered an incorrect One Time Code will be displayed.

Allow String Browsing, This is a Swivel server controlled option, which if enabled will allow the user to browse through security strings on the mobile app.

Provision is numeric, allows the keyboard type to be either alpha numeric of numeric depending on the users provision code type.

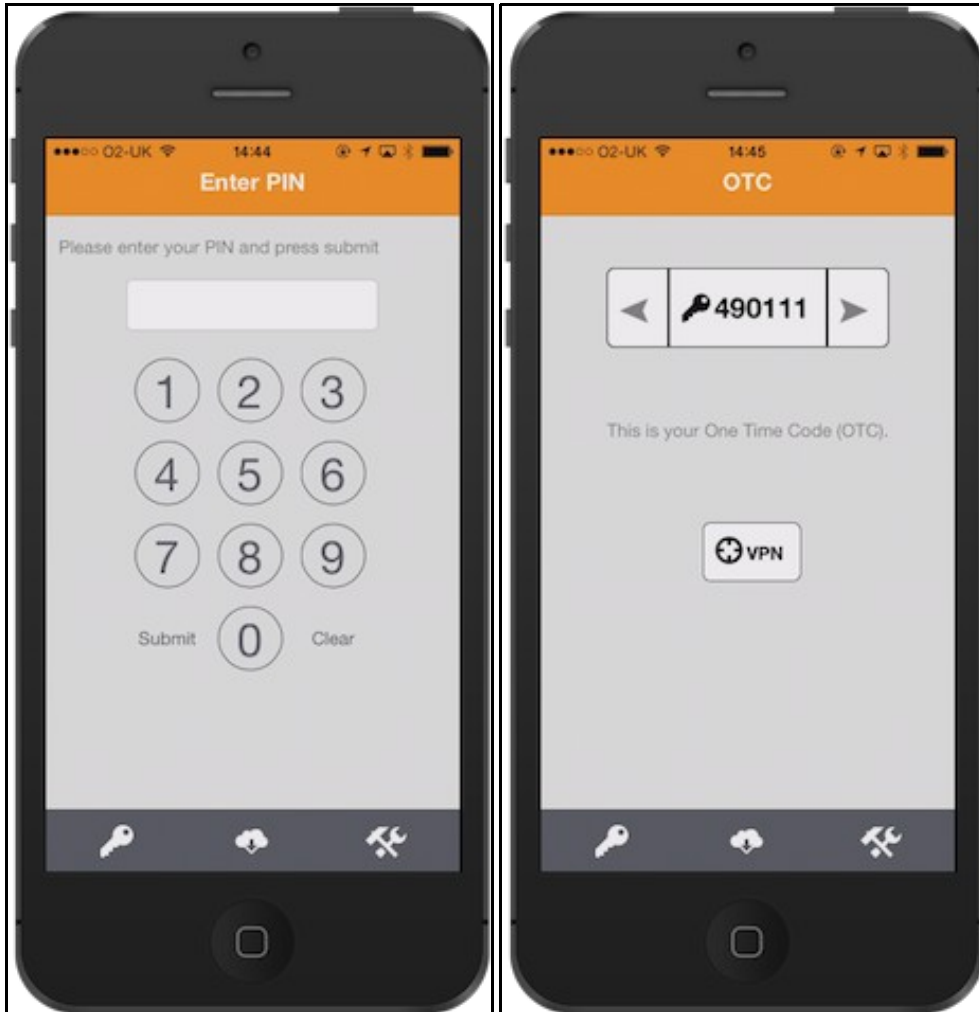
Set Support Email Address. Set Support Phone Number. Set VPN client URL.

84.6 Authenticating with app

To use the Swivel iPhone app to authenticate is very simple.

1. Open the app. on your iPhone.
2. Select the key icon on the bottom menu.
3. Depending on your policy settings you will either be prompted for a PIN or immediately shown a One-Time-Code (OTC).
4. If you are asked for a PIN, enter the PIN number previously sent during the enrolment phase.
5. Enter the OTC into the authentication dialogue, make sure you enter all the characters.

If you need to authenticate again you can select the '<' or '>' button and a new string will be displayed (you may have to enter your PIN again).

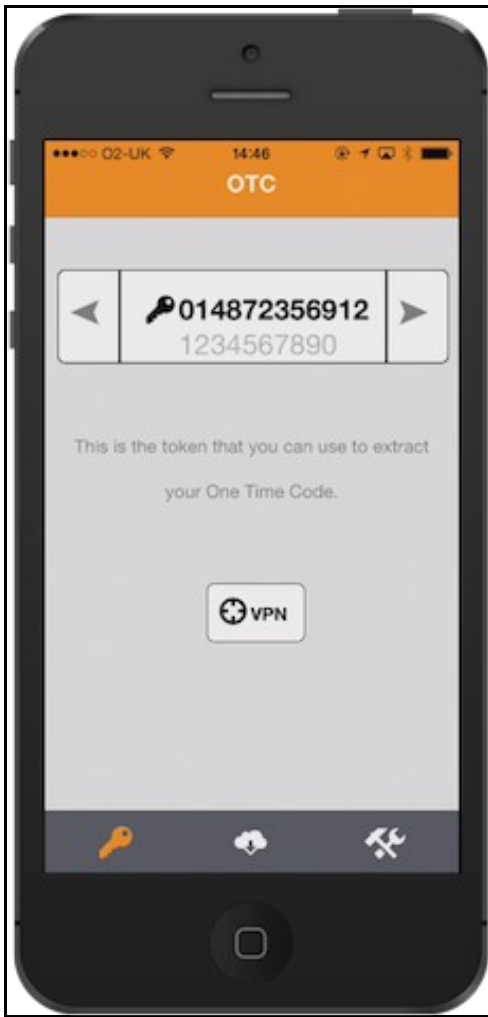


84.7 Authenticating with app and Swivel

To use the Swivel iPhone app to authenticate is very simple.

1. Open the app on your iPhone.
2. Select the key icon on the bottom menu.
3. The client will show a security string with a row of placeholders 1234567890 below it.
4. Use your PIN to extract your One-Time-Code (OTC), eg if your PIN is 2468 take the 2nd 4th 6th and 8th characters of the security string.
5. In the example screen shoot the OTC would be: 1825.
6. After the OTC has been worked out, you will also need to ensure you type in the last two characters shown (the index).
7. Using the example screen shot you would type 182512.

If you need to authenticate again you can select the '<' or '>' button and a new string will be displayed.



84.8 Updating Keys

The client downloads 99 keys at a time and these keys are used one at a time until there are none left. However a new set of 99 keys can be downloaded at any time by selecting Update Keys. Downloading keys requires network connectivity so it is recommended that you download a new set of keys before the iPhone is likely to be without network connectivity for any length of time.

85 Troubleshooting

- Is the Swivel server accessible on the internet
- Check the connection settings to the Swivel server
- Check the Swivel logs for any error messages
- Can the phone access the internet
- If a RADIUS connection is seen from the access device to the Swivel server but authentication fails, try using PAP
- Download new security strings to the phone and retest
- Is the pin 6 characters when you only entered a 4 digit pin? If yes then enter all of the numbers you see on screen (the extra 2 are used as an index).
- Login fails and User receives a security string or One Time Code by SMS or email at each login attempt. Again make sure you are entering all of the numbers shown on screen.
- If the proxy port (8443) on the virtual or hardware appliance is being used, ensure that it supports the proxy request of the key retrieval using AgentXML. If this is the case then contact Support for an updated version of the Proxy.
- If you fail to authenticate successfully using the security string provided by the iPhone app please see [iPhone authentication fails](#)

85.1 Error Messages

Incorrect settings - please check your settings

The settings for downloading the security strings are incorrect. Verify what has been entered, and check what the values should be.

Timed Out

The settings for connecting to the Swivel server may be incorrect or the port is being blocked.

AGENT_ERROR_NO_SECURITY_STRINGS, AGENT ERROR NO SECURITY STRINGS

See [AGENT ERROR NO SECURITY STRINGS](#)

Not a valid command

This error message can be displayed when a mobile client app is attempted to be activated but uses an older version of the app. Remove previous versions of the app.

Cannot Open Page Safari cannot open the page because the address is invalid

The link to the provisioning is incorrect or will not open in Safari.

86 Known Issues and Limitations

- The current version only supports one device per user.

If the Mobile Client fails to provision through the One Step Provision process, exit the app and configure manually. An updated version Mobile Client App will be made available on the Apple store.

87 Legacy

Mobile Phone Compatibility



3.4 - 3.8 <http://itunes.apple.com/gb/app/pinsafe-iclient/id374241218>



3.8 - 3.10 <https://itunes.apple.com/gb/app/swivel-mobile/id872975579>

Keywords: iPhone, iClient, Swivel, App, AppStore, Apple, iPad

88 Mobile Phone Client

89 Mobile Phone Client 2.x

89.1 Overview

Swivel Mobile Phone 2.x apps are named *Mobile Phone Client 2.0*, the Swivlet referring explicitly to the Java Mobile Phone Client

The PINsafe Mobile Phone Client 2.x allows the storage of 99 security strings to be stored on the phone. The PIN is not stored on the phone. Requesting a top up from the PINsafe server resets all the security strings on the mobile phone, providing 99 security strings for authentication. The value of 99 security strings is fixed and cannot be changed. You can use the device to get one-time codes for PINsafe login and PIN change.

Each Mobile Phone Client can be configured automatically using a [SSD](#) server and is provisioned with a unique [Mobile Provision Code](#) which provides information about the Mobile Phone Client that only allows a specific user on a specific mobile phone to request the security strings.

For the PINsafe Android Client see [Android 2.0](#)

For the Blackberry 10 client see [Blackberry 2.0](#)

For the iPhone select [IPhone 2.0](#).

For the Windows Mobile version select [Windows Phone\(8\) 2.0 How To Guide](#).

For the Windows Phone 7 and Blackberry 6 the previous version will still exist and be used for these models, see [Blackberry](#).

89.2 Integrating with the Mobile App

Integration of login portals is usually straight forward with Mobile Apps, although if [TURing](#) and [Pinpad](#) images are used, then these should not be automatically generated as a login will be expected using those methods.

90 Mobile Phone Client 1.0

90.1 Overview

Swivel Mobile phone apps are named *Mobile Phone Client*, the Swivlet referring explicitly to the Java Mobile Phone Client

The PINsafe Mobile Phone Client allows the storage of 99 security strings to be stored on the phone. The PIN is not stored on the phone. Requesting a top up from the PINsafe server resets all the security strings on the mobile phone, providing 99 security strings for authentication. The value of 99 security strings is fixed and cannot be changed. You can use the device to get one-time codes for PINsafe login and PIN change.

Each Mobile Phone Client can be configured automatically using a [SSD](#) server and is provisioned with a unique [Mobile Provision Code](#) which provides information about the Mobile Phone Client that only allows a specific user on a specific mobile phone to request the security strings.

For the PINsafe Android Client see [Android](#)

For the Blackberry client see [Blackberry](#)

For the iPhone select [IPhone](#).

For the Java applet for Java enabled phones see [Swivlet How To Guide](#)

For the Windows Mobile version select [Windows Mobile How To Guide](#).

For the Windows Phone 7 version select [Windows Phone 7 How To Guide](#).

90.2 Integrating with the Mobile App

Integration of login portals is usually straight forward with Mobile Apps, although if [TURING](#) and [Pinpad](#) images are used, then these should not be automatically generated as a login will be expected using those methods.

91 IPad Citrix Receiver

1. REDIRECT Citrix_Receiver

92 Category:Java

93 Java Mobile Phone Client

93.1 Swivlet How To Guide

93.2 Overview

The Swivlet is now deprecated. The Swivlet will only work with Swivel versions up to and including 3.7. For later versions see [Mobile Phone Client](#).

Mobile phone apps are now named *Mobile Phone Client*, the Swivlet referring explicitly to the Java Mobile Phone Client.

The Swivel Mobile Phone Client or Java Applet or Midlet, for the mobile phone allows the storage of 99 security strings or One Time Codes for PINless authentication, on a java enabled mobile phone. The PIN is not stored on the phone. Requesting a top up from the Swivel server resets all the security strings on the mobile phone, providing 99 security strings for authentication. The value of 99 security strings is fixed and cannot be changed. You can use the device to get one-time codes for Swivel login and PIN change.

93.3 Prerequisites

Swivel 3.7 or less, for later versions see [Mobile Phone Client](#) for other supported apps.

On the Swivel Administration Console the user must have Swivlet or Mobile Client enabled to use the Java Applet (or other Mobile Client App)

The Swivel server must be reachable from the mobile phone to receive security strings

Security strings must be entered including the comma and sequence number e.g. nnnn,nn

Appliances using Swivel 3.8 may require an upgrade on their proxy to provision a mobile device, see [Appliance Proxy Server Upgrade](#)

RADIUS authentications made against Swivel must use PAP RADIUS authentication since with other RADIUS protocols such as CHAP and MSCHAP the access device requests the OTC from Swivel.

