Android V5.0

Contents

The Swivel Android 5.0 App Overview

Swivel Secure offers an updated Android client for use with the Swivel platform. This article explains how to download, configure and use this client.

Requirements

Swivel 3.10 or higher. For OATH authentication v4 is required

Android OS Device 4.0 or higher

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

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

Which version do I need?

- "Swivel Mobile" Client version 4.0.
- Swivel Core version 3.10 or later.
- Android OS 4.0 or later.

TLS Protocols

- Android OS 5 or later supports TLS 1.0, 1.1 and 1.2.
- Android OS 4 supports TLS 1.0 only.

Swivel Configuration

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 How To Provision Mobile Client.

Mobile Client Policies

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

Phone Installation and Configuration

The Swivel Android Client 4.0.0 is available from the Android Play Store. You can click on the link below to open the App within Play Store.

Download compatible with Swivel 3.10 onwards

You can download the AuthControlMobile application from here

Downloading the App via SMC

When you receive a provision URL (complete url) you can open the URL on your device.

You will see a button Get The App, press on the button and the Play store will be launched allowing you to download the application.

Getting Started

When you first open the Application you will be taken to a "Not Provisioned" screen with two buttons "QR Code" and "Manual Configuration".

The application straight away gives options to the user of how to provision. Manually or via QR Code.

QR Code will launch an application (Your Android 6 device may ask you to grant permissions for the Swivel application to use the Camera).

If the user clicks on the Manual Configuration they are taken to the Manual Configuration Screen

Manual configuration is just compatible with Security Strings. For Local mode or One Touch you have to provision the device via QR Code or a Quick Provision URL.

To open the side menu the user can swipe from the left to the right(or click on the menu button at the top left corner of the screen). At the side menu you can see different options, if you click on the Info button, information will guide you through the mobile client provisioning options.

Server Settings

The settings can be manually entered with information from the Swivel System administrator.

The settings are

Server: The URL from where the client can download security codes(or keys)

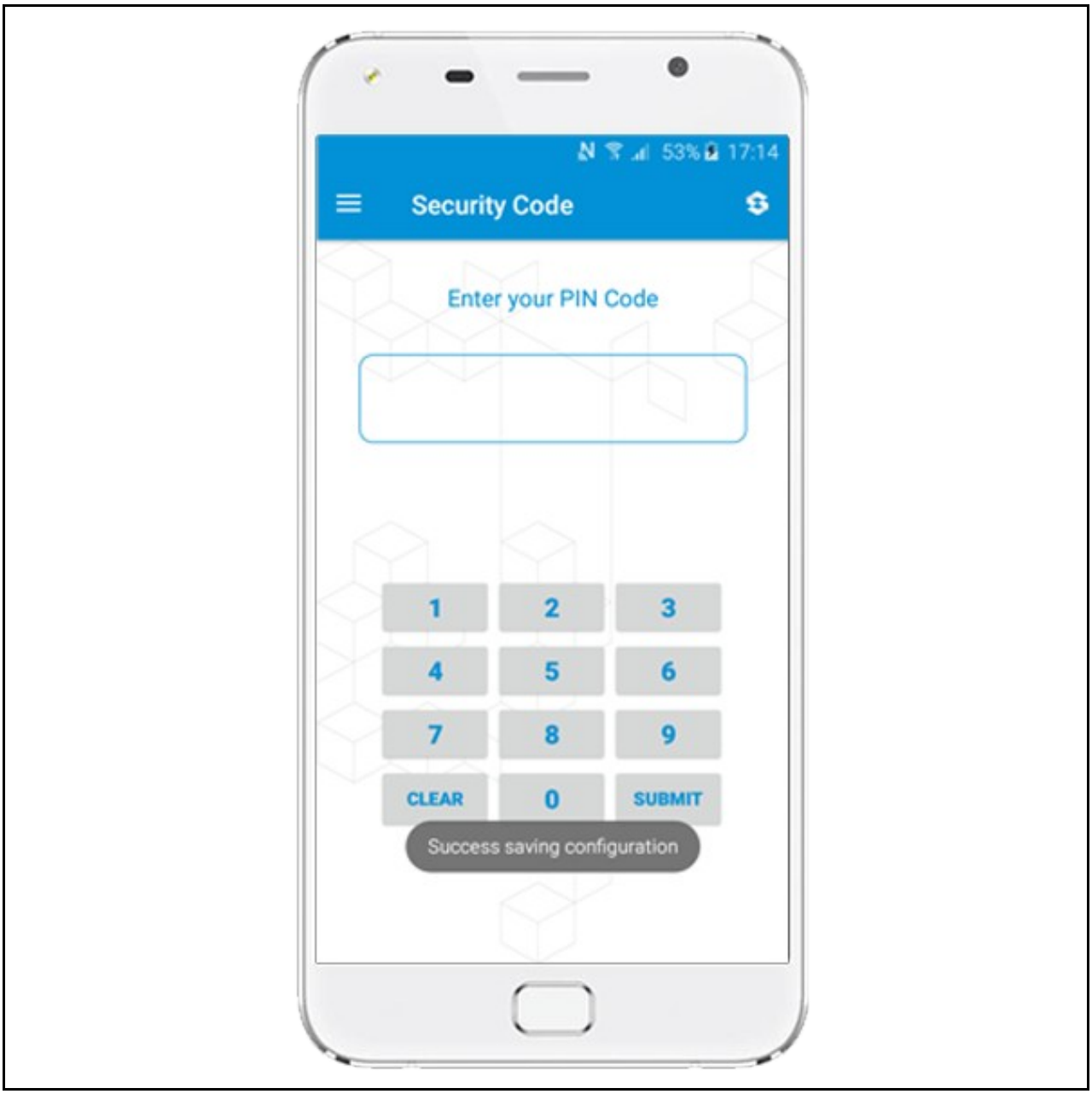
Context: The application used by the web service. For a virtual or hardware appliance this is proxy, for a software install this is usually pinsafe

