OPENOTP & U2F KEYS

OpenOTP & U2F Keys

Token U2F Web-Service

Overview

OpenOTP v1.2 supports both OTP and the newer FIDO-U2F standard from the FIDO Alliance for user authentication. If you intend to use OpenOTP with FIDO U2F, please read this document which explains how to enable and use U2F with your application integrations and WebADM self-services.

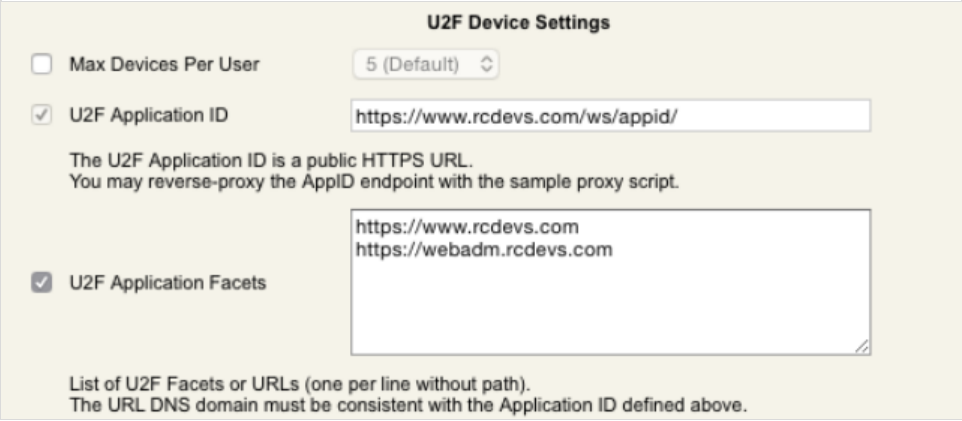
FIDO Universal 2nd Factor (U2F) is a new authentication standard created by the FIDO Alliance which simplifies and strengthens twofactor authentication for businesses and consumers. In addition to being easy to use, U2F stops phishing, one of the most common credential-stealing attacks. Read more about U2F on the FIDO Alliance website at https://fidoalliance.org.

OpenOTP 1.2 supports user authentication with OTP-only, U2F-only and combined OTP+U2F. U2F is a strong authentication method which relies on random challenges and elliptic curve signatures. Unlike OTP, it always requires a Challenge-Response operation mode. When YubiHSM devices are used with RCDevs WebADM, OpenOTP U2F challenges are generated on the HSM's hardware RNG (true random generation engine).

U2F is a complex mechanism which requires a compatible DNS host naming configuration and a public endpoint called "AppId" to be setup. This documentation is intended to clarify these specific integration requirements.

1. Enabling U2F in OpenOTP

To enable U2F, you need to edit your OpenOTP configuration under the Applications menu in WebADM and scroll down to the U2F Device Settings. You need to configure the U2F Application Id URL and the U2F Application Facets.



Once an Application ID URL is configured with at least one application facet, the OpenOTP U2F API will accept U2F requests and

your self-services will display a new menu entry with U2F device enrollment and testing. Also, the SAML and OpenID Web federation applications will automatically support U2F-based user login methods.

1.1. Application ID (AppID)

The Application ID (ie. AppID) is a communication endpoint which is required for any U2F-enable system to operate. The FIDO client implementation in the authenticating systems at the user side needs to connect the AppID during every user authentication in order to validate the current login URL authorized by the U2F service. For this reason, the AppID needs to be available from public network access and Internet. The AppID endpoint URL must have a hostname with a fully-qualified public domain name. The DNS domain MUST end with a valid top-level domain (TLD) and cannot be based on a private naming. It must be a secure URL starting with the HTTPS scheme (https://).

Important

The configured AppID public URL must not be changed after you enrolled user devices. If you need to change the AppID URL, any user registration is void has to re-register all his devices on the self-service.

1.1.1. AppID Proxy Script

By default the AppID is accessible on your OpenOTP server under `https://<webadmserver>/ openotp/appid/`. It is recommended to proxy the AppID endpoint on a public website of your company with the provided sample proxy script available in `/opt/webadm/websrvs/openotp/docs/appid_proxy.php`. You can place/copy the proxy script on your website under `/appid/index.php`. The proxy script contains a configuration line where you need to set the internal OpenOTP AppID URL.

Example

You copy the proxy script under the https://mywebsite.com/appid/ location on your website. The script is reconfigured to have server_url = http://:8080/openotp/ appid/ or server_url = https://:8443/openotp/appid/.