93.4 Swivel Server Configuration

93.4.1 Configuring Swivlet User Access

To allow a user to authenticate using a One Time Code from the Swivlet, the user must have the Swivlet authentication enabled. To do this on the Swivel Administration console ensure that the group they are part of has access to the Swivlet under Repository Groups.

93.4.2 Configuring the Swivel Authentication

Swivel can authenticate users by RADIUS or Agent-XML authentication

- For RADIUS authentication see [RADIUS Configuration](#) Note: The access device must be configured to use PAP for authentication.
- For Agent-XML authentication see [XML Authentication Configuration](#)

Note: The access device must be configured to use PAP for authentication.

93.4.3 Mobile Provisioning

Swivel 3.8 and higher requires each mobile phone to be provisioned so it can be uniquely identified. Ensure that all Mobile Client users have suitable Transports configured to receive their Provision Code. To provision the mobile client select the user and click Re-provision. Earlier versions of Swivel do not need to use a Mobile Provision Code.

93.5 Swivlet Installation on Phone

The Swivlet can be provided on a web page and deployed by the client using a web browser to download it to their phone. The Phone should detect that it is a java application and install it.

The Swivlet can be downloaded from a mobile phone here: <https://demo.swivelsecure.com/provision> (This is the Swivlet version 2 which includes Mobile provision support for Swivel 3.8 onwards)

Another way of provisioning the Swivlet would be by a WAP push to the mobile Phone

93.6 Swivlet Configuration on Phone

The Swivlet needs to be configured with the following information:

Server URL: The Swivel server IP or hostname

Context: The Swivel installation path (usually pinsafe or proxy)

Username: The username used for authentication

93.6.1 Mobile Provision Code

Swivel versions 3.8 and higher require each Mobile device to be Provisioned with a Code sent from the Swivel server. To provision a phone see [Mobile Provision Code](#). Swivel versions earlier than Swivel 3.8 do not need to be provisioned.

93.7 Testing

You can top up the Swivlet and you should see a log message saying strings requested for user XXXX or *security strings fetched for user: XXXX*

93.8 Options

93.8.1 Preconfiguring the Swivlet

You may need to edit the .jad file as this indicates to the browser where to get the .jar file

(see MIDlet-Jar-URL:<https://demo.swivelsecure.com/provision/Swiveler.jar>).

The .jad file is also available here: [PinsafeClient.jad](#)

You can also edit the .jad file to preconfigure the client

Pinsafe-Context: /pinsafe

Pinsafe-URL: <http://demo.swivelsecure.com:8080>

Pinsafe-Username: yourUsername

```
L10N-Bundle: com.swiveltechnologies.l10n.bundle.Bundle_en_US
L18N-Bundle: com.swiveltechnologies.l18n.bundle.Bundle_en_US
MIDlet-1: Swivlet 2,,com.swiveltechnologies.Swivlet2
MIDlet-Jar-Size: 58140
MIDlet-Jar-URL:https://demo.swivelsecure.com/provision/Swiveler.jar
MIDlet-Name: Swivlet2
MIDlet-Vendor: Swivel Technologies
MIDlet-Version: 2.1.0
Main-Menu: com.swiveltechnologies.ui.menu.Remote
MicroEdition-Configuration: CLDC-1.0
MicroEdition-Profile: MIDP-1.0
One-Time-Code-Render: com.swiveltechnologies.render.otc.Standard
Pin-Change-Render: com.swiveltechnologies.render.otc.StandardPinChange
Pinsafe-Context: /pinsafe
Pinsafe-URL: http://demo.swivelsecure.com:8080
Pinsafe-Username: yourUsername
Provision-Type: com.swiveltechnologies.provision.type.Remote
Security-String-Generator: com.swiveltechnologies.generate.ss.Remote
```

93.9 Troubleshooting

Is the Swivel server accessible on the internet

Check the connection settings to the Swivel server

Check the Swivel logs for any error messages

Can the phone access the internet

Does the Swivel applet application have authorisation to access the network connection

Can the phone use self signed certificates if a https connection is being used

If a RADIUS connection is seen from the access device to the Swivel server but authentication fails, try using PAP

Download new security strings to the phone and retest

If the proxy port (8443) on the appliance is being used, ensure that it supports the proxy request of the key retrieval using AgentXML. If this is the case then contact Support for an updated version of the Proxy.

Login fails and User receives a security string or One Time Code by SMS or email at each login attempt. The index is required to be entered as ,nn example 2924,01 otherwise it will see it as a dual channel authentication.

93.10 Error Messages

903 Loss of service HTTP error 400: bad request

The JAD file references http and needs to be changed to https

SwivletException : SE007: java.io. IO exception:-5120

This error message has been seen with an incorrectly configured DNS entry

com.swiveltechnologies.SwivletException: SE007: javax.microedition.io.ConnectionNotFoundException: Protocol not found:
net.rim.device.cldc.io.http.Protocol

This message has been seen when using a blackberry with the Java Mobile Phone Applet without Internet access enabled for the applet. To enable internet access to the Swivlet, select Options, then security, then Application Permissions, select the Swivlet application then press the blackberry button and configure the options available to the applet.

Com.swiveltechnologies.SwivletException:SE007:java.io.IOException:Timed out

This error message has been seen on a Blackberry Swivlet that cannot connect to the Swivel server. Check network settings, and if the application is allowed access to the internet.

Com.swiveltechnologies.SwivletException:SE005:java.io.IOException:Timed out

This error message has been seen on a Blackberry Swivlet where the context has been incorrectly configured.

Com.swiveltechnologies.SwivletException:SE005:java.io.IOException:Failed to transmit

This has been seen on a Blackberry Swivlet where the security strings may already be at 99. Try using one and then requesting new strings.

Requesting Please wait..., 0 to 10 displayed repeatedly then Com.swiveltechnologies.SwivletException:SE007:java.io.InterruptedIOException:Local connection timed out after # 120000

This has been seen on a Blackberry swivlet where the swivlet cannot connect to the Swivel server, check network connectivity.

com.swiveltechnologies.SwiveletException:SE007:

javax.microedition.pki.CertificateException:Certificate failed verification

The Swivel Swivlet is unable to validate the certificate installed on the Swivel server from which the security strings are to be downloaded.

AGENT_ERROR_NO_SECURITY_STRINGS, AGENT ERROR NO SECURITY STRINGS

The OTC is being entered without the ,nn at the end of the OTC, whereby nn is the number given with the security string

93.11 Known Issues and Limitations

The current version only supports one device per user.

93.12 Tested Mobile Phones

As more information is fed back additional phones will be added here. Note that the operator may not supply Java run time environments so we have listed the operator as well.

Mobile Phone Compatibility

Manufacturer	Model	Version	Operator	Compatible Y/N	Swivlet Version
Blackberry	8520	v4.2.0.135	Not Known	Y	Not Known
Blackberry	8820	v4.2.2.175	Orange UK	Y	Not Known
Blackberry	9300	v6.6.0.195	Not Known	Y	Not Known
Blackberry	9300	v6.6.0.207	Not Known	Y	Not Known
Nokia	E52	Not Known	Not Known	Y	Not Known
Nokia	E71	Not Known	Not Known	Y	Not Known

93.13 RADIUS Considerations

One thing to be aware of is that when using RADIUS authentication, except for the PAP protocol, you must use every string from the phone for authentication. If you generate a string and don't use it, authentication will fail until you Top Up again. This is an unavoidable consequence of the way most RADIUS protocols work.

94 Mobile App Privacy Policy

95 Notes

This document refers to requisites of Authcontrol Mobile App.

96 Privacy Policy

Swivel Secure's mobile app requires access to:

- The Camera app to allow scanning of QR codes in our provisioning messages to ensure easy user provisioning.
- The Storage to save the information required to communicate with your AuthControl Sentry system and the storage of the security strings, that are downloaded as part of the provisioning process, allowing authentications even when no mobile phone signal is present.
- The Phone app to allow users to directly call their helpdesk from within the application for support and assistance.
- Your Email app to contact your company's helpdesk via email for support and assistance.

No other information is accessed, copied, collected or stored either within the app, on the phone or anywhere else.

97 Need more help?

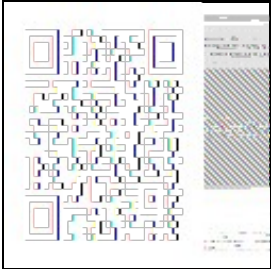
Please contact your partner or create a support ticket in our support portal <https://supportdesk.swivelsecure.com/dashboard>

98 QR Code Provision

99 Overview

Swivel version 3.10.4 onwards supports provision of a Mobile Client [Mobile Provision Code](#) contained within a QR Code. The QR code can be provided in a number of ways:

- Within an Email
- Within a web page, such as a link in an email
- Through the [User Portal](#) (latest User Portal is required)



The Provision code lasts until a Provision attempt is made or the Provision Code Validity is exceeded, see [Mobile Provision Code](#).

100 Prerequisites

Swivel 3.10.4

[User Portal](#)

Mobile Phone Client 2.1.1 onwards

Mobile Phone/tablet with camera

Valid certificate (or non SSL connection) or mail client may block QR image

101 QR Code Setup

To setup QR Code provisioning, on the Swivel Administration console, select Policy, then Self Reset and enter the URL of the User Portal page in the **QR Code URL**:, if this is not present then it may be an older version and require upgrading to Swivel version 3.10.4 or later. The format for an appliance is:

```
https://Public_IP:8443/userportal/getQRCode?text=
```

101.1 Transport Configuration

To send QR Codes by email ensure that HTML is enabled

The QR code url is placed in the message by replacing the phrase url4

So to include the QR code in the HTML email included

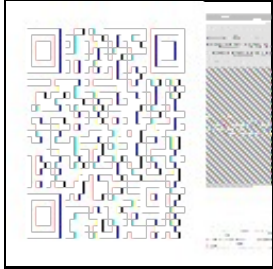
```
<img src=url4>
```

102 Testing

The QR Code should generated when sent by email to a user.

102.1 Provisioning a Mobile Client

Following the [Provision URL](#) links will automatically provision a Mobile Phone Client. To use the QR code, on the Swivel Mobile Phone Client, click on the Information 'i' icon then, About and tap on the **Scan QR Code** link to start the QR code scanner. Hold Mobile Phone so visible area of the scanner so that it contains the QR Code and wait until it recognises it. The Mobile Client should then be provisioned.



103 Known Issues

104 Troubleshooting

104.1 Error Messages

Error Server, Unknown Server ID

The **Site ID** may not exist or may not have been entered.

Error Server Connection

The server details are missing or incorrect

Invalid Username

The User may not exist on the Swivel server.

Invalid Provision Code

The provision code is not valid or has already been used.

Error Dowloading Security Strings

The user may not be a member of an appropriate group with Mobile Client authentication enabled

Reprovision URL not retrieved

This can occur in the User Portal on a QR Code request if the user has been removed

105 How To Configure Local Mode Mobile

105.1 Overview

Local mode allows the mobile app to generate security codes automatically without connection to the Swivel Core. If the device is provisioned on local mode, push Authentication cannot be used.

105.2 Prerequisites

Swivel AuthControl Sentry v4 onwards

Swivel Mobile Phone Client Version v4 for One Touch Mobile client based solution.

Swivel Server Details SSD for mobile client with local mode enabled.

105.3 Swivel core configuration

In order for a user to be able to use the mobile app they must be allocated the right to use the Mobile App mode of operation. This is done by ensuring that they are a member of a group that has this right.

Mobile client users must install the Swivel Mobile Phone Client from the app store.

105.4 Configuring Local Mode policy settings

On the Swivel Administration console select Policy/Self-Reset and ensure the below settings are configured:

Set **Mobile App OATH Mode** to No

Set **Mobile App Local Mode** to Yes

- [Status](#)
- [Log Viewer](#)
- ⊞ Server
- ⊞ Policy
 - [General](#)
 - [PIN and OTC](#)
 - [Password](#)
 - [Self-Reset](#)
 - [Helpdesk](#)
 - [Banned Credentials](#)
 - [Console Login](#)
 - [Mobile App](#)
 - [Reporting](#)
- ⊞ Logging
- ⊞ Messaging
- ⊞ Database
- ⊞ Mode
- ⊞ Repository
- ⊞ RADIUS
- ⊞ Migration
- ⊞ Appliance
- ⊞ OATH
- ⊞ Config Sync
- ⊞ Reporting
 - [User Administration](#)
 - [Save Configuration](#)
 - [Upload Email Images](#)
 - [Administration Guide](#)
 - [Logout](#)

Policy>Self-Reset

Please enter the policies to apply to user se

Allow user self-reset:

Send reset code as security string:

Maximum self-reset tries:

Allow user self-provision of mobile app:

Send provision code as security string:

Enforce HTTP Header Checking:

Mobile App Local Mode:

Mobile App OATH Mode:

Provision Code Validity period (seconds):

URL provisioning:

URL to get settings:

URL complete:

QR Code URL:

105.5 Testing

For testing local mode you can click App provision button on the user admin screen for the user that has been configured as a mobile OATH user and then provision the device with the URL or QR Code as explained:

Provision the device via URL. [Please read more on Provision URL page.](#)

Provision the device via QR code. [Please read more on QR Code page.](#)

105.6 Troubleshooting

Security code not working or mobile app tries to connect to Swivel Core

Please ensure that the SSD server for that Site ID has been configured as local mode and OATH is set to false. After changing the setting in SSD server, the users must me re-provisioned.