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

SSL: To use HTTPS or HTTP connection

You can click the Submit button, and the application will try and access the given settings.

If the settings are correct, the Server panel will be greyed out, and you will see a successful message as on the picture below.



If you don't want to enter the setting manually, you are able to get the server settings and provision the device automatically via QR Code or Quick Provision URL

Provision the Device

Before you can use the Swivel Mobile Client you need to go through the provision process.

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 Quick Provision.

The user will be sent a Provision URL and a QR code.

There are three ways to be authorized:

1) You can provision the device via URL. Please read more on Provision URL page.

2) You can provision the device via QR code. Please read more on QR Code page.

3) Alternatively you can provision manually by entering your provision code and username into Manual Configuration page.

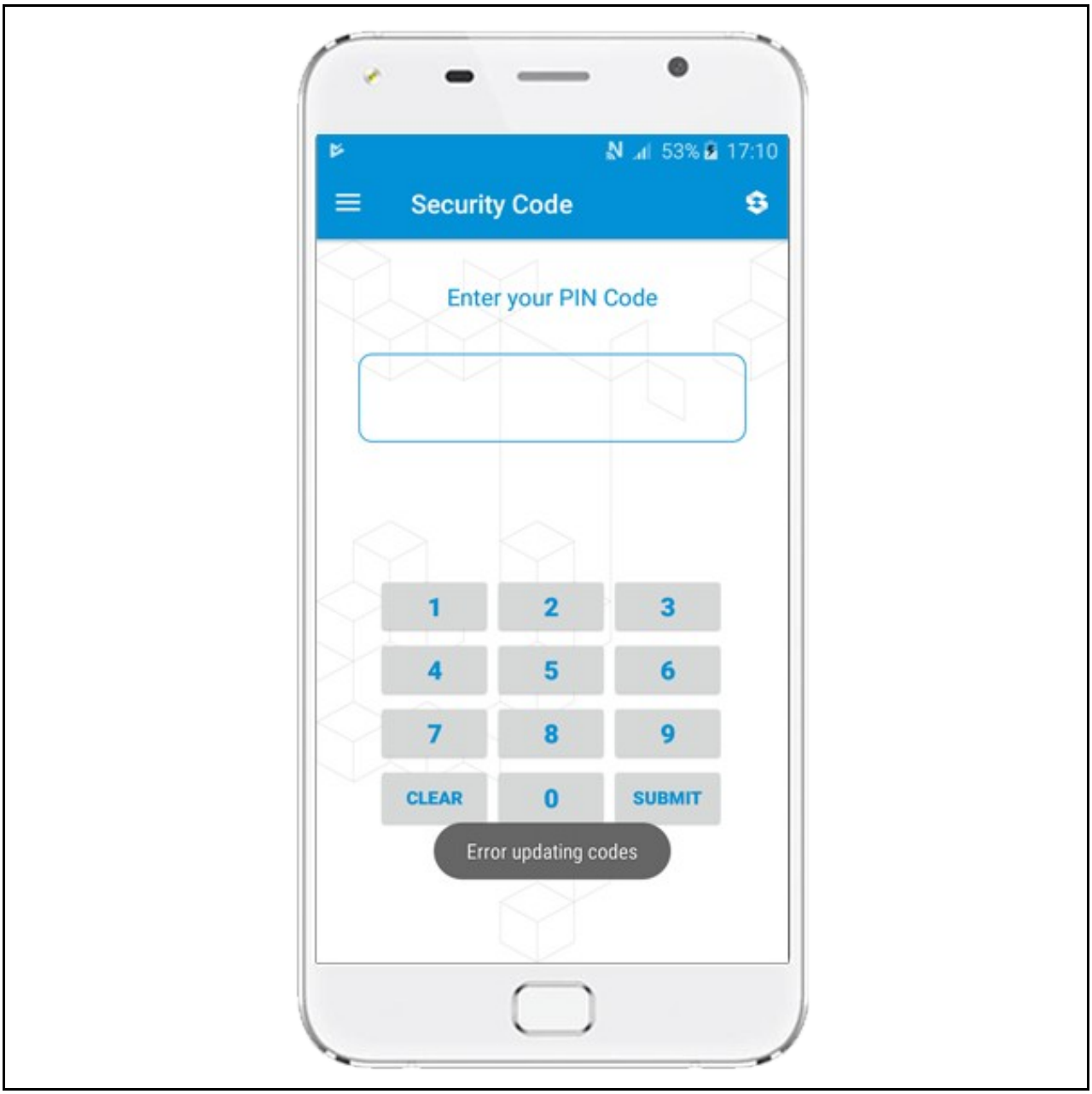
Please remember that you can only provision one device, and only once with the same URL, QR Code or Provision Code (For the manual provision) although if you are using OATH or Local mode, then you can provision more than one device with the same Quick Provision URL or a QR Code.

Update Security Codes

At the bottom of the side menu, you will find an Update Codes button, pressing this will get you a new set of 99 security codes. This will attempt to retrieve Security codes from the Swivel server.

If the update was successful you will see a message "Codes Updated Successfully" and if PIN Policy is Set To Yes a PIN Pad will be shown

If there are any problems an error message will be displayed



For more information on troubleshooting and error messages click here.

You can confirm that keys have been downloaded by checking the server logs The Swivel server will display the following log message Security codes fetched for user: username

Downloading keys requires network connectivity so it is recommended that you download a new set of keys before the Android device is likely to be without network connectivity for any length of time.

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 codes on the mobile app (to be able to see previous codes).

