

Integrating YubiKey HOTP With Centrify Identity Platform

Objectives

The HOTP algorithm specifies an event-based OTP algorithm, where the moving factor is an event counter. HOTP uses a counter which increases each time a code is created and, therefore, is time independent

The following is an end-to-end guide for integrating Yubikeys with the Centrify Identity Service platform using the OATH-HOTP

What would you need

- Centrify Identity Service tenant. Registration at: <https://www.centrify.com/free-trial/identity-service-form/>
- Yubico Personalization tool. This can be downloaded from: <https://www.yubico.com/support/knowledge-base/categories/articles/yubikey-personalization-tools/>
- Yubico Keys. Different keys can be compared at: <https://www.yubico.com/products/yubikey-hardware/>
- For this article, I have used a Yubico Neo key

Setting

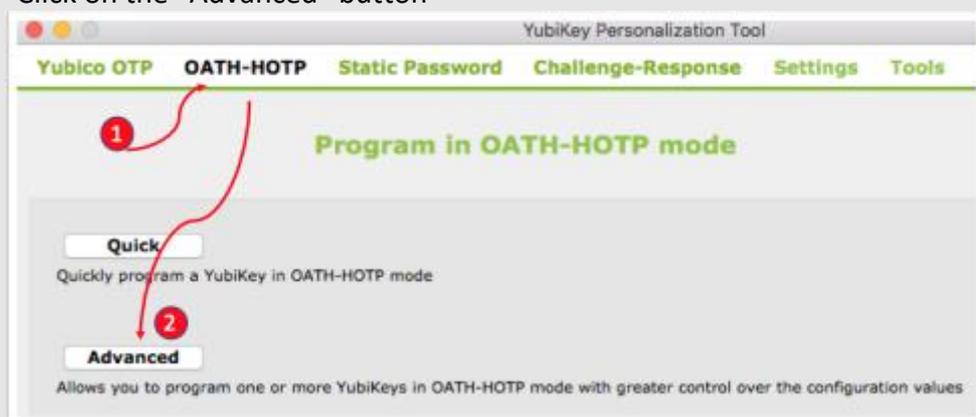
Insert your Yubikey in your USB port as it is a full-featured key with USB contact

Additional capabilities can be reviewed at [YubiKey NEO](#)