106 How To Configure OATH Mobile

106.1 Overview

OATH authentication allows a mobile device to be prompted a new OTC every 60 seconds without requiring the connection to AuthControl Sentry. Optionally, this can be changed to every 30 seconds for compatibility with Google and Microsoft Authenticators. See below for more details.

106.2 Prerequisites

Swivel AuthControl Sentry v4 onwards

Swivel Mobile Phone Client Version v4 for One Touch Mobile client based solution.

Swivel Server Details SSD for mobile client with OATH enabled.

106.3 Swivel core configuration

In order for a user to be able to use the mobile app as a OATH token they must be allocated the right to use the OATH mode of operation. This is done by ensuring that they are a member of a group that has this right.

Mobile client users must install the Swivel Mobile Phone Client from the app store.

106.4 Configuring OATH policy settings

On the Swivel Administration console select Policy -> Mobile App and ensure the below settings are configured:

Set **Mobile App OATH Mode** to Yes

Status

Log Viewer

▸ Server

▾ Policy

▸ General

▸ PIN and OTC

▸ Password

▸ Self-Reset

▸ Helpdesk

▸ Banned
Credentials

▸ Console Login

▸ Mobile App

▸ Reporting

▸
[policy_dualchannel]

▸ Logging

▸ Messaging

▸ Database

▸ Mode

▸ Repository

▸ RADIUS

▸ Migration

Policy / Mobile App ?

Set the polices to be downloaded to mobile app.

Allow user self-provision of
mobile app:

Yes ▾

Send provision code as
security string:

No ▾

Use long provision code:

No ▾

Use 30 second timestep for
OATH:

No ▾

Issuer for OATH token
label:

Enforce HTTP Header
Checking:

No ▾

Mobile App Local Mode:

No ▾

Mobile App OATH Mode:

No ▾

Base64 Encode Username
in provision URL:

No ▾

Other relevant options on this page are:

- Use 30 second timestep for OATH - if this is enabled, OATH codes are compatible with Google and Microsoft Authenticators. AuthControl Mobile Authenticator also supports this.
- Issuer for OATH token label - this only applies to 30-second OATH mode, and sets part of the label for authenticator display

Note that OATH mode (60 second timestep) is compatible with Push authentication provided that local mode is not also enabled.

106.4.1 Notes for 30 Second Mode

Note that if 30 second mode is enabled, provisioning can only be done using the QR code, in AuthControl Mobile Authenticator, Google Authenticator, Microsoft Authenticator or any other compatible authenticator app.

Please note that for 30 second mode, the URL placeholder needs to be url5, rather than url4. See the article on provisioning mobile apps for more details.

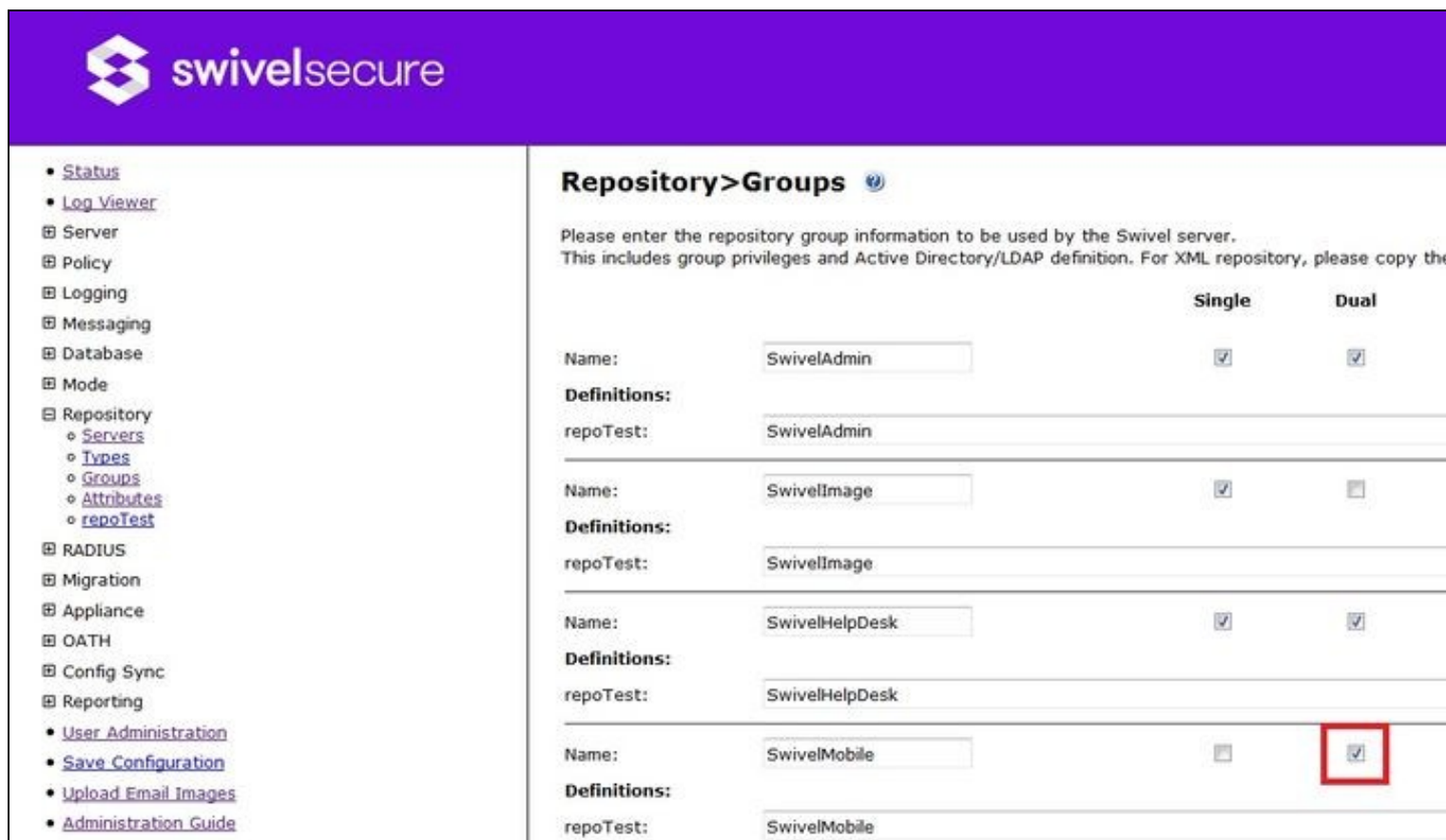
As 30-second timestep does not send any information back to Sentry, it is not compatible with Push authentication.

You can have both 30- and 60- second timestep tokens. Changing the setting only affects new tokens created after the change and does not change or invalidate tokens created before the change.

106.5 Define a group of Mobile OATH users

On the Swivel Administration console, select a group of users that will be using Mobile OATH authentication and ensure that the OATH box is ticked then click Apply.

OATH Mobile Users



swivelsecure

- [Status](#)
- [Log Viewer](#)
- ▣ Server
- ▣ Policy
- ▣ Logging
- ▣ Messaging
- ▣ Database
- ▣ Mode
- ▣ Repository
 - [Servers](#)
 - [Types](#)
 - [Groups](#)
 - [Attributes](#)
 - [repoTest](#)
- ▣ RADIUS
- ▣ Migration
- ▣ Appliance
- ▣ OATH
- ▣ Config Sync
- ▣ Reporting
- [User Administration](#)
- [Save Configuration](#)
- [Upload Email Images](#)
- [Administration Guide](#)

Repository > Groups

Please enter the repository group information to be used by the Swivel server.
This includes group privileges and Active Directory/LDAP definition. For XML repository, please copy the

	Single	Dual
Name: SwivelAdmin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions: repoTest: SwivelAdmin		
Name: SwivelImage	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Definitions: repoTest: SwivelImage		
Name: SwivelHelpDesk	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions: repoTest: SwivelHelpDesk		
Name: SwivelMobile	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions: repoTest: SwivelMobile		

106.6 Testing

For testing OATH you can click App provision button on the user admin screen for the user that has been configured as a mobile OATH user and then provision the device with the URL or QR Code as explained:

Provision the device via URL. [Please read more on Provision URL page.](#)

Provision the device via QR code. [Please read more on QR Code page.](#)

106.7 Troubleshooting

Security code is showing instead of OATH Token

Please ensure that the SSD server for that Site ID has been configured as OATH and local mode is set to false. After changing the setting in SSD server, the users must be re-provisioned.

Check the Swivel logs for error messages

Error Messages:

CANNOT_CREATE_TOKEN for the <username> user does not belong to the OATH Group

This error can be seen where the button App Provision is clicked on the User Admin Console and the user does not have OATH permission. To solve that you need to add the OATH right to the group the user is member of.

OATH token does not allow the authentication.

When you click Provision App ensure that a token for that user has been created. For that you can go to the OATH/OATH Tokens screen and check that a new token has been created for that user.

- [Status](#)
- [Log Viewer](#)
- ⊞ Server
- ⊞ Policy
- ⊞ Logging
- ⊞ Messaging
- ⊞ Database
- ⊞ Mode
- ⊞ Repository
- ⊞ RADIUS
- ⊞ Migration
- ⊞ Appliance
- ⊞ OATH
 - [OATH Policies](#)
 - [OATH Tokens](#)
 - [OATH Users](#)
- ⊞ Config Sync
- ⊞ Reporting
 - [User Administration](#)
 - [Save Configuration](#)
 - [Upload Email Images](#)
 - [Administration Guide](#)
 - [Logout](#)

OATH>OATH Users

Total number of users : 2

Users per page :

Search by username :

Search by serial ID :

Username	Allocated Token
admin	..none.. <input type="button" value="Assign Token..."/>
Imorales	Imorales <input type="button" value="Un-assign"/>

If the token has not been created, ensure that the policy Mobile App OATH Mode is set to Yes.

107 How To Configure Push Mobile

107.1 Overview

Push (or OneTouch) authentication allows a mobile device to be prompted by the Swivel server to let the user authenticate by pressing a confirm button on the mobile device screen, via a Swivel mobile application. You can see how that works on the following video:

107.2 Prerequisites

Swivel AuthControl Sentry v4 onwards

Swivel Mobile Phone Client Version v4 for One Touch Mobile client based solution.

Swivel Server Details SSD for mobile client with OneTouch enabled.

Swivel Server will need connection with Google and Apple servers: android.googleapis.com:443, fcm.googleapis.com:443, gateway.push.apple.com:2195, feedback.push.apple.com:2196

107.3 Swivel core configuration

In order for a user to receive the Push / OneTouch Mobile push message they must be allocated the right to use the OneTouch mode of operation. This is done by ensuring that they are a member of a group that has this right.

In addition they must be in a group associated with an Push / OneTouch transport. The transport must be the PNA (push notification authentication) Transport for Push / OneTouch Mobile client users.

Push / OneTouch Mobile client users must install the Swivel Mobile Phone Client from the app store. You can see how that works on the following videos:

107.4 Configuring Dual Channel settings

On the Swivel Administration console select Server/Dual Channel and ensure the below settings are configured:

Set **On-Demand Delivery** to Yes

Set **Allow message request by Username** to Yes

In Bound OTC Rule: Confirm key - enter the digits defined under Confirm Key to authenticate, example: if 1234 is entered then confirm by entering 1234 on the telephone keypad. OneTouch Mobile client solution currently only supports the confirm key mode of operation Confirmation key: (may be shown as [server_dualchannel_inboundconfirmkey]): The key(s) to be pressed to confirm authentication Call/Notification gap(s) (may be shown as [server_dualchannel_inboundcallgap]):

Domain Allowed to get OTC: Indicates the domain (e.g. <http://localhost:8080>, <http://domain>) authorized to get OTC. That is used by 2 way transport like Push Voice telephone or Push Mobile PNA (push notification authentication). The domain will correspond with the domain client (e.g. AuthControl Sentry, OnePushDemo, ...). If the value is * it will allow all the domains.