Note

The backend AppID connection doesn't need to be secured. Only the FIDO client communication with the public AppID URL requires SSL.

1.1.2. AppID with WAProxy

If you are using the RCDevs WAProxy reverse-proxy package to publish your WebADM applications, then your WAProxy provides an AppID proxy URL out-of the box under `https:// <waproxyserver>/ws/appid/`. Please refer to the RCDevs WAProxy documentation for more details.

1.1.3. Testing the AppID.

You can test the AppID URL is working by pointing your Web browser to the AppID location. It should display the AppID JSON document containing the list of configured U2F facets.

1.2. Application Facets

The FIDO U2F standard requires the list of URLs where the users will authenticate to be declared in a U2F Facet list. A facet is any Web URL in your organization where you deploy an OpenOTP authentication mechanism.

Example

A website where you integrated OpenOTP login must be registered.

A facet is the combination of a protocol scheme, a DNS hostname and an optional port number.

The trailing path in the URL is ignored in the FIDO specification and should not be set. Let's imagine your organization DNS domain is mycompany.com and you deployed the AppID under the URL https://www.mycompany.com/appid/. All your facets MUST be under the same fullyqualified public DNS suffix. A valid list of facets would also be:

```
- https://www.mycomany.com
- https://othersite.mycompany.com:8888
- https://local.area.mycompany.com
```

A FIDO U2F facet cannot be on another DNS suffix line `mysecondcompany.com` or `mycompany.org`.

1.2.1. Naming Considerations

By design the U2F standard has strong DNS naming constraints which oblige an organization to federate U2F over its own services only (those services located on an identical DNS domain). If you intend to integrate U2F authentication for both public and private services, it becomes even more complex as there must be a DNS name coherence with the internal (private) DNS naming.

For example you can use U2F for internal services provided that the internal DNS names are under the same suffix than the AppID.

Example: If your internal domain is local.mycompany.com, then you can add internal facets like:

```
- https://intranet.local.mycompany.com
- local.mycompany.com:8888
```

But you cannot use U2F with facets like:

```
- https://intranet.local
- https://www.mylocalnet
```

As a general rule, U2F facets MUST be under the same DNS domain suffix as the AppID URL. And this domain suffix must be under a public top-level domain (public DNS). The AppID and the application login URLs must be under HTTPS.

1.2.2. Public and Private Facets

You may decide to protect internal applications in your intranet and private networks. In this case the corresponding facets must be added to the facet list. OpenOTP automatically protects the internal (private) facets from being listed on the AppID when the origin of the user request is on a public network. This mechanism prevents the AppID from disclosing your internal domain naming.

1.2.3. Self Services and Web SSO Applications

RCDevs self-service, Web SSO applications and password reset are concerned by the U2F DNS requirements because they include U2F enrollment and login facilities. OpenOTP will automatically add a facet for these applications without needing to configure a facet manually.

Moreover, OpenOTP will mark those facets as private to prevent them from being displayed by the AppID from public networks. The automatic facets will also be present when you access the WebADM applications from the trusted network, but they won't be shown when the AppID is accessed from Internet, unless WebADM is deployed on a public server.

1.2.4. Admin Portal

Under the WebADM Admin Portal, administrators are able to register U2F devices for users and test U2F login. For this reason, the Admin Portal itself is automatically added to the private facets too.

If WebADM Admin Portal is not located on a compatible DNS naming, then the facet is not included and it is not possible to use U2F features from the Admin Portal.

2. Using U2F in OpenOTP

In OpenOTP, U2F is enabled as long as one or more facets exists in "U2F Application Facets". For a user to authenticate with U2F, you need to change his Login Mode. The following modes are supported:

- LDAPOTP: User authenticates with LDAP password and OTP password.
- LDAPU2F: User authenticates with LDAP password and U2F signature.
- LDAPMFA: User authenticates with LDAP password and either OTP or U2F signature.

Example

If the user does not have a U2F device registered, then only the OTP option works.

- LDAP: User authenticates with his LDAP password only.
- OTP User authenticates with OTP password only.

Some integrations like RADIUS VPNs do not support U2F. OpenOTP will automatically discard the U2F option when the integration

cannot deal with the U2F protocol.

3. Additional Information

More information and specifications about FIDO U2F can be found under the FIDO Alliance Website.

For any question regarding the U2F integration with OpenOTP, please contact RCDevs support.