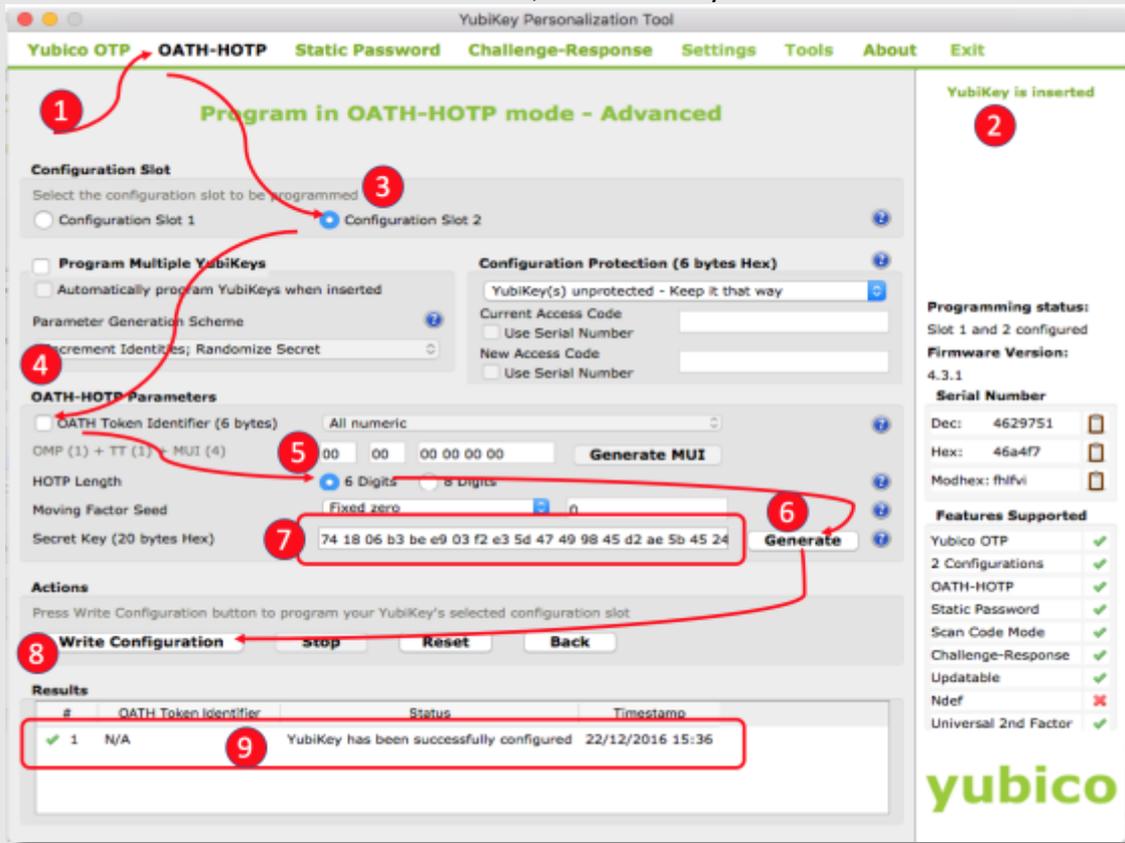


Configuring the YubiKey

1. Start the Yubikey Personalization tool
2. Select OATH-HOTP
3. Click on the "Advanced" button



- 1- Confirm you are within the OATH-HOTP configuration tab
- 2- Confirm that the Yubikey is inserted and can be read
- 3- Make sure to select "Configuration Slot 2"
- 4- Untick the "OATH Token Identifier, if it is already selected"

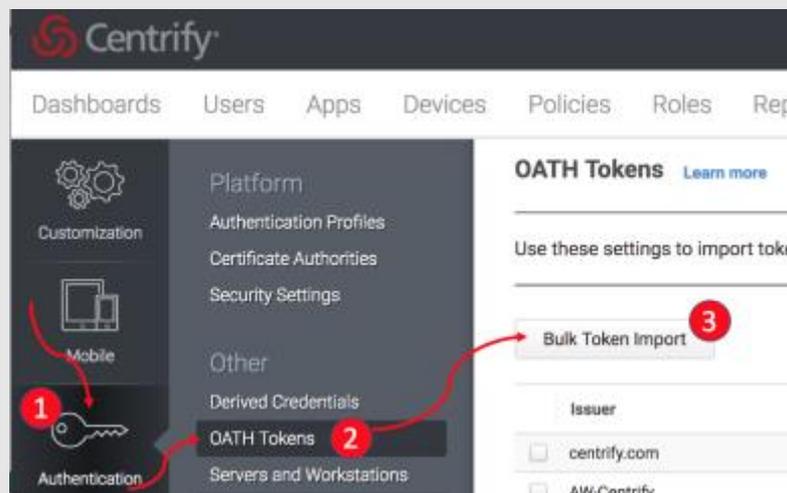


- 5- Select "6 digits" option
- 6- Generate a secret key
- 7- A key is generated. Highlight the key and Copy it as it will be used later
- 8- Finally write the above configuration to the key
- 9- Confirm config is written and no errors are displayed

Integration with Centrify Identity Cloud Platform

Log on to the Centrify Cloud Service as a Cloud Admin user and navigate to the “Settings” tab

1. Select Authentication
2. OATH Tokens
3. Click on the “Bulk Token Import” to open the CSV file for filling the Yubikey token details



Fill in and Complete the bulk import spreadsheet as per the example below. Insure to paste the previously copied HEX key in the appropriate cell.

1	User Principal Name	Secret Key (HEX)	Account Name	Issuer	Algorithm	OTP Digits	Type	Period	Counter
2	awaneis@aw-centrify.com	fd 14 42 3f ee b7 58 65 69 32 53 7b 5e 2a 27 89 61 c3 2b 0c	Ayman Waneis	AW-Centrify	Sha1	6	Hotp	30	0
3	jem@aw-centrify.com	f6 1d 9d 95 c3 ef b4 bd 7f 28 c6 d8 72 af 15 43 a5 f3 4e 7c	Jem	AW-Centrify	Sha1	6	Hotp	30	0
4									
5									
6									

Save the file, then browse to that file to upload it and click next to complete importing the keys.

You should end up with a similar configuration as below

The screenshot shows the 'OATH Tokens' settings page. A table lists the imported tokens:

Issuer	Account name	User principal name	Type	Created By
<input type="checkbox"/> centrify.com	ayman.waneis@centrify.com.1427	ayman.waneis@centrify.com.1427	Totp	User
<input type="checkbox"/> AW-Centrify	Jem	jem@aw-centrify.com	Hotp	Admin
<input type="checkbox"/> AW-Centrify	Ayman Waneis	awaneis@aw-centrify.com	Hotp	Admin
<input type="checkbox"/> centrify.com	wfapprover@aw-centrify.com	wfapprover@aw-centrify.com	Totp	User
<input type="checkbox"/> centrify.com	awaneis@ed-aw-centrify.com	awaneis@ed-aw-centrify.com	Totp	User

Additional Configuration required within the Centrify Identity platform

Create your custom “Authentication Profile” to specify the Multi-Factor Authentication profile with the options required