In Bound OTC Rule:	Confirm Key ▾
Confirmation key:	67890
Call/Notification gap (s):	10
In Bound SMS Timeout (ms):	500

107.5 Define a group of Push Users

On the Swivel Administration console, select a group of users that will be using Push authentication and ensure that the Push box is ticked then click Apply.

Push Mobile Users

Repository>Groups

Please enter the repository group information to be used by the Swivel server.

This includes group privileges and Active Directory/LDAP definition. For XML repository, please copy

		Single	Dual
Name:	<input type="text" value="SwivelAdmin"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions:			
repoTest:	<input type="text" value="SwivelAdmin"/>		
Name:	<input type="text" value="SwivelImage"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Definitions:			
repoTest:	<input type="text" value="SwivelImage"/>		
Name:	<input type="text" value="SwivelHelpDesk"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions:			
repoTest:	<input type="text" value="SwivelHelpDesk"/>		
Name:	<input type="text" value="SwivelMobile"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions:			
repoTest:	<input type="text" value="SwivelMobile"/>		
Name:	<input type="text" value="SwivelSMTP"/>	<input type="checkbox"/>	<input type="checkbox"/>
Definitions:			
repoTest:	<input type="text" value="SwivelSMTP"/>		
Name:	<input type="text" value="SwivelToken"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions:			
repoTest:	<input type="text" value="SwivelToken"/>		

107.6 Define a Push Transport

On the Swivel Administration console, select or create a Push Transport

For OneTouch Mobile Client this will be the PNA (push notification authentication) Transport

Push Mobile Client Transport



Identifier:	<input type="text" value="PNA"/>
Class:	<input type="text" value="com.swiveltechnologies.pinsafe.server.transport.PNATransport"/>
Strings per message:	<input type="text" value="1"/>
Copy to alert transport:	<input type="button" value="No"/>
Destination attribute:	<input type="button" value="platformandpushid"/>
Strings Repository Group:	<input type="button" value="---NONE---"/>
Alert repository group:	<input type="button" value="---NONE---"/>
Push repository group:	<input type="button" value="SwivelMobile"/>

Configure Push Transports Configure a One Touch Mobile Client (PNA) Transport

The PNA (push notification authentication) Transport is preconfigured, no configuration changes are required unless requested by Swivel support

Timeout (ms): default 30000. Notification timeout. If the notification is pressed or arrives after the specified time, a message will be shown to the user to indicate that the Authentication Request has expired. 0 is no Timeout.

Notification title: Text displayed on the device notification.

Notification body: Text displayed on the authentication screen of the Swivel Mobile App.

iOS cert password: iOS certificate password which should correspond with the kind of certificate that is being used: production or development. The certificate used will depend of the attribute 'Production environment'.

BB URL: Push URL for BB10 Swivel Mobile App.

BB application id: BB10 Swivel Mobile App's identifier.

BB password: Push password for BB.

Android key: Key related with the Swivel Mobile app used.

Production environment: Indicates if the current environment is development or production. Depending of this value the certificate used to send the notification to the device will be the production one or the development one.

107.7 PNA configuration

Messaging>PNA

Please enter the details for the Push transport. Platforms supported: iOS, WP8, BB10, Android

Timeout (ms):	<input type="text" value="300000"/>
Notification title:	<input type="text" value="Authentication request received"/>
Notification body:	<input type="text" value="Do you want to continue with the authentication?"/>
iOS cert password:	<input type="password" value="....."/>
BB URL:	<input type="text" value="https://cp1253.pushapi.na.blackberry.com"/>
BB application id:	<input type="text" value="1253-8719a7580ri086467oooco209r60880oa86"/>
BB password:	<input type="password" value="....."/>
Android key:	<input type="text" value="AIzaSyAi-Kc1VQmQr7frgMeHWVqyg8RdWGc3Ow"/>
Production environment:	<input type="text" value="Yes"/> ▼

107.8 PNA V5 Configuration

Messaging>PNAV5

Please enter the details for the Push transport. Platforms supported: iOS, WP8, BB10, Android

Timeout (ms):	<input type="text" value="300000"/>
Notification title:	<input type="text" value="Authentication request received"/>
Notification body:	<input type="text" value="Do you want to continue with the authentication?"/>
iOS cert password:	<input type="password" value="....."/>
BB URL:	<input type="text" value="https://cp1253.pushapi.na.blackberry.com"/>
BB application id:	<input type="text" value="1253-8719a7580ri086467oooco209r60880oa86"/>
BB password:	<input type="password" value="....."/>
Android key:	<input type="text" value="AIzaSyCWMrCle6zwXvpLWG-dxzzIwgklfiSCYUs"/>
Production environment:	<input type="button" value="No"/> ▼

107.9 iOS Users

A renewal of the certificate might be due to happen from time to time as for now this is a non permanent certificate. Instructions and file: [APNS Push Certificates](#)

Bear in mind that v4 has an Update available but for internal database type we suggest that you either update the appliance and get the newer version (4.0.5) or if you decide to go for the manual option we strongly advise you to change from Internal to Appliance Database - there is a known bug when tomcat is restarted for v4.0.4 using the Internal database - check: https://kb.swivelsecure.com/w/index.php/Migrate_How_to_guide

107.10 Android Users

For AuthControl Mobile App v5 please ensure you create a PNA_V5 as Push Transport. Open it and replace the Android key by the following: AIzaSyCWMrCle6zwXvpLWG-dxzzIwgklfiSCYUs

107.11 Testing

For testing OneTouch you can use [AuthControl Sentry](#) adaptative authentication system or [RADIUS with OneTouch](#) enabled.

107.12 Troubleshooting

Check the Swivel logs for error messages

Error Messages:

Calling or sending notification to user "push" failed, error: The transport destination is empty.

This error can be seen where the user is authentication with the PNA and if the Mobile device has not been provisioned.

Authentication failure. Please Reprovision the device

The mobile device needs to be provisioned.

The authentication request expired

The authentication request took too long to reach the Mobile Client and is no longer valid. A large time difference between the mobile client and the Swivel server can cause this error. To increase the value, change the PNA Transport Timeout (ms): to a larger value or to 0 to prevent timeout.

PNA user id error

The wrong User is associated with the Provisioned mobile device. Provision with the correct user.

Calling or sending notification to user "gfield" failed, error: The transport destination is empty.

This can be caused where the SSD has a value of false for Push. To allow OneTouch Mobile this value needs to be true. To check this, verify on the Swivel Administration Console User Administration, View by Attributes to see platform and push id.

108 How To Provision Mobile Apps

108.1 Provisioning Mobile Apps

This article sets out how to set up your Swivel installation to provision the Swivel AuthControl Mobile App using the preferred Quick Provision Approach.

To be able to use quick provisioning you'll first need to contact Swivel Secure to enable this feature if it hasn't been enabled.

Please note that quick provisioning only works with SMTP transports. You cannot provision a mobile app with SMS.

108.2 How it works

The provisioning works in the following way.

1. User is sent a Provision Message
2. User accesses the provision url on their mobile (by clicking the link or scanning the QR code)
3. Mobile accesses the url, that takes the device to the Swivel Mobile Client Server
4. Mobile downloads the specific server settings required for that client
5. Mobile then uses those settings to access the Swivel Core Server to be provisioned

For this process to work the Swivel server needs to be allocated a Site ID and have a method of sending the required message to the user to be provisioned.

108.3 Site ID

When the mobile app is provisioned, it contacts the Swivel Mobile Configuration (SMC) server and presents its Site ID, and in return is given the server settings for that customer. To request a site ID you need to send a request to Swivel Support and include the following details:

- The public hostname/ip address of the Swivel server, along with the port number, context, and where the server is set to use SSL. A typical entry would be

```
Host:      swivel.company.com
Port:      8443
Context:   proxy
SSL:       true
```

You may also optionally state two other settings to define whether you wish the clients to work in Local Mode and if you want to use One Touch

```
One Touch: true
Local:      false
OATH:       false
```

Swivel support will inform you of your Site ID and this needs to be enter on the Site ID field on the Server - Name screen.

Server>Name

Please enter the name by which this Swivel server should be known.

Site ID:

Server Name:

108.4 Provision URLs

The URLs that will be used to contact the Swivel SMC server are set under Policy -> Self Reset.

URL provisioning:	https://smc.swivelsecure.net/smc/provision/
URL to get settings:	https://smc.swivelsecure.net/smc/getsettings/
URL complete:	https://smc.swivelsecure.net/smc/complete/
QR Code URL:	https://smc.swivelsecure.net/smc/qrcode?text=

108.5 Quick Provision Link

If the user can access their email on their mobile device they can be sent an email that contains a url that will instigate the provision process. Alternatively this url can be sent as a Text Message.

To use this method of provisioning you need to ensure that on the Messaging configuration screen, eg Messaging -> SMTP, the following text is included:

To automatically provision your device, click the following URL: %URL_COMPLETE%SITE_ID/%NAME/%CODE

When the message is sent to the user the %URL_COMPLETE%SITE_ID/%NAME/%CODE will be replaced by the SMC url, the site-id, the user's username and the user's provision code.

108.6 QR Code

The other option is for the provision message to include a QR code that the user can scan from their Swivel Mobile App in order to start the provision process.

The Swivel User Portal includes an application that will display the QR code relevant to the provision message. This needs to be available via the internet so that the provision message can include a link to it. For example if your userportal is deployed as <https://portal.domain.com:8443/userportal>, then the QR code should be available from <https://portal.domain.com:8443/userportal/getQRCode?text=>

To use this approach the provision message must be in html format include text along the lines of

Click here to view QR Code: url4

When this message is sent to the user, url4 is replaced by the html required to pull in the image.

108.6.1 Note for 30-second timestep

If you select 30-second timestep mode, you must change the placeholder to url5. The default provision template contains url4, so make sure you look for that and change it. You should also remove the provision link, as it is not compatible with 30-second timestep mode.

108.7 Policies

There are a number of policies you can set around the provision and use of the Swivel Mobile App.

108.7.1 Provision Policies

These policy settings define how the provision process operates and are on the Policy -> Self Reset page

Allow user self-provision of mobile client:	<input type="button" value="Yes"/> ▼
Send provision code as security string:	<input type="button" value="No"/> ▼
Log device information when provisioning:	<input type="button" value="Yes"/> ▼
Provision Code Validity period (seconds):	<input type="text" value="360000"/>

Allow user self-provision of mobile client

If set to yes the user can, at any time, request a new provision code via the user portal. If set to no then once a user has provisioned a mobile device, the only way to provision a new device is via the admin console.

Send provision code as security string

If this is set to No, then the provision message will be sent to the same destination as all other alert messages, usually an email address. If this is set to yes then the provision message will be sent to the same destination as their security strings, usually a mobile phone number. This option allows the system administrator to ensure that provision messages are only sent to the users registered mobile device

Log device information when provisioning

If set to yes, any http headers parameters sent by the mobile device will be logged against that user's device. If a mobile client attempts to download security strings and presents a different set of headers to that that was logged when the device was provisioned, the request will fail

Provision Code Validity period (seconds)

108.7.2 Usage Policies

When a mobile client is provisioned it downloads a set of policies from the Swivel Server. These policies are set on the Policy->Mobile Client screen

Policy>Mobile Client

Set the polices to be downloaded to mobile clients

Allow user to enter PIN:	Yes ▾
Allow user to choose how to extract OTC:	Yes ▾
Allow user to browse strings:	No ▾
Provision is numeric:	No ▾
Show Settings:	No ▾
Sync Index:	No ▾
Support Email Address:	support@domain.com
Support Phone Number:	+44 1234 5678
VPN URL Scheme:	

ApplyReset

These policies are

Allow user to enter PIN

If the user has a PIN they can enter that PIN into the mobile client and it will extract the associated one-time code. If this policy is set to Npo, the user will be shown the security string and the user will have to perform the one-time extraction mentally.