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

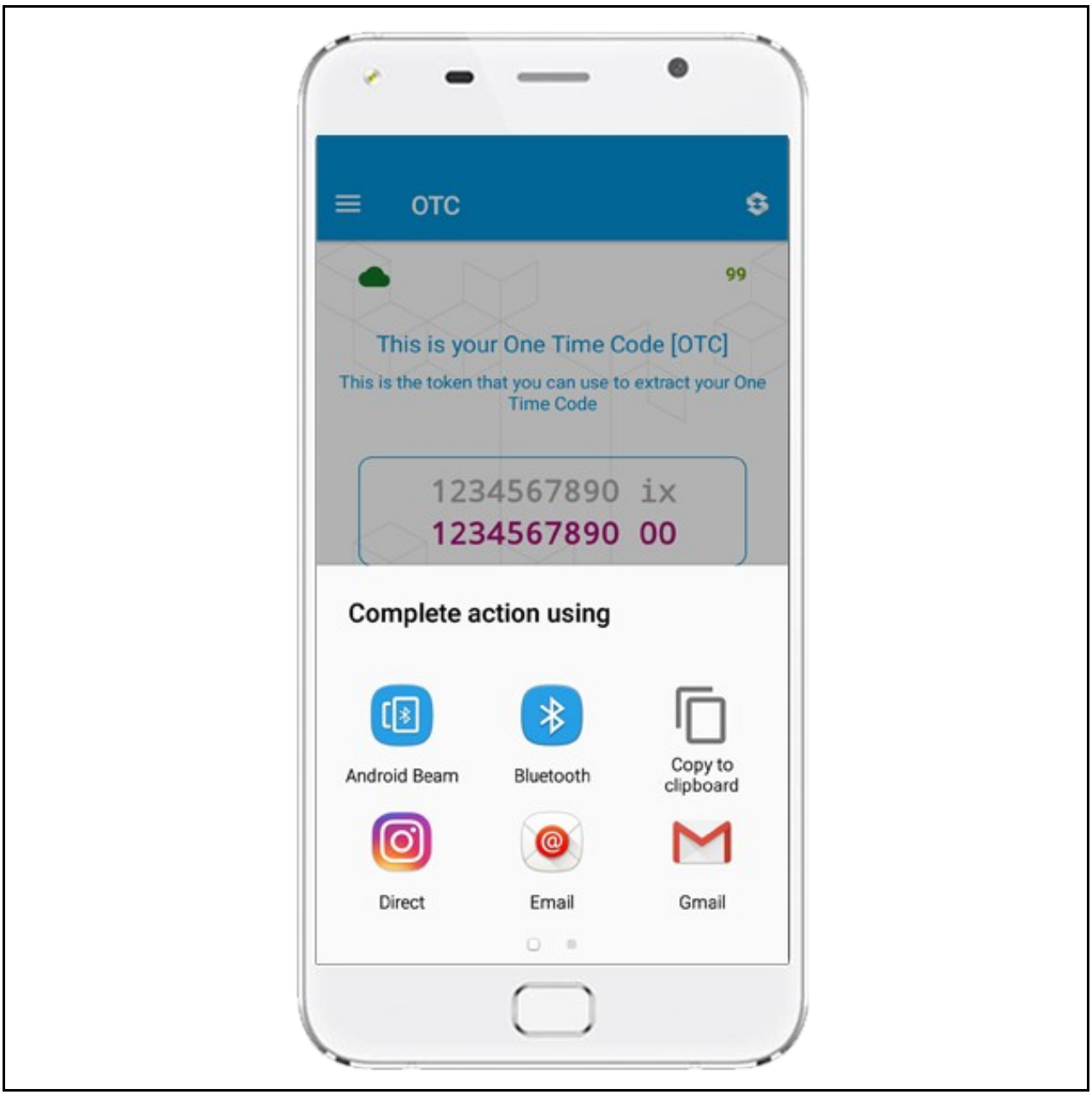
Set Support Email Address. Set Support Phone Number.