Ensure to select “OATH OTP Client” either on the 1st or 2nd challenge

Authentication Profile

Profile Name *
Application with 2 MFA

Authentication Mechanisms

Challenge 1	Challenge 2 (optional)
<input type="checkbox"/> Password	<input checked="" type="checkbox"/> Password
<input checked="" type="checkbox"/> Mobile Authenticator	<input type="checkbox"/> Mobile Authenticator
<input type="checkbox"/> Phone call	<input type="checkbox"/> Phone call
<input type="checkbox"/> Text message (SMS) confirmation code	<input type="checkbox"/> Text message (SMS) confirmation code
<input checked="" type="checkbox"/> Email confirmation code	<input type="checkbox"/> Email confirmation code
<input type="checkbox"/> User-defined Security Question	<input type="checkbox"/> User-defined Security Question
<input checked="" type="checkbox"/> OATH OTP Client	<input type="checkbox"/> OATH OTP Client
<input type="checkbox"/> 3rd Party RADIUS Authentication	<input type="checkbox"/> 3rd Party RADIUS Authentication

Challenge Pass-Through Duration ⓘ
30 minutes

OK Cancel

Default Policy - Active

Enable authentication policy controls (2)

Login Authentication Rules ⓘ

Condition	Authentication Profile
<input type="checkbox"/> Identity Cookie - is not present	Authentication Profile

Default Profile (used if no condition matches) ⓘ
Default Policy high login profile (auto generated)

Enable the login Authentication option

Select the desired Login Profile previously configured

Enable OATH OTP in the Policies Set

Default Policy - Active

OATH OTP

(4) Allow OATH OTP integration

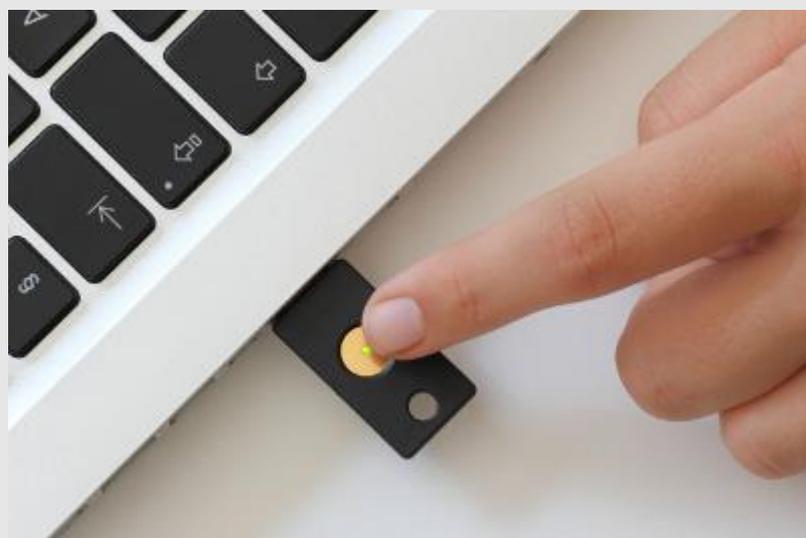
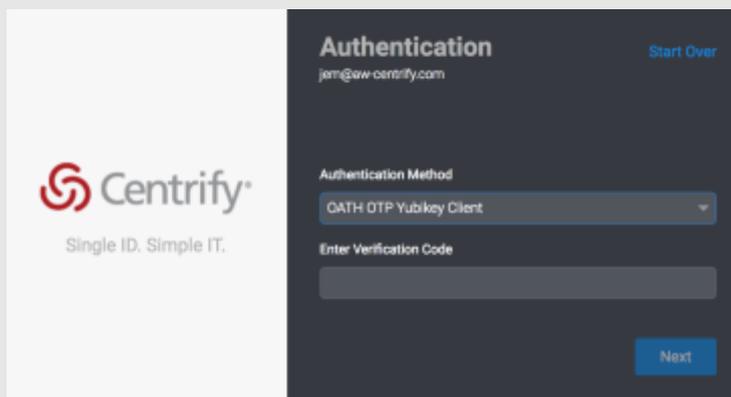
(5) Show QR code for self-service ⓘ

OATH OTP Display Name * ⓘ
 (6)

Results and Conclusion

Now that all configuration and integration is completed, users can use the Yubikey to login to the Centrify Identity Portal

Start the Centrify portal and provide your login ID and click next to move to the MFA login screen



Touch the Yubikey key for about 3 seconds to generate the counter based HOTP

You should be able to login successfully now to your Centrify Portal environment

We hope this integration guide was helpful. For all other questions on how Centrify can help you consolidate user identities and solve the #1 cause of all cyber-attacks, please contact us at <https://www.centrify.com/about-us/contact/>