OIDC

IT SEEMS TO BE HIP

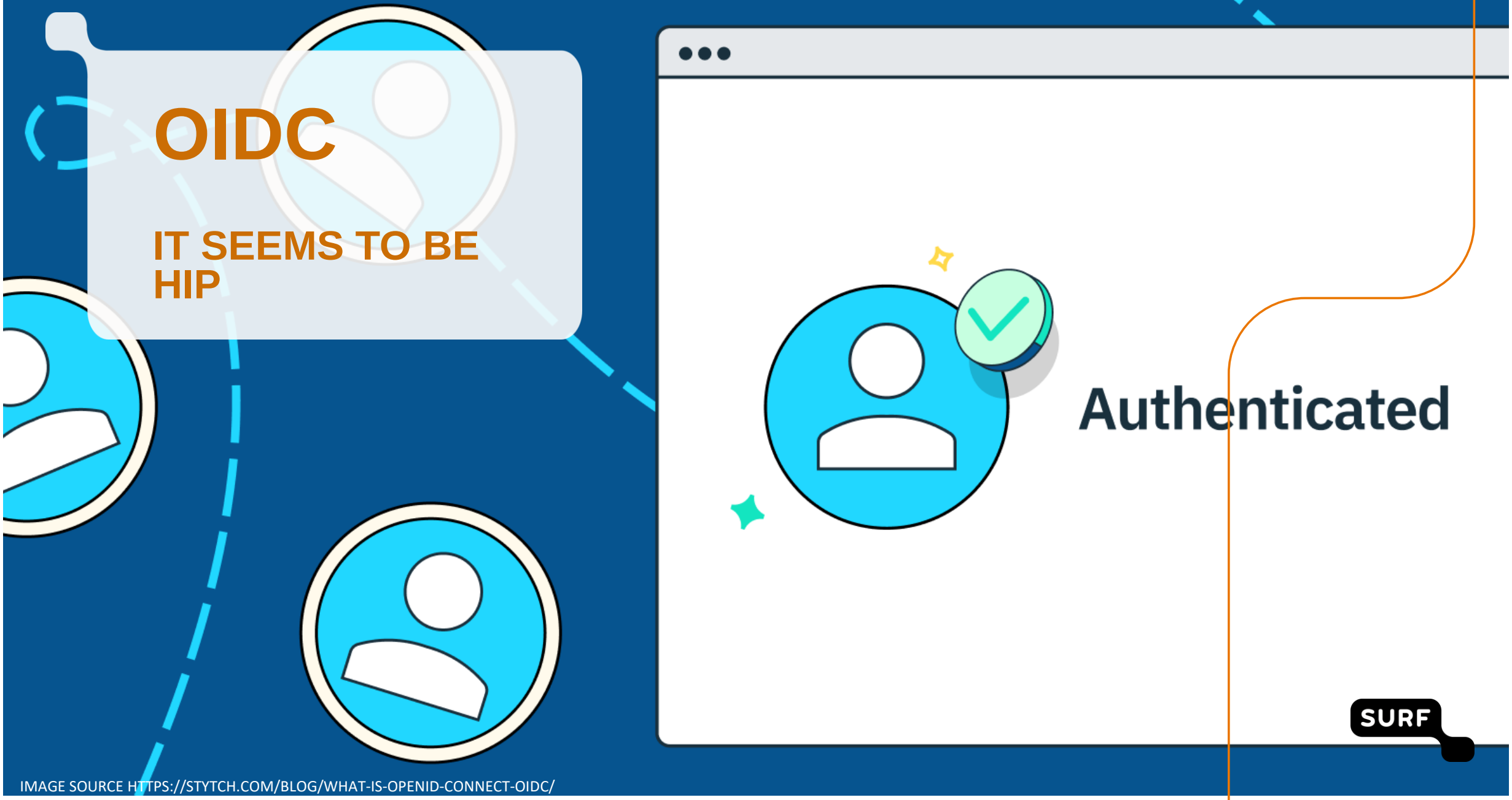
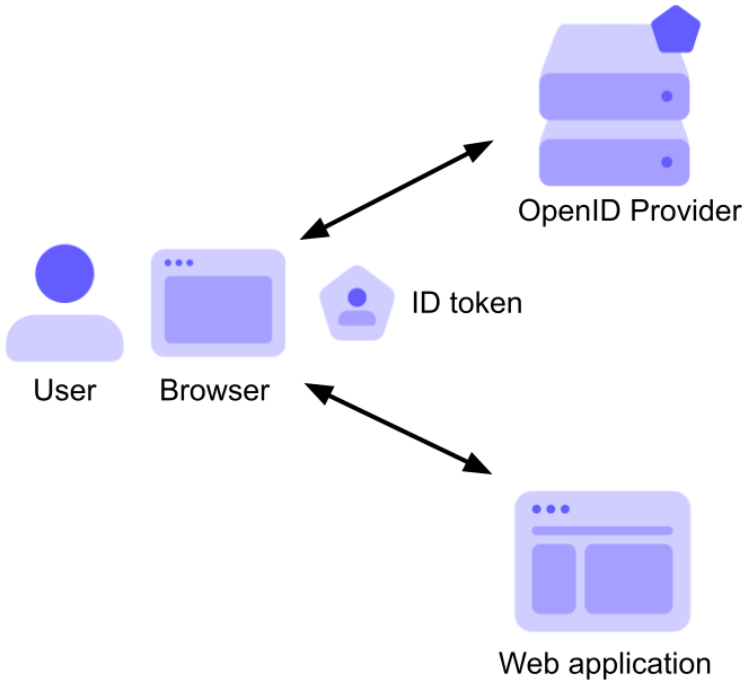


