How To Provision Mobile Apps

Contents

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.

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.

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
```

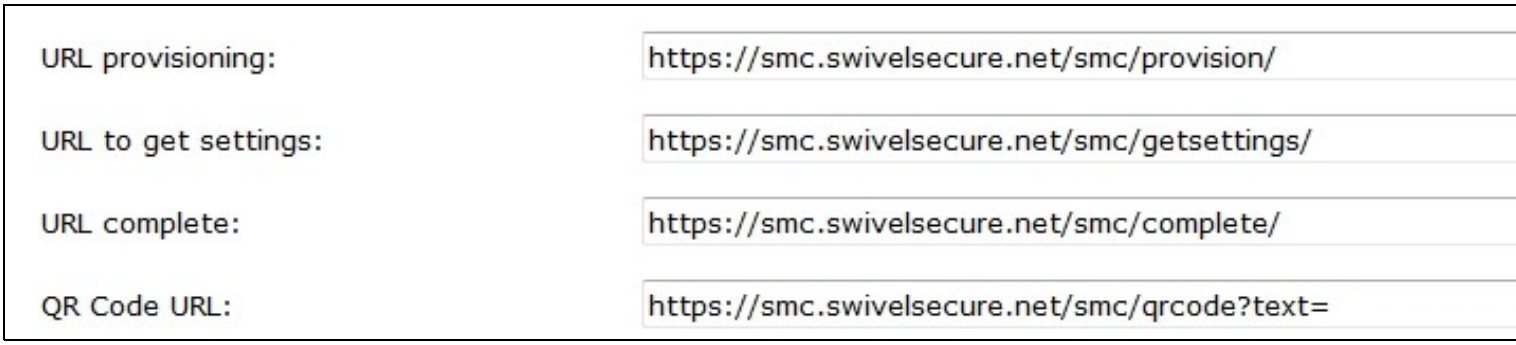
You may also optionally state two other settings to define whether you wish the clients to work in Local Mode and if you want to use One Touch

```
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.

Provision URLs

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



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.

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.

Note for 30-second timestep

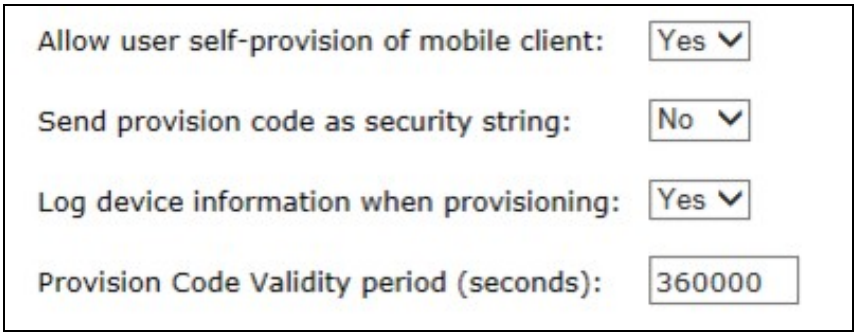
If you select 30-second timestep mode, you must change the placeholder to url5. The default provision template contains url4, so make sure you look for that and change it. You should also remove the provision link, as it is not compatible with 30-second timestep mode.

Policies

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

Provision Policies

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



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.

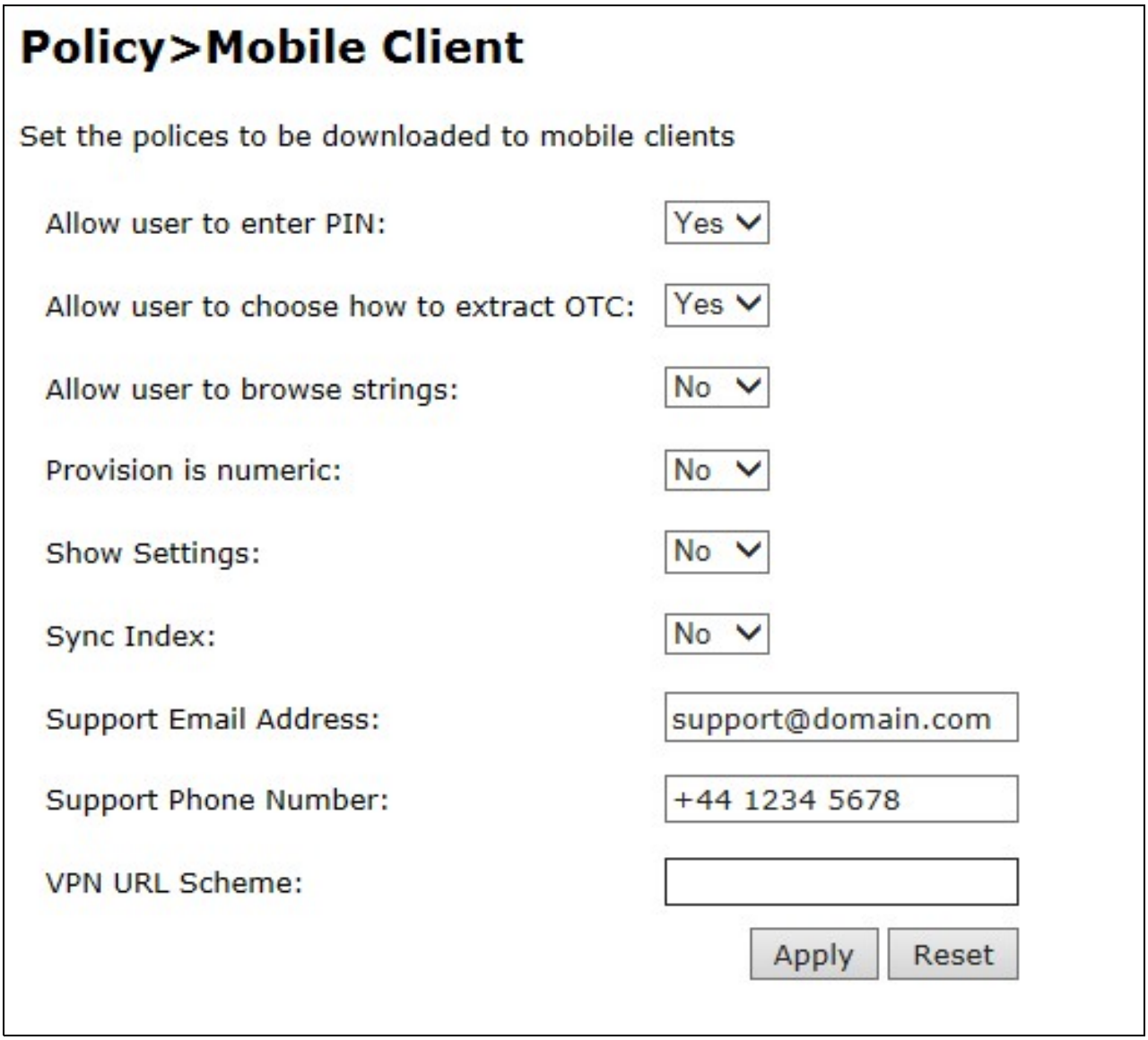
Send provision code as security string
: If this is set to No, then the provision message will be sent to the same destination as all other alert messages, usually an email address. If this is set to yes then the provision message will be sent to the same destination as their security strings, usually 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)
: For how long the provision code is valid

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



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

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 provison code also received the provision request from the mobile or that Session Synchronisation has been enabled/