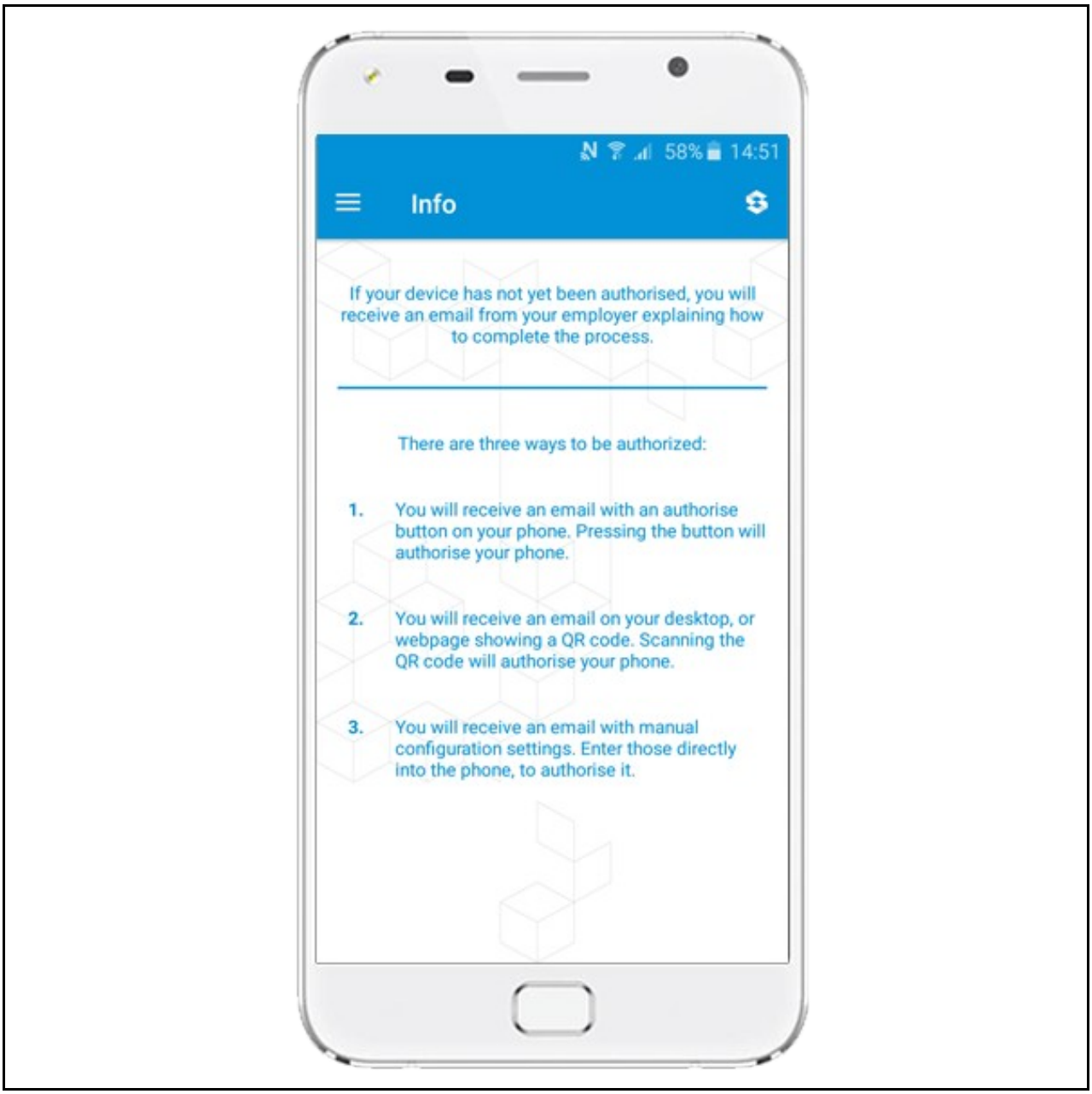
Other Options

If on the Core Policy there is a support e-mail and phone number, the user will be able to use them options on their Swivel Mobile Client.

The user will be able to open the side menu, and click on "Direct Call" or "Email" which will allow them to call the provided phone number or e-mail to the provided e-mail address

Additionally if the user finds any step of the provision unclear, they can click on the Info page which explains in more details three options to provision the device





If you have Sync-Index Policy on, or you have a green or red sync index icon at the top left of the application, please read more about Sync here

Authenticating with an app (PIN Policy On)

