Token

Contents

Overview

Swivel supports the use of hardware tokens for authentication and can be used as **"something you have"** in Two Factor Authentication. The Swivel OATH HOTP Hardware Token and Swivel OATH TOTP Hardware Token provide a value that is a One Time Code (OTC) which can be used to authenticate a user, other compatible tokens may also be used. For other forms of authentication see Transports How To Guide.

- Each user can be assigned a single token.
- Each token can be assigned to a single user.
- A Swivel installation can use HOTP, TOTP and OCRA tokens
- The token can be a software token or a hardware token as in the picture below

Prerequisites

Swivel 3.9.6 onwards

OATH HOTP compatible Token such as the Swivel OATH HOTP Hardware Token, Yubikey

Swivel 3.10.1 onwards

OATH TOTP compatible Token such as the Swivel OATH TOTP Hardware Token

Swivel 3.10.2 onwards

OATH OCRA compatible Token such as the Swivel OATH OCRA Hardware Token

Configuring tokens

Each token has a serial number and an associated seed. The Serial number and seed are entered into the Swivel database and then associated with a single user. Hardware tokens usually have a serial number on the back of the token. The seed is usually sent separately from the token.

Tokens and PIN numbers

If the feature to allow a PIN to be is used with the Token is enabled, the OTC is entered first from the hardware token, then the PIN number.

<OTC><PIN>

For example for a token OTC of 111111 and a PIN of 0000, then enter 1111110000.

It is also possible to use a Token with an additional One Time Code (PINless), if the PINless code is more than six digits to differentiate it from the Token code.

OATH Menu

A new menu entry can be found on the left hand side of the Swivel Administration Console. This is where the tokens are added and then assigned to users.

Adding tokens

On the Swivel Administration Console select OATH then OATH Tokens, enter the serial number and seed. Large numbers of tokens can be imported through a CSV (Comma Separated Values) file. The format for the CSV file is:

```
Serial,Seed
Serial,Seed
Serial,Seed
```

One per line, entries after the first two per line are ignored.

The seed format Swivel is expecting is in HEX, 40 Characters long is the standard. The OATH standard generates a numeric One Time Code.

Hardware Tokens

Compatible tokens can be used with Swivel, for details on the Swivel token see Swivel OATH HOTP Hardware Token. Hardware tokens are supplied with a unique seed and serial number that is valid only for the specified hardware token.

Software Tokens

Software tokens may be used with an appropriate seed, and may be used with an appropriate software token such as Google Authenticator.

Configuring users with tokens

Hardware and Software tokens can be used with Swivel using a compatible seed.

On the Swivel Administration Console select OATH then OATH Users, for the required user click on Assign token, then select the required token serial number. The user must be a member of a Swivel Group that contains the permission to allow tokens.

OATH configuration

The following options may be configured for OATH.

Token Type: HOTP

OTP Length:, default 6, the Swivel OATH HOTP Hardware Token is a six digit token.

Error Window (Events):, default 5. If the difference between the number of button presses that the server has recorded and the actual number of button presses on the token is less than the error-windows, the authentication is allowed

Sync Windows (Events):, default 10. If the difference between the number of button presses that the server has recorded and the actual number of button presses on the token is greater than the error window but less than the Sync window, the authentication will fail but the server button-press count on the server is updated. This means if the user attempts to authenticate again, the next authentication will succeed.

Append PIN (if user has one) after OTP: , default No, Options Yes/No. If set to Yes the user must enter their PIN directly after the OTC generated by the token, without any decoration (i.e. ?,?).

Administering Tokens

Tokens can be synchronized for use.

Either from the OATH Tokens or the OATH Users list click on Re-sync for the required token or user. Enter the value displayed by the token, and then enter the next value for that token (must be the next value).

User Self Help for Synchronizing Tokens

Users may synchronize tokens themselves through the User Portal.

Integrating with Tokens

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

Testing

Add a token and ensure that it can be used for authentication.

An Administrator or Helpdesk user can test a token by logging into the Swivel Administration console if they have OATH and Admin or Helpdesk permissions, and do not generate a TURing image, if a TURing image is generated, then it will expect that to be used for authentication for the length specified under Server/Jobs/Session Cleanup (default 2 minutes).

Known Issues

Swivel 3.9.6 and 3.9.7 Oath seeds are not moved when a Swivel database is migrated. Workaround: Upgrade to 3.10 or re-import seeds into new database

Swivel 3.9.6 using PIN and Token fails. Upgrade to Swivel 3.10 or later.

Troubleshooting

Check the Swivel logs.

Token is out of synchronization, re-synchronize as described above.

On the User Administration for the user click on Reset Password, and reset it, but leave the password fields blank.

Are you using PIN entry with the Token? When a PIN is used with the Token, the OTC is entered first from the hardware token, then the PIN number. For example for a token OTC of 111111 and a PIN of 0000, then enter 1111110000

Is the serial number correct for the token?, Was the seed entered automatically or manually? Try re-entering it

Error Messages

Unable to synchronize OATH Token

Note - This error appears on-screen if the OATH Token fails to synchronise. Namely, with Time based (TOTP) tokens, there may be a time drift on the Swivel Server. From the Command Line, run the command: date

Ensure that the time stamp is correct and it has not drifted over 5 minutes.

Servlet.service() for servlet SyncOathToken threw exception

Incorrect seed entered for token

Token autosynced for user gfield

This message is logged when the Sync Windows (Events) is matched and the token is resynced. The login fails but the next login will succeed.

AgentXML request failed, error: The XML request sent from the agent was malformed

This has been seen when using the User Portal with Swivel version 3.10. Upgrade the User Portal.

TOKEN_BAD_SEED

The seed used is incorrect or in the wrong format