Allow user to choose how to extract OTC

If the user is allowed to enter their PIN, if this policy is set to yes, the user can opt to disable PIN entry

Allow user to browse strings

The mobile client will work sequentially through the security strings that it has downloaded, however if this policy is enabled the user can browse through strings, eg skip strings. This maybe required where the user has to use a specific string in order to authenticate (eg for MSCHAP authentication)

Provision is numeric

Should the user need to enter their provision code manually, by setting this you yes the mobile client will display a numeric only keypad on the provision code entry screen

Show Settings

If Quick Provision is being used, there should be no reason for a user to be able to view their settings. However this policy enables the user to see these settings

Sync Index

Some RADIUS protocols work in such a way that only a specific security string can be used to authenticate. Syncing the index means the Swivel Mobile Client will always use the security string that the server is expecting. To Read more about Sync please go [here](#)

Support Email Address, Support Phone Number

These support details will be shown to the user when they access the help screen on the mobile client

VPN URL Scheme

Certain versions of the mobile client may support the launching of a VPN client. This setting defines the format used to enable this

108.8 Troubleshooting

A key question when diagnosing provisioning issues is to determine if the Swivel Client is contacting the Swivel server or not. If there are no log entries in the Swivel logs when the provision fails, it implies the error is a configuration or network issue prior to this stage in the process/

User clicks the link or scans the QR Code and nothing happens This implies the settings for the SMC server are not correct

User sees the initial config screen then provision fails with connection error Check site is set and site id settings are correct Check that the urls are accessible. To test this you can paste

`http(s)://<site id settings>/AgentXML?xml=?xml version="1.0" ?><SASRequest><Version>3.6</Version><Action>ping</Action></SASRequest>`

Where site id settings represents the server, port and context set for your server ID

You should see a response

```
<?xml version="1.0" encoding="UTF-8"?>
<SASResponse>
<Version>3.6</Version>
<RequestID/>
<Result>PASS</Result>
</SASResponse>
```

Check the validity of the certificate and also check that there are no issues in relation to weak ciphers or encryption standards

Invalid Provision Code If the user gets an invalid provision code check when the code was sent and how long the validity of the code is sent to. If this is an HA pair, need to ensure that the same appliance that issue the provision code also received the provision request from the mobile or that Session Synchronisation has been enabled/

109 Mobile Client Policies

110 Mobile Client Policy Overview

From Swivel 3.9.4 onwards the Swivel Mobile client can be configured with server settings that will be applied to all Mobile Clients.

This document supplements the existing documents for individual phone types.

Policy changes made on the server are applied to the clients when they provision the device or request new security strings.

111 Requirements

Swivel Mobile Client that supports PINsafe 3.8 or higher provisioning

Older Swivel appliances (2.0.12 and earlier) will need their proxy upgrade to handle the provisioning, see [Appliance Proxy Server Upgrade](#)

112 Swivel Configuration

112.1 Mobile Provisioning

Swivel 3.9.4 can be configured to allow users to enter a PIN for an automatic PIN extraction. On the Swivel Administration console select Policy/Mobile Client, the following options are available:

Allow user to enter PIN: Options Yes/No, Default No. If set to No, the user is not prompted to enter a PIN. If set to Yes, the user will be prompted to enter their PIN and will then be presented with a One Time Code.

Allow user to choose how to extract OTC: Options Yes/No, Default No. If set to No, the user cannot choose between automatic or manual PIN extraction. If set to Yes, then the user may choose the PIN extraction type on the Mobile client.

Allow user to browse strings: Options Yes/No, Default No. Version 3.9.6 onwards. This option allows the Mobile Phone App user to browse through the security strings. Availability to this feature is server controlled.

Policy>Mobile Client

Set the polices to be downloaded to mobile clients

Allow user to enter PIN:

Yes ▾

Allow user to choose how to extract OTC:

Yes ▾

Allow user to browse strings:

Yes ▾

Apply

Reset

113 Error Messages

114 Mobile Client Policies 2.0

115 Mobile Client Policy Overview

From Swivel 3.9.4 onwards the Swivel Mobile client can be configured with server settings that will be applied to all Mobile Clients.

This document supplements the existing documents for individual phone types.

Policy changes made on the server are applied to the clients when they provision the device or request new security strings.

116 Requirements

Swivel Mobile Client 2.0 that supports Swivel 3.10 or higher provisioning

117 Swivel Configuration

117.1 Mobile Provisioning

Swivel 3.10 has extended the mobile policies to allow the following policies to be set on a 2.0 mobile client.

Provision is numeric: Options Yes/No, Default No. If set to No, the keyboard type that will be displayed to the user on the mobile when entering a provision number will be alphanumeric. If set to YES then the keyboard type will be numeric.

Sync Index: Option Yes/No, Default No. Swivel version 3.10.3 onwards. This setting allows the mobile client to connect to the server to determine the next index code to be used. If set to Yes, when Swivel detects an authentication from the mobile client, it will allow the user to select the next **Security String** or **OTC**. If the index has not increased then the user will not be able to select the next code. If the Swivel server is not contactable, it will allow the user to browse their security strings.

Support Email Address: Option text, Default empty. If an email address is set, the user will be shown an option under the help section to contact support via email. The email is populated automatically and set in the users default mail client.

Support Phone Number: Option text, Default empty. If a phone number is set, the user will be shown an option under the help section to call customer support. The number is populated automatically and set in the users dialer ready to call.

VPN URL Scheme: Only For Iphone Option text, Default empty. If a VPN client is set, the user will be shown a VPN button on the OTC page. The VPN button will launch the mobile VPN client only if one is installed and supports the URL Scheme protocol.

The screenshot shows the 'Policy > Mobile Client' configuration page. The title is 'Policy > Mobile Client'. Below the title is a subtitle 'Set the policies to be downloaded to mobile clients'. The page contains several configuration options, each with a label and a corresponding input field or dropdown menu. The options are: 'Allow user to enter PIN:' with a dropdown menu set to 'Yes'; 'Allow user to choose how to extract OTC:' with a dropdown menu set to 'Yes'; 'Allow user to browse strings:' with a dropdown menu set to 'Yes'; 'Provision is numeric:' with a dropdown menu set to 'Yes'; 'Support Email Address:' with a text input field containing 'syed4@gmail.com'; 'Support Phone Number:' with a text input field containing '07905325768'; and 'VPN URL Scheme:' with a text input field containing 'citrixreceiver://auth?co'. At the bottom of the form are two buttons: 'Apply' and 'Reset'. The right side of the image is heavily distorted with digital noise.

Policy	Value
Allow user to enter PIN:	Yes
Allow user to choose how to extract OTC:	Yes
Allow user to browse strings:	Yes
Provision is numeric:	Yes
Support Email Address:	syed4@gmail.com
Support Phone Number:	07905325768
VPN URL Scheme:	citrixreceiver://auth?co

118 Messages

Pre Swivel 3.10 Users should still refer to the existing mobile client documentation [Mobile Client Policies](#)

119 Mobile Phone Client RADIUS Authentication

119.1 Overview

Mobile Phone Clients require the access device to use PAP authentication to provide a more resilient authentication.

With PAP authentication, the OTC and sequence number is sent to the PINsafe server for authentication. This allows for in and out of sequence OTC's to be used. With other forms of RADIUS authentication, the Access devices requests the expected OTC from the PINsafe server, and thus the next authentication must be the ext in sequence.

119.2 Prerequisites

PINsafe Mobile Phone Client or Swivlet

PINsafe 3.x

Access device using RADIUS authentication

119.3 Symptoms

User enters a OTC that sometimes fails to authenticate but appears correct

If an OTC code is entered out of sequence, the authentication fails.

119.4 Solution

Set the Access device to use PAP RADIUS authentication

Use another authentication method such as AGENT-XML

120 Mobile Provision Code

121 Mobile Provision Code Overview

121.1 Swivel Core Verion information

121.1.1 Swivel version 3.10.4

[QR Code Provision](#)

121.1.1.1 Swivel version 3.10

Swivel version 3.10 onwards supports one step Mobile Client Provisioning using a [Provision URL](#) and a [Site ID](#).

121.1.1.2 Swivel version 3.8

From Swivel 3.8 onwards the Swivel Mobile client must be provisioned to allow the Mobile client to download security strings for a user. The advantages of this are:

- A user cannot download another persons security strings
- Provisioning a mobile device prevents a user from downloading security strings to another device without being provisioned.

Each username may have one Mobile Client Provisioned. A request to provision a new mobile device or re-provision an existing mobile device that reaches the Swivel server will invalidate the current security strings. This article explains how to provision or re-provision a Swivel Mobile client.

This document supplements the existing documents for individual phone types.

For information on how a user can self provision or request a new provision code see [Mobile Re-Provision How to Guide](#)

122 Requirements

Supported [Mobile device](#)

Swivel Mobile Client installed that supports Swivel 3.8 or higher provisioning, see [Mobile Phone Client](#)

Swivel appliances will need their proxy upgrade to handle the provisioning, see [Appliance Proxy Server Upgrade](#)

If a Swivel cluster is configured with multiple servers, then session sharing should be enabled, otherwise the provision code is stored in memory and only valid on the Swivel instance that it is generated.

Ensure Provision code settings are configured across multiple Swivel instances.

122.1 Swivel Configuration

122.1.1 Mobile Provisioning

Swivel 3.8 and higher requires each mobile phone to be provisioned so it can be uniquely identified. Ensure that all Mobile Client users have suitable Transports configured to receive their Provision Code. To provision the mobile client on the Swivel Administration Console select User Management, locate the required user, click on the user to reveal the management functions and click Reprovision. The code sent to the user is valid for a length of time set under: Swivel Administration Console select Policy/Self-Reset. Earlier versions of Swivel do not need to use a Mobile Provision. From version 3.9.7 the user is sent a [Provision URL](#).



On the Swivel Administration Console log a message should indicate that the Mobile Provision Code has been successfully sent to the user:

Message sent to user: username, destination: username@emailaddress.com.

User "username" can now reprovision their mobile device.

Message added to message queue for user: username, destination: username@emailaddress.com.

Provision code created for user "username"

122.2 Mobile Self Provisioning

A user can be permitted to provision their own mobile device. To allow this, on the Swivel Administration Console select Policy/Self-Reset then set the following parameters as required:

Allow user self-provision of mobile client: Default No, Options Yes/No

Log device information when provisioning: Default No, Options Yes/No

Provision Code Validity period (seconds): Default 600, Options 10-1000000 Note: this value is for all Mobile Provision Codes.

To configure the self Provision/Re-provision see the [Mobile Re-Provision How to Guide](#)

122.3 Obtaining a Provision code using the Self Provisioning feature

A user should be able to access the Provision page of either the [User Portal](#) or from the resetPIN utility using <https://ApplianceIP:8443/reset/provision.jsp>. From version 3.9.7 this can be sent as a [Provision URL](#).

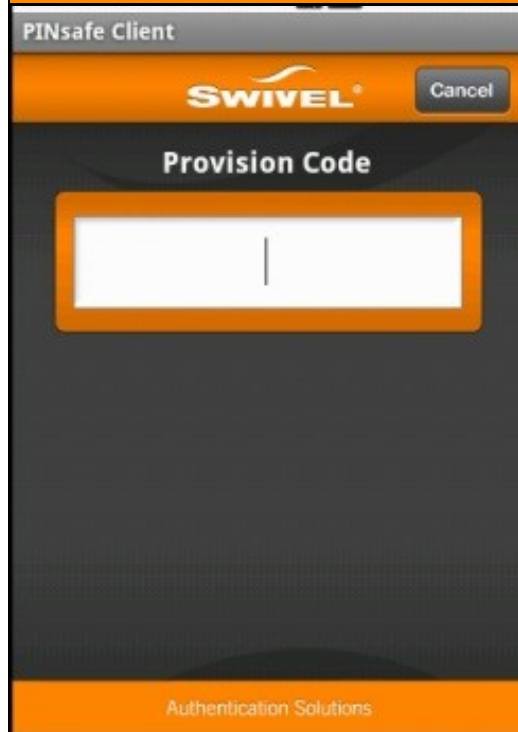
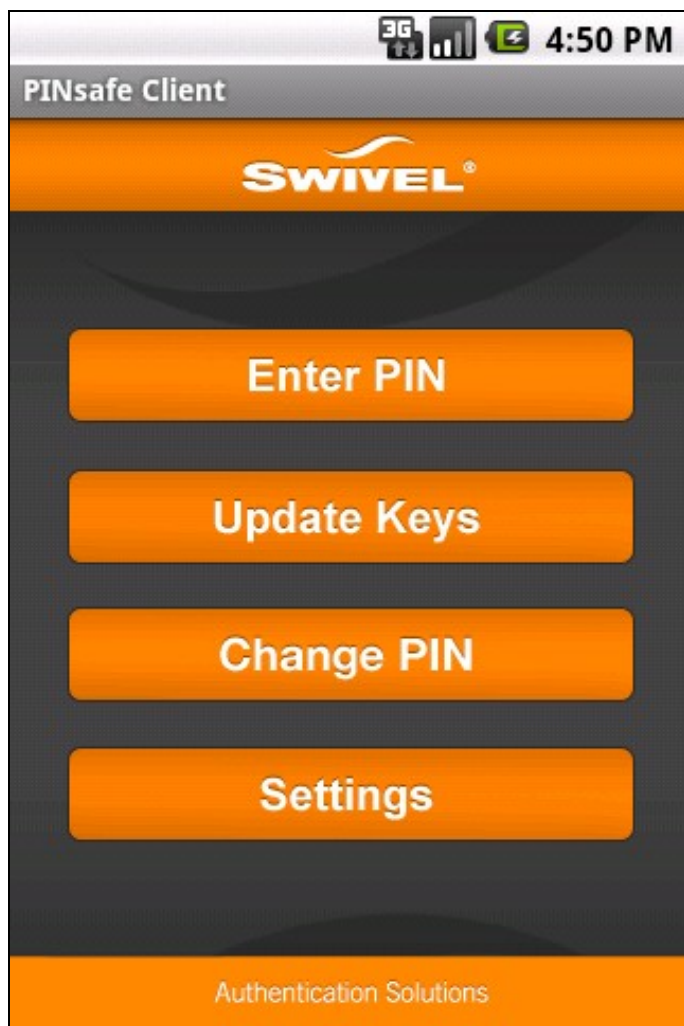
122.4 Mobile Client Configuration

If a [SSD](#) has been configured then the settings can be automatically pulled from the Swivel server, together with any [Mobile Client Policies](#).