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

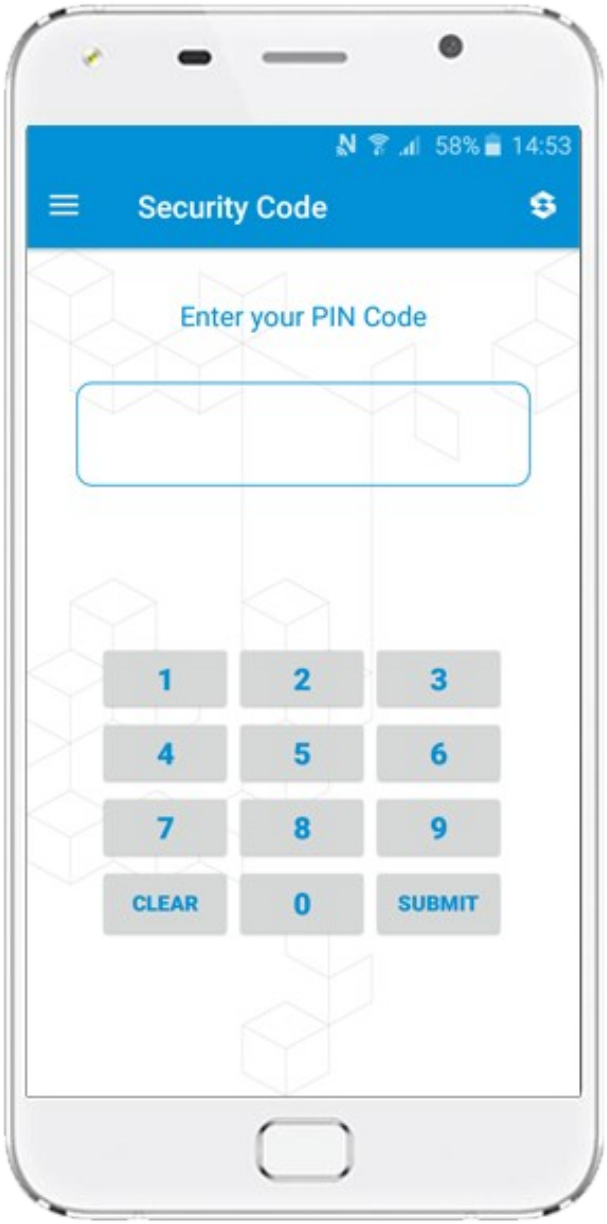
Open the app. on your Android device (if application is already opened, navigate to Security