IMAGE SOURCE HTTPS://STYTCH.COM/BLOG/WHAT-IS-OPENID-CONNECT-OIDC/

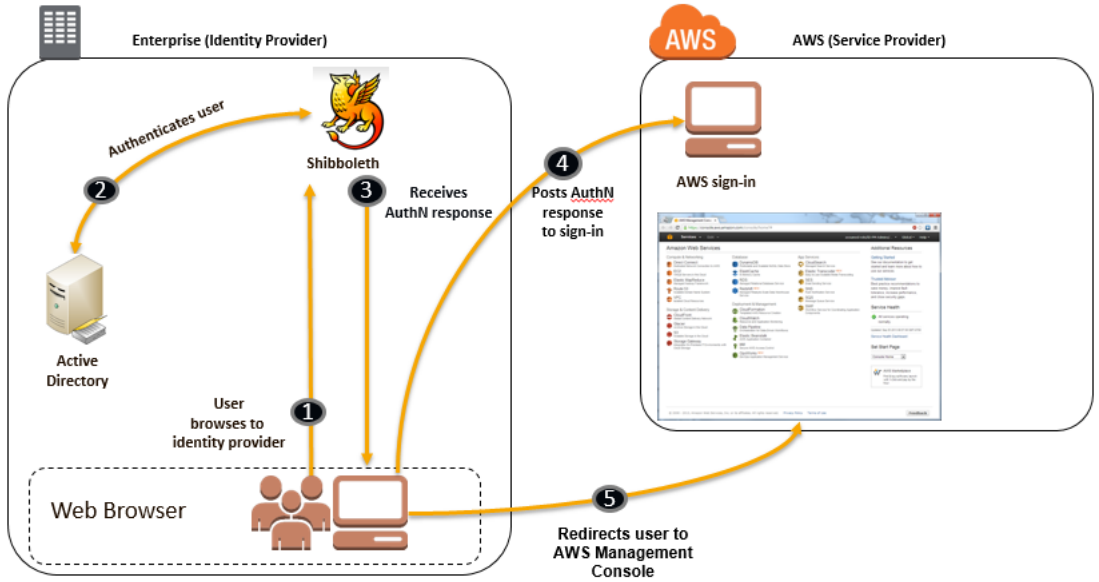
What is OIDC

- OpenID Connect (OIDC) is an open authentication protocol that works on top of the OAuth 2.0 framework.
- OAuth 2.0, which stands for “Open Authorization”, is a standard designed to allow a website or application to access resources hosted by other web apps on behalf of a user.



What do we have now?

- Shibboleth – SAML authentication protocol for ownCloud
- SimpleSAMLphp for SURFdrive management application
- oAuth2 to authenticate applications for user session



Why change, when it works ?

- Shibboleth is somewhat unstable
  - ***Healthcheck which kicks shibboleth when it crashed***

