

How To Configure OATH Mobile

Contents

- 1 Overview
- 2 Prerequisites
- 3 Swivel core configuration
- 4 Configuring OATH policy settings
 - ◆ 4.1 Notes for 30 Second Mode
- 5 Define a group of Mobile OATH users
- 6 Testing
- 7 Troubleshooting

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.

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.

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.

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: ▾

Send provision code as security string: ▾

Use long provision code: ▾

Use 30 second timestep for OATH: ▾

Issuer for OATH token label:

Enforce HTTP Header Checking: ▾

Mobile App Local Mode: ▾

Mobile App OATH Mode: ▾

Base64 Encode Username in provision URL: ▾

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.

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.

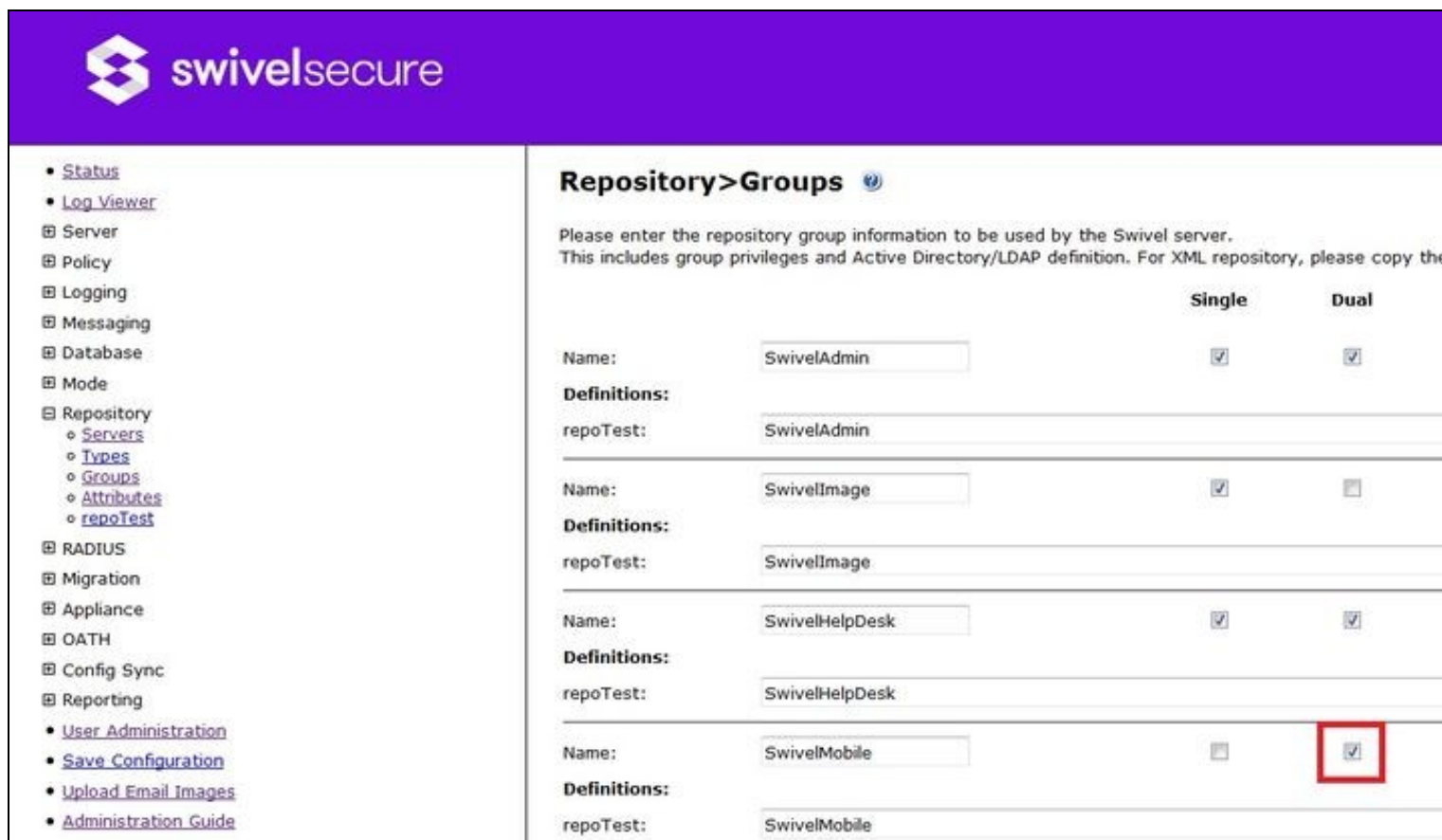
As 30-second timestep does not send any information back to Sentry, it is not compatible with Push authentication.

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.

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



The screenshot shows the Swivel Administration console interface. On the left is a navigation menu with categories like Status, Log Viewer, Server, Policy, Logging, Messaging, Database, Mode, Repository, RADIUS, Migration, Appliance, OATH, Config Sync, Reporting, and Administration. The main content area is titled 'Repository > Groups' and contains a table of repository groups. Each group has a 'Name' field, 'Definitions', and 'repoTest' field. There are checkboxes for 'Single' and 'Dual' authentication. The 'Dual' checkbox for the 'SwivelMobile' group is highlighted with a red box.

	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		

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.](#)

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.