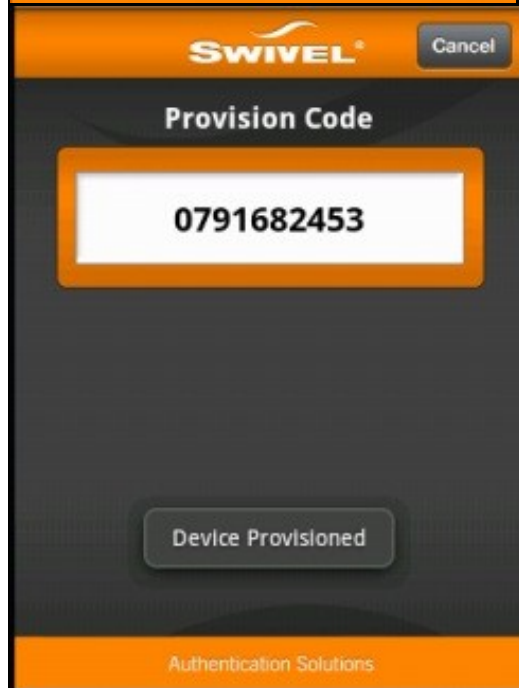
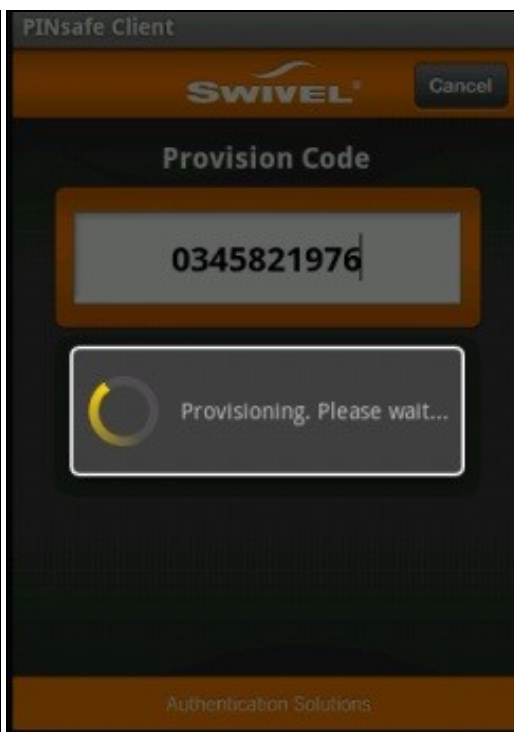
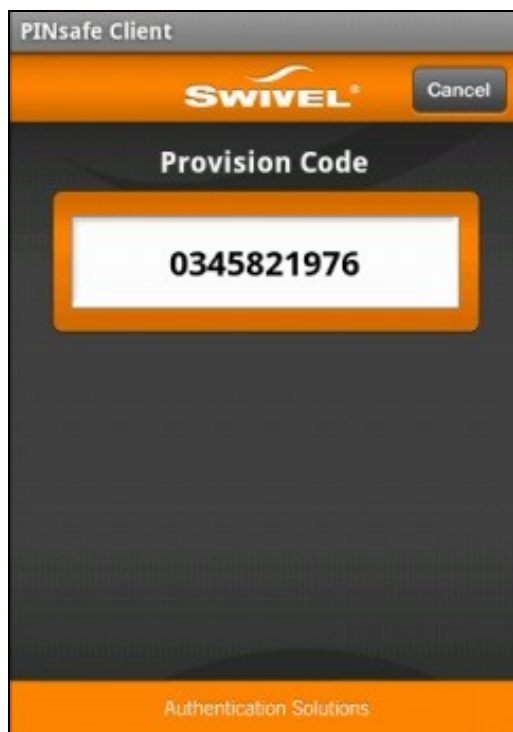
Mobile clients may have some variation.

Note: Re-Provisioning a mobile client will invalidate the current security strings for the client.

From the Swivel Mobile Client select settings, then select Re-Provision. A text box should appear to enter the Mobile Provision Code.



Enter the Mobile Provision Code and observe the screen input for a *Provisioning. Please wait...* message. When complete a *Device Provisioned* message briefly appears on the screen.



123 Verify Device Provisioning

On the Swivel Administration console, check the logs for a provisioning message:

User "gfield" provisioned successfully

124 Error Messages

Error Server, Unknown Server ID

The **Site ID** may not exist or may not have been entered.

Error Server Connection

The server details are missing or incorrect

Invalid Username

The User may not exist on the Swivel server.

Invalid Provision Code

The provision code is not valid or has already been used.

User not set

No username has been entered under options. Enter the username and retry.

Error Downloading Security Strings

The user may not be a member of an appropriate group with Mobile Client authentication enabled

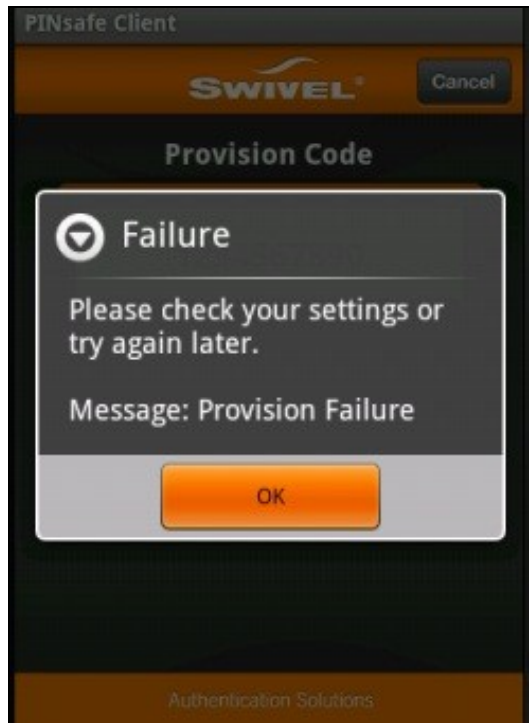
Failure Please check your settings or try again later. Message: Provision Failure

The following log message may be seen in the Swivel Administration Console:

User "gfield" provision failed, A valid session could not be loaded or created for the user.

This can be caused by an incorrect Mobile Provision Code, or the time allowed for provisioning a device has been exceeded.

Note: The security strings on the mobile phone will be invalid until a successful provision is carried out and a new set of security strings are downloaded.



AgentXML request failed, error: No suitable authentication method for the user "qwerty" was found. The user may be missing from the user repository or a synchronisation has not yet occurred.

or

Mobile request from unknown user; the user needs to reprovision

A Mobile Provision Code was entered for a user who is not present on the Swivel user database.

125 Category:Swivel Policy Mobile

126 Category:Windows

127 Windows Mobile How To Guide

129 Overview

NOTE: this version is for Windows Mobile versions 6.x and earlier. For Windows Phone 7.x, see [Windows Phone 7 How To Guide](#).

The Windows Mobile Swivel application, for the Windows Mobile phone allows the storage of 100 security strings or One Time Codes for PINless authentication on a .Net mobile phone. The PIN is not stored on the phone. Requesting a top up from the Swivel server resets all the security strings on the mobile phone. You can use the device to get one-time codes for Swivel login and PIN change.

For the Mobile Phone Clients such as the Java based version select [Swivlet How To Guide](#). For other phones see [Mobile Phone Client](#).

130 Prerequisites

User must have Mobile Phone Client or Swivlet enabled to use this application

The Swivel server must be reachable from the mobile phone to receive security strings

Security strings must be entered including the comma and sequence number e.g. nnnn,nn

This application is not compatible with Swivel 3.8 or later

RADIUS authentications made against Swivel must use PAP RADIUS authentication since with other RADIUS protocols such as CHAP and MSCHAP the access device requests the OTC from Swivel.

130.1 Mobile App Store versions

- "Swivel Mobile Client" which is compatible with Windows 8 phones but not Windows 7 phones.
- "Swivel" which is compatible with Windows 7 phones but not Windows 8 phones.
- "Swivel Mobile" which is compatible with Windows 8 phone only and not a Windows 7 phone.

131 Swivel Configuration

131.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance

To allow a user to authenticate using a One Time Code from the Mobile Phone Client, the user must have the Mobile Client authentication enabled. To do this on the Swivel Administration console ensure that the group they are part of has access to the Mobile Client under Repository Groups.

131.2 Configuring the Swivel Authentication

Swivel can authenticate users using the mobile client to authenticate by RADIUS or Agent-XML authentication

- For RADIUS authentication see [RADIUS Configuration](#) Note: The access device must be configured to use PAP for authentication.
- For Agent-XML authentication see [XML Authentication Configuration](#)

131.2.1 Mobile Provisioning

Swivel 3.8 and higher requires each mobile phone to be provisioned so it can be uniquely identified. Ensure that all Mobile Client users have suitable Transports configured to receive their Provision Code. To provision the mobile client select the user and click Re-provision. Earlier versions of Swivel do not need to use a Mobile Provision Code. See [Mobile Provision Code](#).

131.2.2 Mobile Client Policies

For the Server based policies see [Mobile Client Policies](#)

132 Windows Mobile Installation

To install it, you need either ActiveSync or Windows Mobile Device Centre installed on your computer (the latter is for Vista and Windows 7). Attach the mobile device to your computer, and copy the attached .cab file to it. Execute the cab file to install the Mobile Phone Client. You can remove the cab file once it is installed.

The first time this application is used, it must be configured with the details of the Swivel server. If a **SSD** server is being used, then select **Get Server Settings** and enter the Server ID, otherwise the settings can be manually entered with information from the Swivel System administrator by choosing the Configuration. Your administrator will provide you with these.

Once the Swivel server details are configured, for Swivel version 3.8 or later, you must provision your phone before you can request security strings. Press **Provision** to provision this phone with the Swivel server. You will need to request a provision code from your helpdesk, which must be used immediately. The code will be sent either to your phone as an SMS, or via email, depending on how your Swivel server is configured. Provisioning is not necessary for versions of Swivel earlier than 3.8.

Set the configuration as appropriate (note that the Swivel server must be publicly visible for the Mobile Phone Client to work, or else the phone must be able to access the Swivel server via the internal network). Once the device is configured, select the Top Up option to download 100 security strings to the phone. The phone doesn't need access to the Swivel server again until it runs out of strings and you need to Top Up again.

The **Beta** version of the software can be downloaded here: <http://www.swivelsecure.com/userfiles/File/software/beta/SwivletDeploy.zip>

133 Testing

You can top up the Mobile Phone Client and you should see a log message saying strings requested for user XXXX.

Send a user a provision code, the following should be displayed in the Swivel logs:

User "username" can now reprovision their mobile device

The user has been sent a provision code to provision their mobile client

User "username" provisioned successfully

The user has successfully provisioned their Mobile Phone Client, this message is displayed in the Swivel Administration console log.

134 Troubleshooting

Is the Swivel server accessible on the internet

Check the connection settings to the Swivel server

Check the Swivel logs for any error messages

Can the phone access the internet

Does the Swivel applet application have authorisation to access the network connection

Can the phone use self signed certificates if a https connection is being used

If a RADIUS connection is seen from the access device to the Swivel server but authentication fails, try using PAP

Download new security strings to the phone and retest

If the proxy port (8443) on the virtual or hardware appliance is being used, ensure that it supports the proxy request of the key retrieval using AgentXML. If this is the case then contact Support for an updated version of the Proxy.

Login fails and User receives a security string or One Time Code by SMS or email at each login attempt. The index is required to be entered as nn on the end eexample: 292401, Swivel versions earlier than 3.10 require ,nn example: 2924,01 otherwise it will see it as a dual channel authentication.

134.1 Known Issues

If you have a self-signed certificate - even if you check the box to use a self signed certificate it will ignore this setting due to a problem with the .NET framework.

134.2 Error Messages

Mobile request from unprovisioned device; the user username needs to complete the reprovision process

Security strings are being requested by an unprovisioned device. The user needs to provision the Mobile Phone Client.

User "username" provision failed, A valid session could not be loaded or created for the user

The provisioning of the Mobile Phone Client has failed, either an incorrect provision code was used or the provision code has timed out.