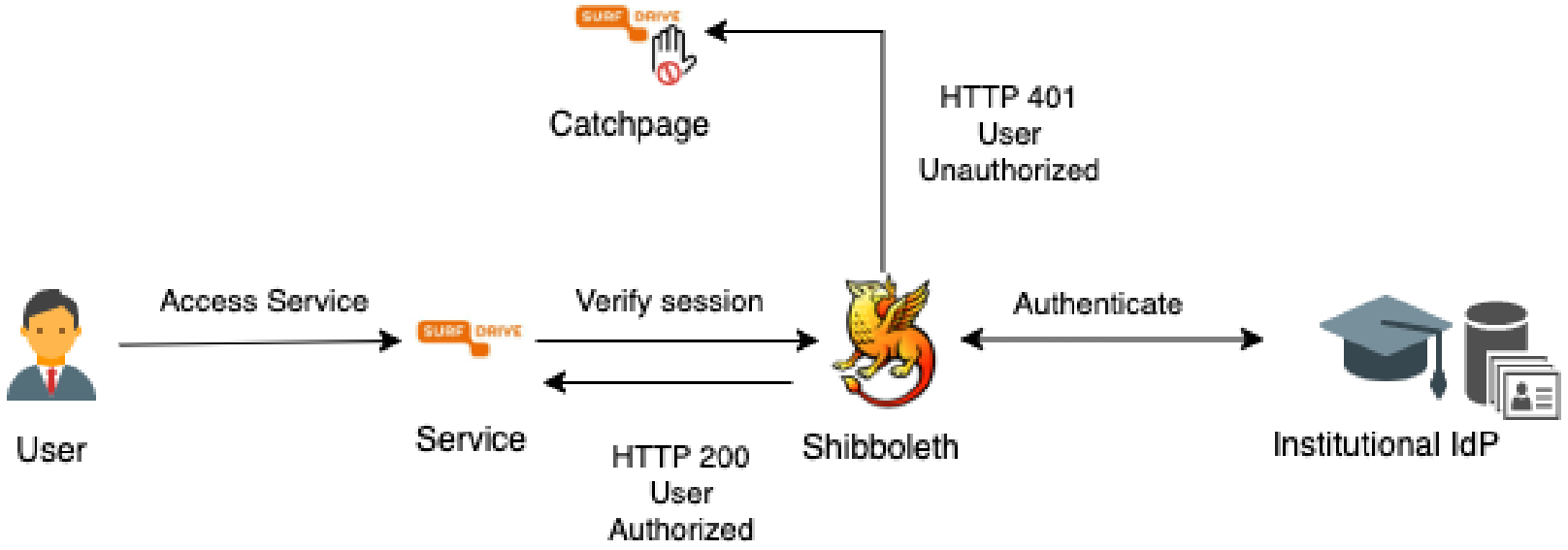
- Remove dependency on application support

- Ability to define user authentication flows

- Discouple application user from idp user
  - Quite hard when a username is changed these days.

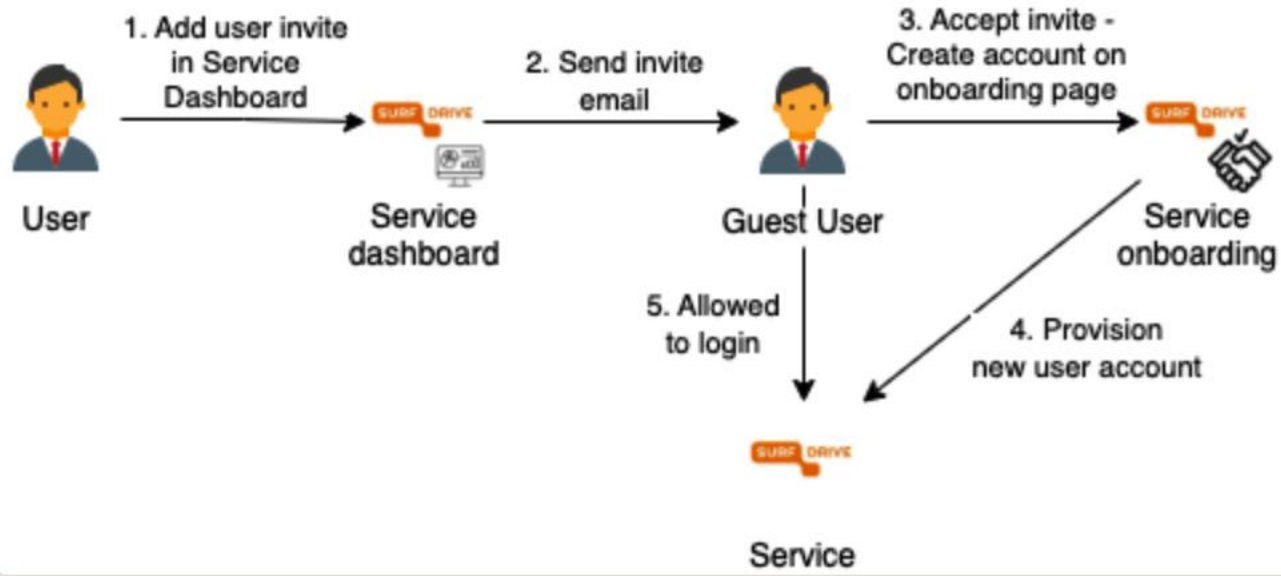
- Session token on Session token (Shibboleth token & oAuth(2) token)

Current authentication flow



Guest accounts

- Invite an user by email address
- Guest account accept invite by choosing for;
  - Account with username/password combination
  - Account via a Social Identity Provider (SURF EduID)
- Guest accounts are placed on an allow list,
  where the required SAML attribute for user accounts is not set.



