Table of Contents

1 2.0 Mobile Clients Administration **1**

2 The Swivel iPhone App v2 Overview **2**

3 Requirements **3**

4 Versions **4**
4.1 Which version do I need? 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
5.3 Mobile Provisioning 5

6 iPhone Installation and Configuration **6**
6.1 Download compatible with Swivel 3.8 onwards 6
6.2 Configuring the app 6
6.3 Mobile Provision Code 7
6.4 Downloading Security Strings 7
6.5 Options 7
6.6 Authenticating with app and PINsafe 7
6.7 Updating Keys 8

7 Troubleshooting **9**
7.1 Error Messages 9

8 Tested Mobile Phones **10**

9 Known Issues and Limitations **11**

10 Legacy **12**

11 Citrix Receiver **13**

12 Introduction **14**

13 Prerequisites **15**

14 iPhone / Android Citrix receiver **16**

15 Citrix Netscaler RADIUS authentication for Receiver **17**

16 Citrix Access Standard Edition Gateway RADIUS authentication for Receiver **18**

17 Citrix Access Advanced Edition Gateway RADIUS authentication for receiver **19**

18 Known Issues and Limitations **20**

19 IPad Citrix Receiver **21**

20 IPhone **22**

21 The Swivel iPhone App Overview **23**

22 Requirements **24**

23 Versions **25**
23.1 Which version do I need? 25

24 Swivel Configuration **26**
24.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance 26
24.2 Configuring the Swivel Authentication 26
24.3 Mobile Provisioning 26

25 iPhone Installation and Configuration **27**
25.1 Download compatible with Swivel 3.8 to 3.9 27
25.2 Configuring the app 27
25.3 Mobile Provision Code 28
25.4 Downloading Security Strings 28
25.5 Options 28
25.6 Authenticating with app and PINsafe 28
25.7 Updating Keys 29

26 Troubleshooting **30**
26.1 Error Messages 30

27 Tested Mobile Phones **31**

28 Known Issues and Limitations **32**

29 Legacy **33**

30 IPhone 2.0 ..... **34**

Table of Contents

31 The Swivel iPhone 2.0 App Overview **35**

32 Requirements **36**

33 Versions **37**
33.1 Which version do I need? 37

34 Swivel Configuration **38**
34.1 Configuring Mobile Client user access on the Swivel virtual or hardware appliance 38
34.2 Configuring the Swivel Authentication 38
34.3 Mobile Provisioning 38

35 User Experience with 'Quick Provisioning' **39**

36 iPhone Installation and Configuration **40**
36.1 Download compatible with Swivel 3.10 onwards 40
36.2 Configuring the app 40
36.3 Mobile Provision Code 41
36.4 Downloading Security Strings 41
36.5 Options 41
36.6 Authenticating with app 42
36.7 Authenticating with app and Swivel 42
36.8 Updating Keys 43

37 Troubleshooting **44**
37.1 Error Messages 44

38 Known Issues and Limitations **45**

39 Legacy **46**

40 Mobile Phone Client **47**

41 Mobile Phone Client 2.x **48**
41.1 Overview 48
41.2 Integrating with the Mobile App 48

42 Mobile Phone Client 1.0 ..... **49**
42.1 Overview 49
42.2 Integrating with the Mobile App 49

1 2.0 Mobile Clients Administration

2 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.

3 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

4 Versions

version 2.0 BETA release around 1st May 2014

- Navigate back and forward through security strings
- URL provisioning

4.1 Which version do I need?

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

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 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.

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 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.

5.3 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.

5.3.1 Mobile Client Policies

For the Server based policies see Mobile Client Policies

6 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.

6.1 Download compatible with Swivel 3.8 onwards

6.2 Configuring the app

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

6.2.1 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.

6.3 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.

6.4 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**

6.5 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 ths 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.

6.6 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

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 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.

7 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 eaxample: 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

7.1 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

8 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	Deutche Telekom	Y

The iPhone applet will also work on the iPad

9 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

10 Legacy

Download compatible with Swivel 3.7 and earlier

11 Citrix Receiver

[[Category:android|A]