Code from the side menu).

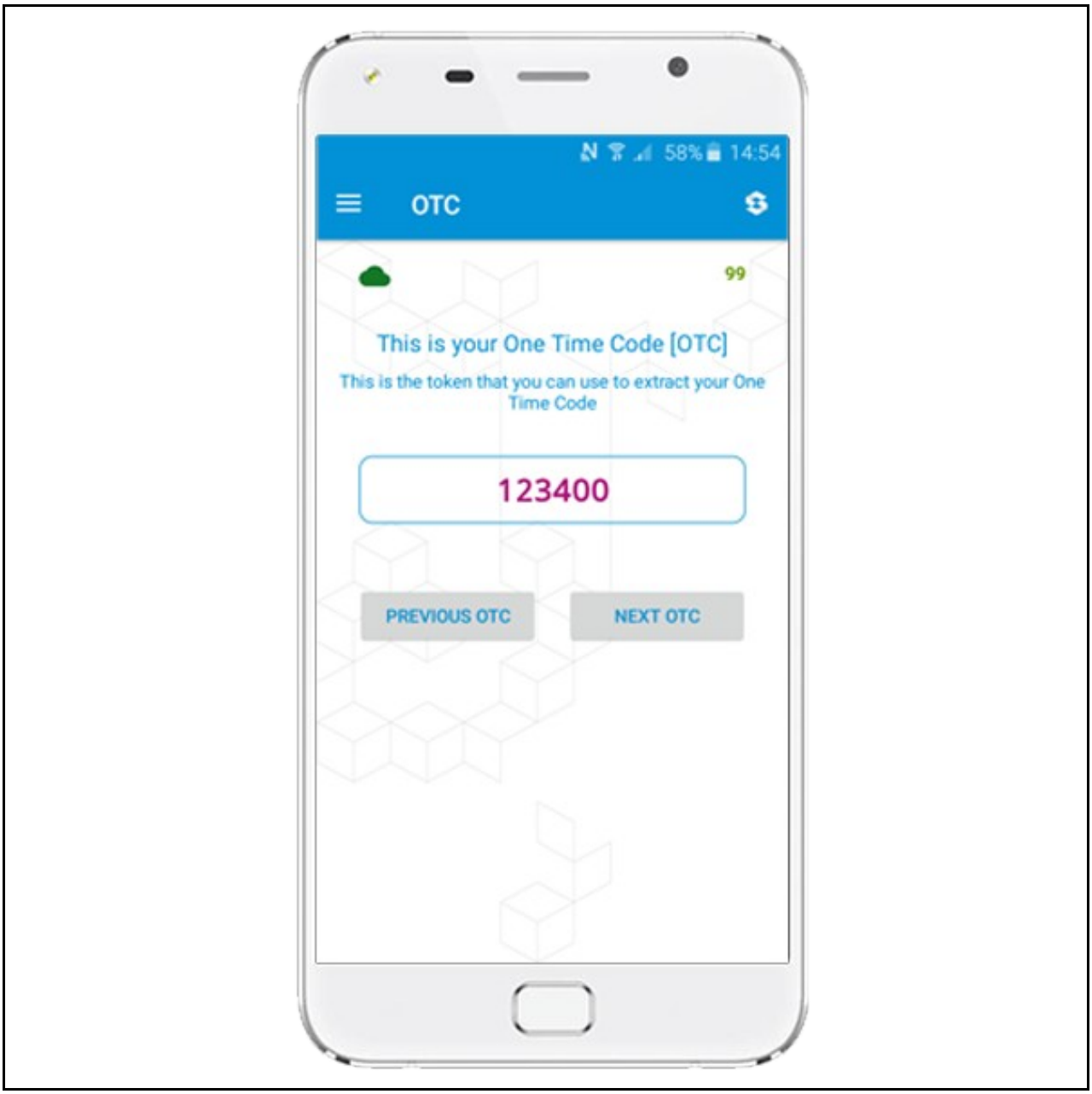
Depending on your policy settings you will either be prompted for a PIN or immediately shown a One-Time-Code (OTC).