AGENT_ERROR_NO_SECURITY_STRINGS, AGENT ERROR NO SECURITY STRINGS

The OTC is being entered without the ,nn at the end of the OTC, whereby nn is the number given with the security string

AGENT_ERROR_SESSION

Provisioning of Mobile Phone Client attempted without Provision code. Ensure user attempts with a valid provision code.

NOT FOUND

Provisioning error, this is displayed in the Swivel Windows Mobile Phone Client version 1.0 and is resolved by upgrading to version 1.2 or higher.

135 Tested Mobile Phones

As more information is fed back additional phones will be added here.

Mobile Phone Compatibility

Manufacturer	Model	Version	Windows Mobile Version	Operator	Compatible Y/N	.Net Applet Version
Samsung	Omnia	Not Known	6.5	Not Known	Y	Not Known

136 RADIUS Considerations

One thing to be aware of is that when using RADIUS authentication, except for the PAP protocol, you must use every string from the phone for authentication. If you generate a string and don't use it, authentication will fail until you Top Up again. This is an unavoidable consequence of the way most RADIUS protocols work.

137 Windows Phone 7 How To Guide

138 Overview

The Swivel Windows Phone 7 Mobile client allows the storage of 100 security strings on a Windows Phone 7 (and 7.5). The PIN is not stored on the phone. Requesting a top up from the Swivel server resets all the security strings on the mobile phone. You can use the device to get one-time codes for Swivel login and PIN change. The app is available for Windows 7 Phones as Swivel, for Windows 8 phones use the **Swivel Mobile Client**.

139 Prerequisites

This application is for phones running Windows Phone 7.x only

User must have Mobile Phone Client or Swivlet enabled to use this Application

The Swivel server must be reachable from the mobile phone to receive security strings

The index is required to be entered as nn on the end example: 292401, Swivel versions earlier than 3.10 require ,nn example: 2924,01 otherwise it will see it as a dual channel authentication.

This application is compatible with versions of Swivel from 3.2 onwards. To download security strings from Swivel versions 3.8 onwards, the phone must be provisioned first. For versions 3.7 and earlier, provisioning is not required or supported.

Appliances using Swivel 3.8 may require an upgrade on their proxy to provision a mobile device, see [Appliance Proxy Server Upgrade](#)

RADIUS authentications made against Swivel must use PAP RADIUS authentication since with other RADIUS protocols such as CHAP and MSCHAP the access device requests the OTC from Swivel.

139.1 Mobile App Store versions

- "Swivel Mobile Client" which is compatible with Windows 8 phones but not Windows 7 phones.
- "Swivel" which is compatible with Windows 7 phones but not Windows 8 phones.
- "Swivel Mobile" which is compatible with both Windows 8 phone only and not a Windows 7 phone.

140 Swivel Configuration

140.1 Configuring Mobile Client user access on the Swivel appliance

To allow a user to authenticate using a One Time Code from the Mobile Phone Client, the user must have the Mobile Client authentication enabled. To do this on the Swivel Administration console ensure that the group they are part of has access to the Mobile Client under Repository Groups.

140.2 Configuring the Swivel Authentication

Swivel can authenticate users using the mobile client to authenticate by RADIUS or Agent-XML authentication

- For RADIUS authentication see [RADIUS Configuration](#) Note: The access device must be configured to use PAP for authentication.
- For Agent-XML authentication see [XML Authentication Configuration](#)

140.2.1 Mobile Provisioning

Swivel 3.8 and higher requires each mobile phone to be provisioned so it can be uniquely identified. Ensure that all Mobile Client users have suitable Transports configured to receive their [Mobile Provision Code](#). To provision the mobile client select the user and click Re-provision. Earlier versions of Swivel do not need to use a Mobile Provision Code. See [Mobile Provision Code](#).

140.2.2 Mobile Client Policies

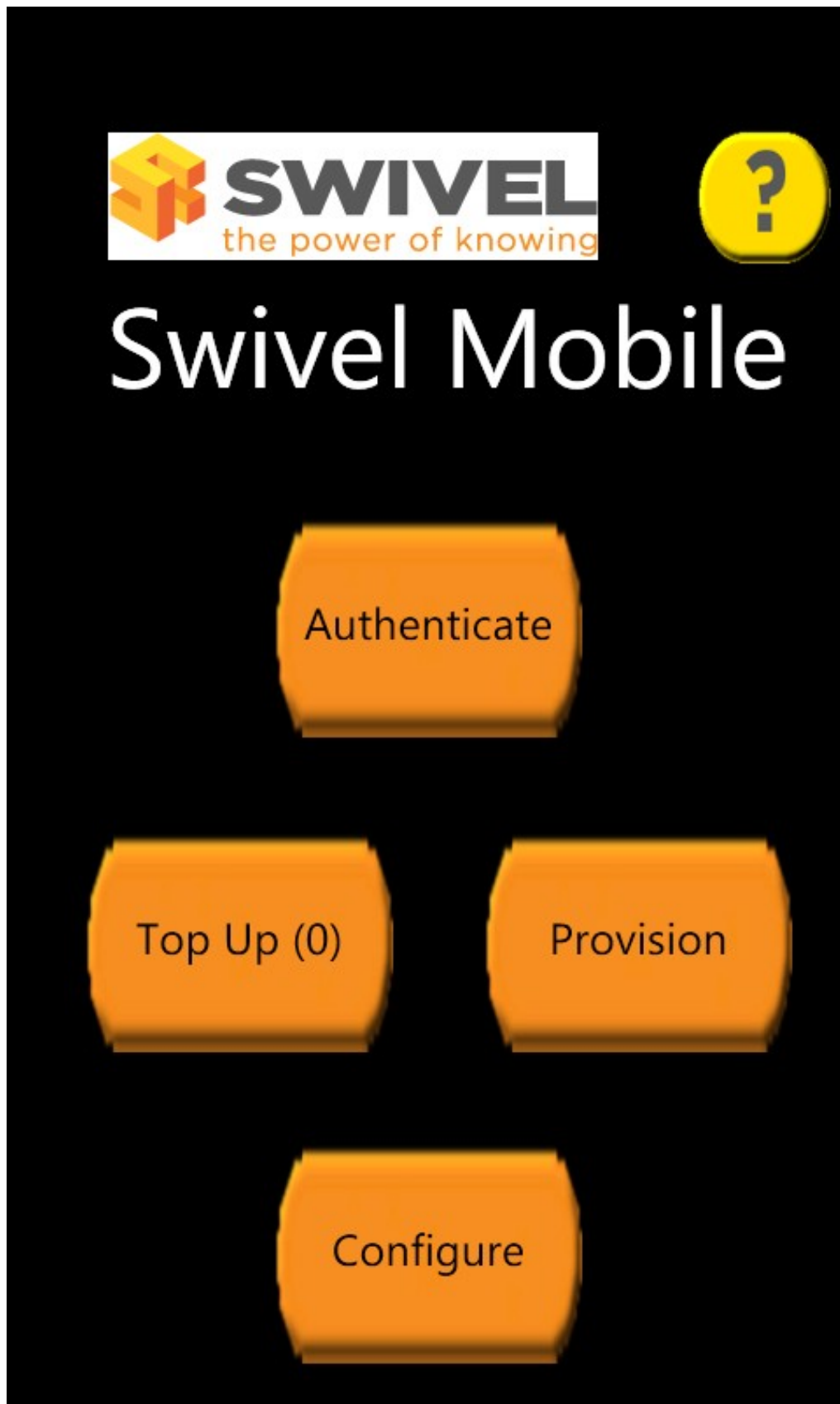
For the Server based policies see [Mobile Client Policies](#)

141 Getting the Application

The application must be downloaded from Windows Marketplace. Search for "Swivel".

142 Using the Application

When you start the application, you will see the following screen:



Help is available from the application on all pages by pressing the ? button at the top right.



The first time this application is used, it must be configured with the details of the Swivel server. If a **SSD** server is being used, then select **Get Server Settings** and enter the Server ID, otherwise the settings can be manually entered with information from the Swivel System administrator by choosing

the Configuration. Your administrator will provide you with these.

Once the Swivel server details are configured, for Swivel version 3.8 or later, you must provision your phone before you can request security strings. Press **Provision** to provision this phone with the Swivel server. You will need to request a **Mobile Provision Code** from your helpdesk, which must be used immediately. The code will be sent either to your phone as an SMS, or via email, depending on how your Swivel server is configured. Provisioning is not necessary for versions of Swivel earlier than 3.8.

Once the phone is provisioned, you can request new security strings. Press the **Top Up** button to do this. Your phone will be pre-loaded with 100 new security strings.

Once you have carried out the 3 steps above, you can use the **Authentication** button to request security strings one at a time for Swivel authentication. Your phone will not need to connect to the Swivel server again until you have used all your strings.



Configuration

Server:

Port:

Context:

☒ SSL

☐ Allow self-signed

Username:

Enter the Swivel server details on this page.

You will need to get the server details from your system administrator.

WARNING: the "Allow self-signed" option does not work. Unfortunately, there is no way on a Windows Phone 7.x to connect to a web server over HTTPS if the SSL certificate is not valid. There may also be a problem with some servers, even if the certificate is valid, due to an issue with TLS Server

Name Indication (SNI). This has been observed and fixed on the Swivel Taskbar client for Windows 7 (desktop), but unfortunately the same fix cannot be used on Windows Phone. In this case, the only fix is on the server side: either disable HTTPS or ensure that the server (or firewall if Swivel is being proxied) either has SNI (or TLS) disabled, or has the correct server name(s) configured.



Provision

Provision Code:

1234567890



Before you can request security strings, you must provision your phone with the PINsafe server (PINsafe version 3.8 or later). Make sure that the phone is properly configured with the Swivel server details before doing this.

Ask your administrator or helpdesk to send you a provision code. You will receive this via SMS or email, depending on the configuration of your Swivel server. You must enter this code into this phone as soon as you receive it, as it has a limited lifespan.



Top Up Strings

Top Up

Cancel

Use this page to request more security strings. Before you do this, make sure your phone is correctly provisioned with the PINsafe server (PINsafe version 3.8 or later).

Click **Top Up** to request more strings. If successful, you will be sent 100 new strings. Any previous strings you had been issued with will no longer be valid.



Authentication

Get Next String

Security String:

1	2	3	4	5	6	7	8	9	0
-	-	-	-	-	-	-	-	-	-

Index:

--

Back

To get the next available security string, click *Get Next String*. You will be shown the next string and its index.

To authenticate, calculate your one-time code from the security string, then append "," and the 2-digit index shown.

For example, if the security string is "2468013579", the index is "02" and your PIN is 1357, the authentication code will be "2603,02".

146.1 Change PIN

To change your PIN, you need to apply the same process to both the current and the new PIN. Use the same security string for both PIN's.

For example to use the string above to change your PIN, if your existing PIN is 1357 and your new PIN will be 2468, use "2603,02" as your old one-time code, and "4815,02" as your new one-time code.

147 Known Issues

Allow self-signed Certificate does not work with the Windows Phone, where HTTPS is used a valid certificate must be used.

Windows Phone does not support connecting to HTTPS servers with certificate errors. If you are publishing a Swivel server using HTTPS, make sure that the certificate is valid, and that you use the correct host name when configuring the client.

If you are using a proxy server that supports TLS for HTTPS connections, be aware that you must configure the correct host name for server name indication (SNI), or the phone will reject the connection. There is no way to disable this, or to force the connection to use SSL instead of TLS.

We have had reports that this application is not available in all markets. To the best of our knowledge, the application should be available in all countries supported by the Microsoft Market Place, but if you have difficulty finding the application in your country, please let us know through support@swivelsecure.com, so that we can investigate the problem.

148 Troubleshooting

The remote server returned an error: Notfound

The Swivel server cannot be contacted. This may be due to certificate errors described above.

Login fails and User receives a security string or One Time Code by SMS or email at each login attempt. The index is required to be entered as nn or ,nn example 2924,01 otherwise it will see it as a dual channel authentication.

149 Windows Phone(8) 2.0 How To Guide

150 The Swivel Windows Phone 8 2.0 App Overview

Swivel Secure now offers a Windows Phone 8 mobile client for use with the Swivel platform. This article explains how to download, configure and use this client. For other phones see [Mobile Phone Client](#) for earlier versions.

151 Requirements

Swivel 3.10 or higher

Windows Phone 8, Q10, Bold, Curve, 8210

The Swivel virtual or hardware appliance must be reachable from the mobile phone to receive security strings

The index is required to be entered as nn on the end example: 292401, Swivel versions earlier than 3.10 require ,nn example: 2924,01 otherwise it will see it as a dual channel authentication.