12 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

13 Prerequisites

Citrix receiver Client

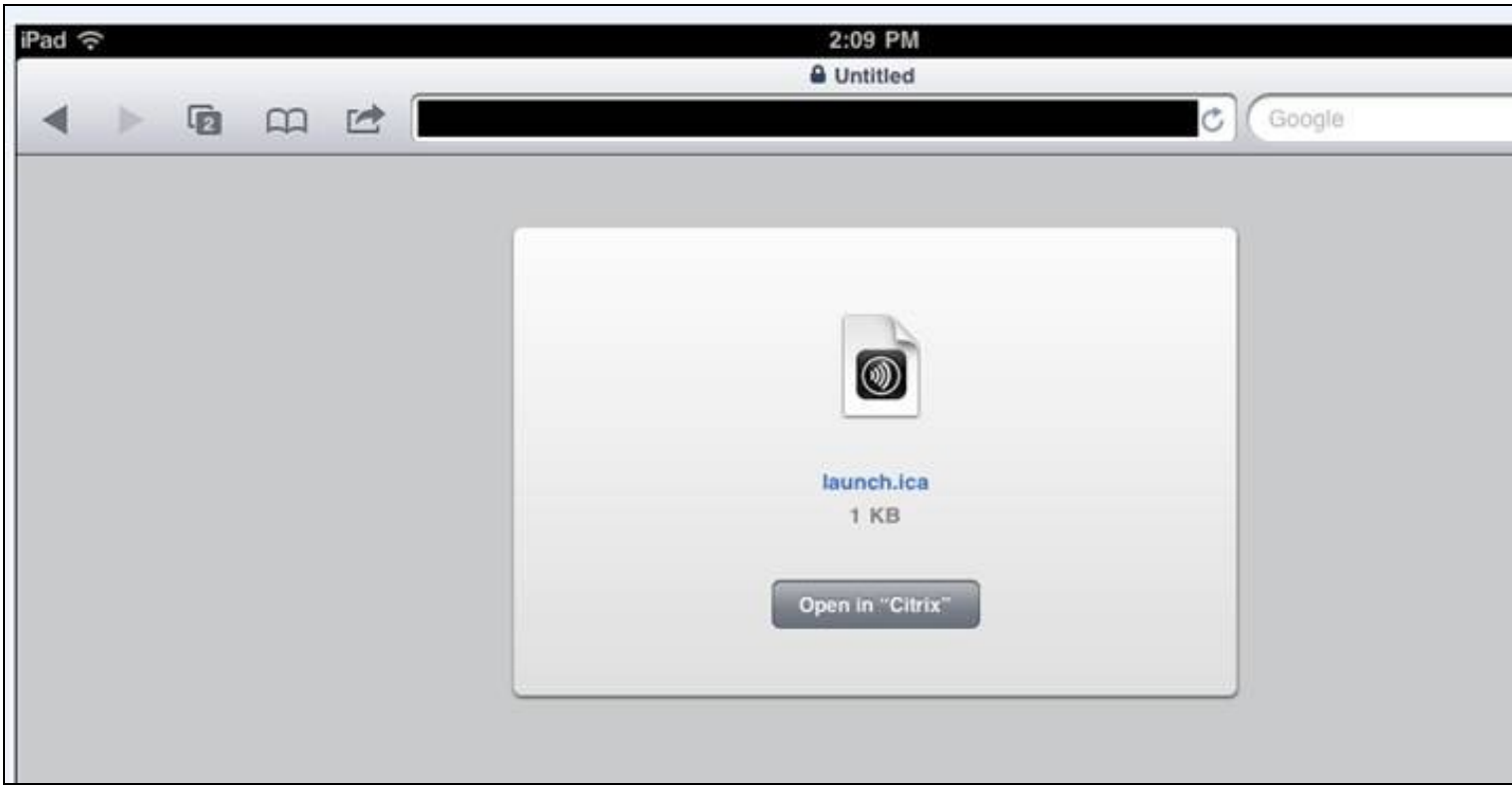
Swivel Appliance or Server

Citrix Gateway integrated with Swivel

14 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.



15 Citrix Netscaler RADIUS authentication for Receiver

For configuring Netscaler and Receiver to work with multiple authentication servers see Citrix Netscaler configuration for Receiver

16 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

17 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

18 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)

19 IPad Citrix Receiver

1. REDIRECT Citrix_Receiver

20 IPhone

21 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.

22 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 eaxample: 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

23 Versions

version 1.6 released 10 December 2013

- Navigate back and forward through security strings
- URL provisioning

23.1 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

24 Swivel Configuration

24.1 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.

24.2 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.

24.3 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.

24.3.1 Mobile Client Policies

For the Server based policies see Mobile Client Policies

25 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.

25.1 Download compatible with Swivel 3.8 to 3.9

25.2 Configuring the app

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

25.2.1 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.

25.3 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.

25.4 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**

25.5 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 ths 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.

25.6 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

25.7 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.

26 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 eaxample: 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

26.1 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.

27 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	Deutche Telekom	Y

The iPhone applet will also work on the iPad

28 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

29 Legacy

Download compatible with Swivel 3.7 and earlier

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

30 IPhone 2.0

31 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.

32 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 eaxample: 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

33 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,

33.1 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

34 Swivel Configuration

34.1 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.

34.2 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.

34.3 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.

34.3.1 Mobile Client Policies

For the Server based policies see Mobile Client Policies 2.0 for previous versions see Mobile Client Policies

35 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.

36 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.

36.1 Download compatible with Swivel 3.10 onwards

36.2 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.

36.2.1 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.

36.3 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.

36.4 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**

36.5 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.

36.6 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).

36.7 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.

36.8 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.

37 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

37.1 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.

38 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.

39 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

40 Mobile Phone Client

41 Mobile Phone Client 2.x

41.1 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.

41.2 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.

42 Mobile Phone Client 1.0

42.1 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.

42.2 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.