If you are asked for a PIN, enter the PIN number previously sent during the enrolment phase and click Submit (if you have made a mistake in the PIN, you can click Clear to clear the Pin Field).

Enter the OTC into the authentication dialogue, make sure you enter all the characters.

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


58% 14:53
Security Code
Enter your PIN Code
1
2
3
4
5
6
7
8
9
CLEAR
0
SUBMIT



Authenticating with an app (PIN Policy Off)

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

Open the app on your Android Device (if application is already opened, navigate to Security Code from the side menu).

The client will show a security string with a row of placeholders 1234567890 below it.

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.

In the example screen shoot the OTC would be: 8362.

After the OTC has been worked out, you will also need to ensure you type in the last two characters shown (the index).

Using the example screen shot you would type 836200.

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

Authenticating with an app (Mobile OATH Mode)

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

Open the app on your Android Device (if application is already opened, navigate to Security Code from the side menu).

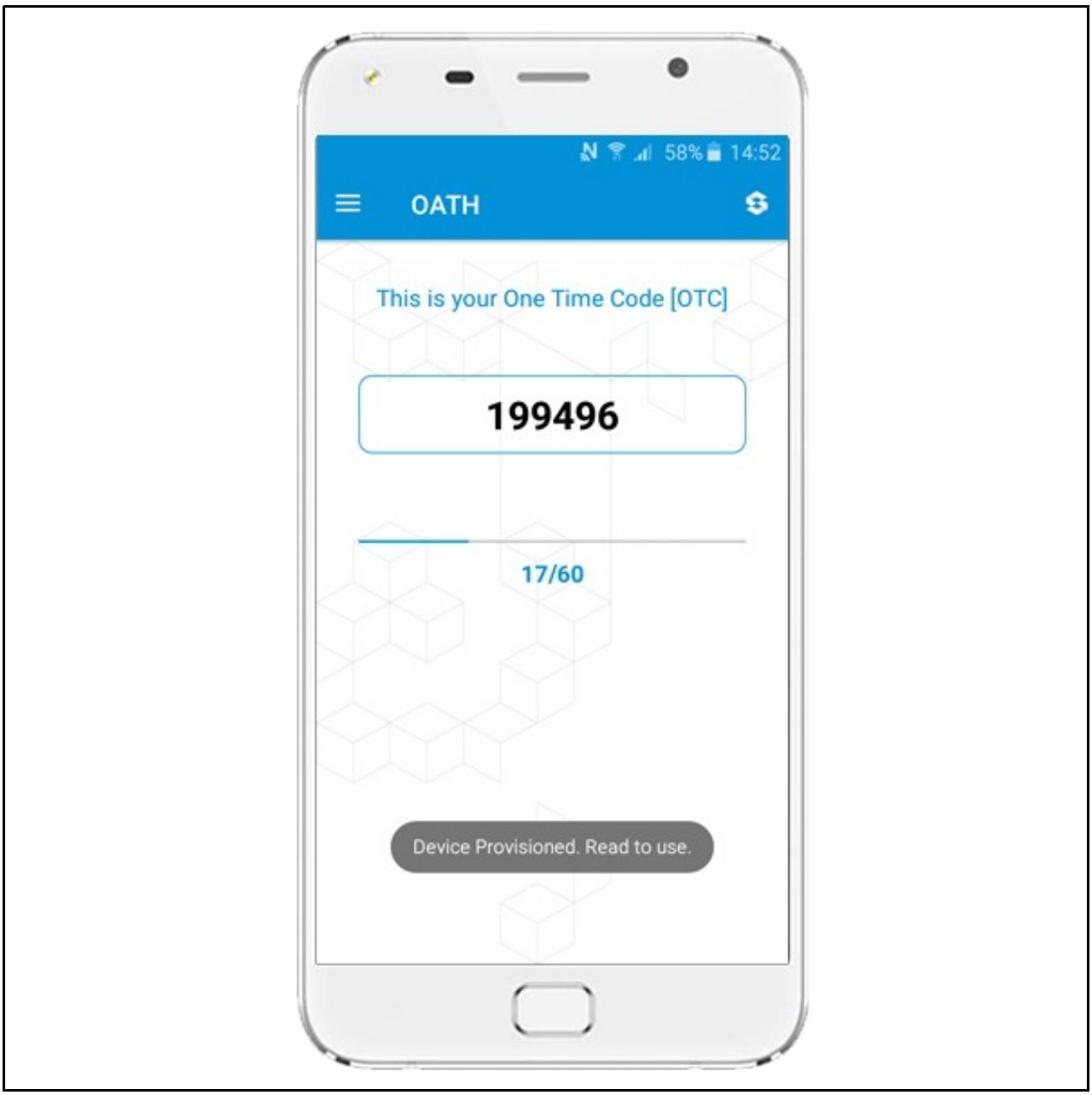
The client will show a security string with a timer below it

With the Mobile OATH mode enabled you don't have to use your PIN

Using the example screen shot you would type 800315 to authenticate.

If you need to authenticate again you can enter the code again or wait until the new code is created after timer resets to 60.

Please see How To Configure OATH Mobile to know how to configure Swivel Core to allow to provision the device in OATH mode.



Troubleshooting