Valid certificate on the Swivel server or non SSL, but not a self signed certificate

152 Versions

version 2.1.1 released: 05/02/2014

- QR Code Provision
- Push Authentication Support

version 2.0 released

- Simple User Interface
- Extra Mobile Policies
- Help Section
- Citrix Receiver VPN Client support (iPhone Only)
- Removal of comma from OTC,

152.1 Which version do I need?

Pinsafe version 3.10 or later, Mobile Client 2.0

Windows Phone 8 Mobile Client 2.0 version 2.0

152.2 Mobile App Store versions

- "Swivel Mobile Client" which is compatible with Windows 8 phones but not Windows 7 phones.
- "Swivel" which is compatible with Windows 7 phones but not Windows 8 phones.
- "Swivel Mobile" which is compatible with both Windows 8 phone only and not a Windows 7 phone.

153 Swivel Configuration

153.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance

To allow a user to authenticate using a One Time Code from a mobile app, the user must have Mobile app authentication enabled. To do this on the Swivel Administration console ensure that the group they are part of has access to the Mobile Client under Repository Groups.

153.2 Configuring the Swivel Authentication

Swivel can authenticate users using the mobile client to authenticate by RADIUS or Agent-XML authentication

- For RADIUS authentication see [RADIUS Configuration](#) Note: The access device must be configured to use PAP for authentication.
- For Agent-XML authentication see [XML Authentication Configuration](#)

Allow user to browse strings: Options Yes/No, Default No. Version 3.9.6 onwards. This option allows the Mobile Phone App user to browse through the security strings. Availability to this feature is server controlled.

153.3 Mobile Provisioning

Swivel 3.8 and higher requires each mobile phone to be provisioned so it can be uniquely identified. Ensure that all Mobile Client users have suitable Transports configured to receive their Provision Code. To provision the mobile client select the user and click Re-provision. Earlier versions of Swivel do not need to use a Mobile Provision Code. See [Mobile Provision Code](#).

153.3.1 Mobile Client Policies

For the Server based policies see [Mobile Client Policies 2.0](#) for previous versions see [Mobile Client Policies](#)

154 Windows Phone 8 Installation and Configuration

The Swivel Windows Phone 8 Client 2.0 is available from the Windows App Store. You can click the icon below to open the App within the windows app store, or follow the instructions in this article to navigate to the App within the App Store.

154.1 Download compatible with Swivel 3.10 onwards

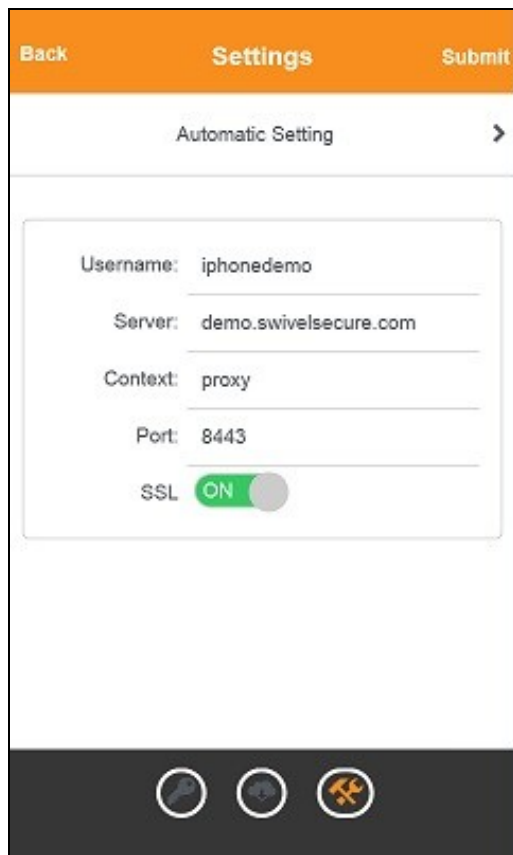


154.2 Configuring the app

When you launch the app you will see the helper wizard, at the bottom of the screen there will be menu icons to guide you through the mobile client options.

154.2.1 Get Server Settings

If an [SSD](#) server is being used, select **Get Server Settings** and enter the Server ID. Otherwise the settings can be manually entered with information from the Swivel System administrator.



The settings are

1. Username: Your username that you use when you authenticate via Swivel
2. Server: The URL from where the client can download security strings (or keys)
3. Context: The context used by the web service. For a virtual or hardware appliance this is **proxy**, for a software install this is usually **pinsafe**
4. Port: The port number used by the web service. For an virtual or hardware appliance this is **8443**, for a software install this is **8080**

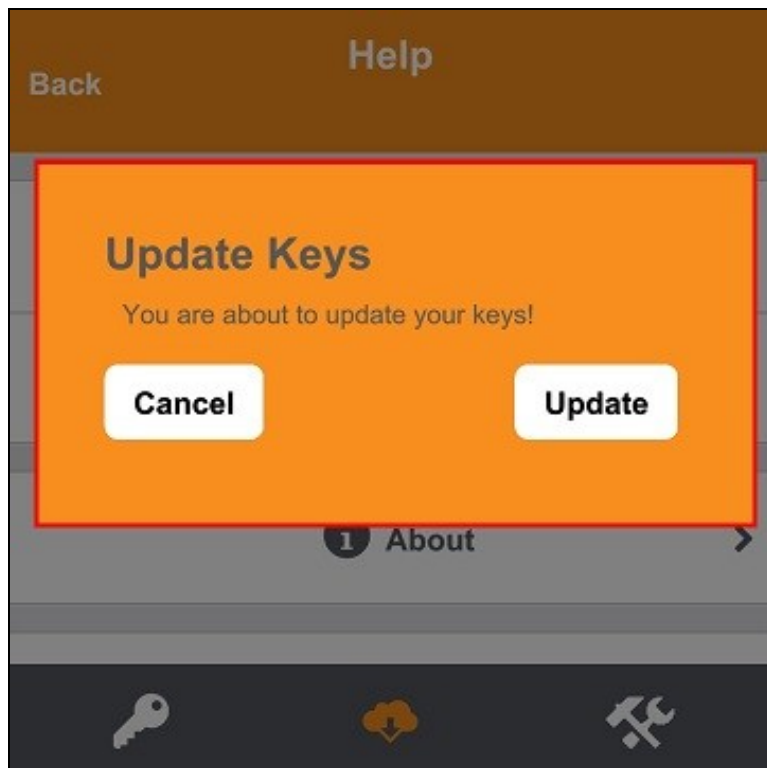
Once you have entered the settings you can select Submit in the header location of that page.

154.3 Mobile Provision Code

Swivel versions 3.10 and higher require each Mobile device to be Provisioned with a Code sent from the Swivel server. To provision a phone see [Mobile Provision Code](#).

154.4 Downloading Security Strings

From the bottom menu there is a update keys button, pressing this will get you a new set of 99 security strings. This will attempt to retrieve Security Strings from the Swivel server.



If there are any problems and error message will be displayed

You can confirm that keys have been downloaded by checking the server logs

The Swivel server will display the following log message **Security strings fetched for user: username**

154.5 Options

The following options are available:

Auto extract OTC, Prompt for PIN Number to auto-extract OTC. Options, enable/disable. This option may be turned off on the Swivel server. When enabled this allows the user to enter their PIN number and a One Time Code will be displayed. Note that there is no error checking of the PIN, so if an incorrect PIN is entered an incorrect One Time Code will be displayed.

Allow String Browsing, This is a Swivel server controlled option, which if enabled will allow the user to browse through security strings on the mobile app.

Provision is numeric, allows the keyboard type to be either alpha numeric of numeric depending on the users provision code type.

Set Support Email Address. **Set Support Phone Number.** **Set VPN client URL.**

154.6 Authenticating with app

To use the Swivel Windows Phone 8 app to authenticate is very simple.

1. Open the app. on your Windows Phone 8.
2. Select the key icon on the bottom menu.
3. Depending on your policy settings you will either be prompted for a PIN or immediately shown a One-Time-Code (OTC).
4. If you are asked for a PIN, enter the PIN number previously sent during the enrolment phase.
5. Enter the OTC into the authentication dialogue, make sure you enter all the characters.

If you need to authenticate again you can select the '<' or '>' button and a new string will be displayed (you may have to enter your PIN again).

Enter PIN

Please enter your PIN and press submit

1

2

3

4

5

6

7

8

9


Submit

0

Clear









OTC


<


 342801

>

This is your One Time Code (OTC).







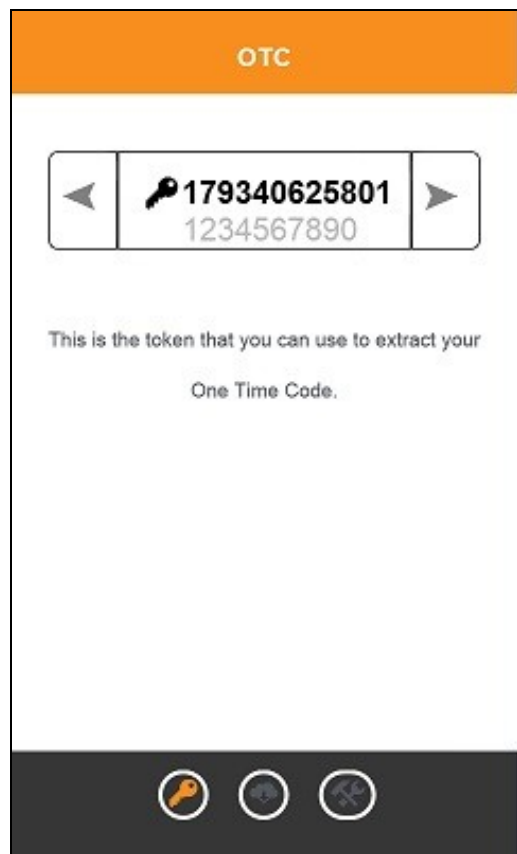
154.7 Authenticating with app and PINsafe

To use the Swivel Windows Phone 8 app to authenticate is very simple.

1. Open the app on your Windows Phone 8.

2. Select the key icon on the bottom menu.
3. The client will show a security string with a row of placeholders 1234567890 below it.
4. Use your PIN to extract your One-Time-Code (OTC), eg if your PIN is 2468 take the 2nd 4th 6th and 8th characters of the security string.
5. In the example screen shoot the OTC would be: 1825.
6. After the OTC has been worked out, you will also need to ensure you type in the last two characters shown (the index).
7. Using the example screen shot you would type 182512.

If you need to authenticate again you can select the '<' or '>' button and a new string will be displayed.



154.8 Updating Keys

The client downloads 99 keys at a time and these keys are used one at a time until there are none left. However a new set of 99 keys can be downloaded at any time by selecting Update Keys. Downloading keys requires network connectivity so it is recommended that you download a new set of keys before the Windows Phone 8 is likely to be without network connectivity for any length of time.

155 Troubleshooting

- Is the Swivel server accessible on the internet
- Check the connection settings to the Swivel server
- Check the Swivel logs for any error messages
- Can the phone access the internet
- If a RADIUS connection is seen from the access device to the Swivel server but authentication fails, try using PAP
- Download new security strings to the phone and retest
- Is the pin 6 characters when you only entered a 4 digit pin? If yes then enter all of the numbers you see on screen (the extra 2 are used as an index).
- Login fails and User receives a security string or One Time Code by SMS or email at each login attempt. Again make sure you are entering all of the numbers shown on screen.
- If the proxy port (8443) on the virtual or hardware appliance is being used, ensure that it supports the proxy request of the key retrieval using AgentXML. If this is the case then contact Support for an updated version of the Proxy.

155.1 Device fails to Quick Provision

If the mobile device fails to quick provision and displays the provision information but the input fields cannot be edited, it may be that the Internet Explorer on the Windows Mobile is setup to use Desktop mode and for this reason they cannot see the button. This has been seen on a Nokia Lumia. Take the following steps to change this to the Mobile Version:

- a. Go to Internet Explorer.
- b. Click 'More'.
- c. Click Settings.
- d. Website preference > change to mobile version.

155.2 Error Messages

Incorrect settings - please check your settings

The settings for downloading the security strings are incorrect. Verify what has been entered, and check what the values should be.

Timed Out

The settings for connecting to the Swivel server may be incorrect or the port is being blocked.

AGENT_ERROR_NO_SECURITY_STRINGS, AGENT ERROR NO SECURITY STRINGS

See [AGENT ERROR NO SECURITY STRINGS](#)

156 Tested Mobile Phones

The following phones have been tested

Mobile Phone Compatibility

Manufacturer	Model	Version	Operator	Compatible Y/N
Windows Phone 8	Lumina	-	Y	
Windows Phone 8	Lumina	-	O2	Y
Windows Phone 8	Lumina	-	Vodafone	Y

- The current version only supports one device per user.

Keywords: Windows Phone 8, Lumina, AppStore

157 Legacy

Download compatible with Swivel 3.10 and later.