- If the link on the provisining email is pointing to the old Swivel Mobile application (orangle logo), change the templates to point to the new AuthControlMobile application (purple logo)
- 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 mobile device access the internet
- If a RADIUS connection is seen from the access device to the Swivel server but authentication fails, try using PAP
- Update security codes 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.

Error Messages

Error Server Connection
The mobile client can't reach the Swivel core when downloading security codes or provisioning. Check that the mobile device is connected to the internet and that the core can be reached via mobile devices browser. If you are positive that the mobile device can connect to the Swivel core your Android devices may fail the connection because of the weak cipher. To remove all of the weak ciphers, including the Diffie-Hellman keys please download the Tomcat Ciphers patch here and follow the instructions here on how to apply the path. **Patch can only be applied on 2.0.x and 2.1 appliance!**

Incorrect settings - please check your settings
The settings for downloading the security codes 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.

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.

Cannot Open Page
This error can appear when you try to use a quick provision URL. This error usually means that you don't have a valid Swivel Mobile client installed on your device

Error Server, Unknown Server ID
This error can appear when you try to provision with a Quick Provision URL or QR Code. This error usually means that when the Swivel Mobile client tries to download Server Settings from the SSD server, it cannot find the Server ID (Site ID). Please check that you have a valid Site ID set on your Swivel core.