What to keep in mind

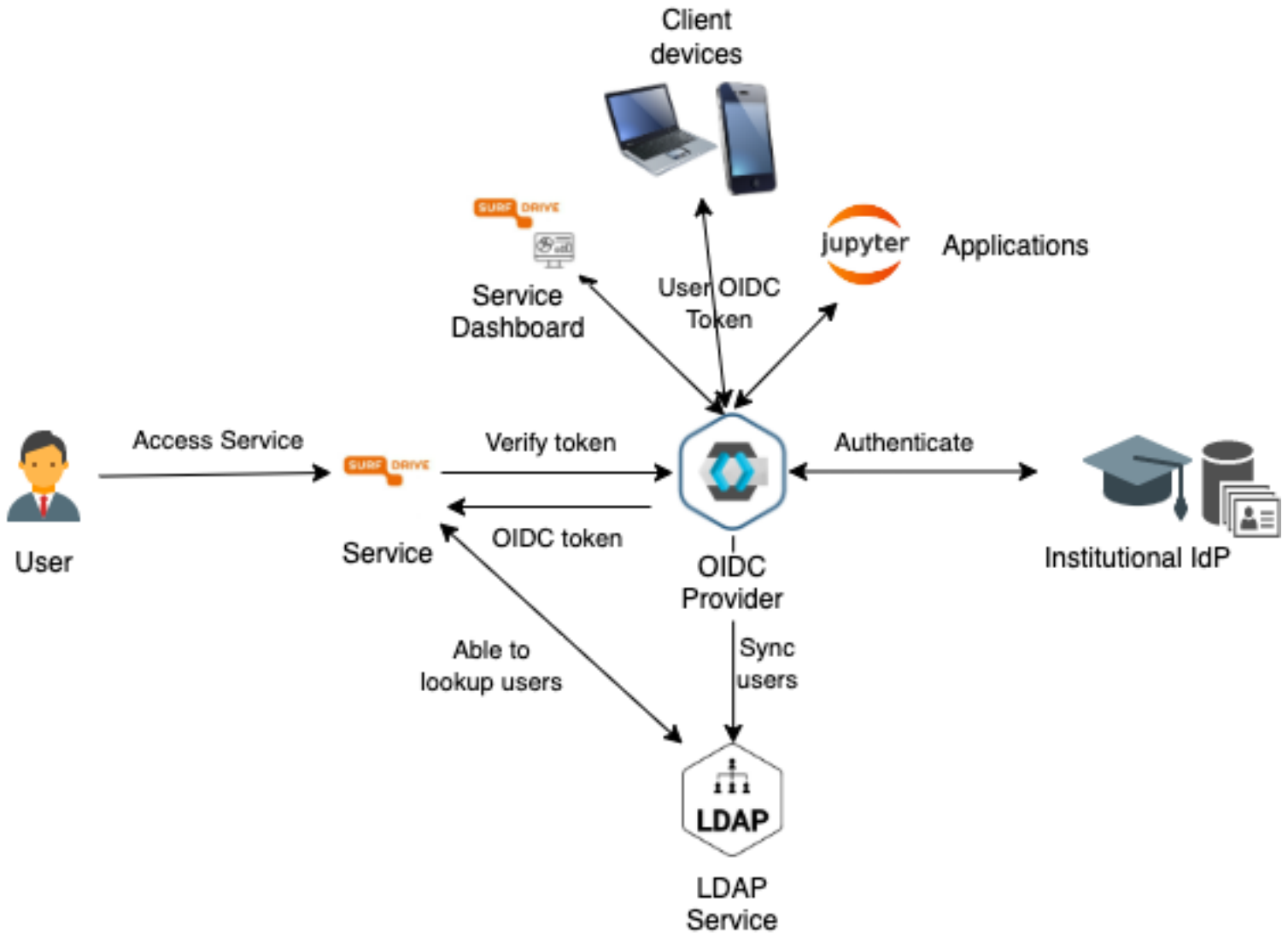
- User authentication based on SAML claim attribute
- Guest accounts via allow list
- Ability to force MFA for not institutional accounts
- Option to discouple application account from IdP user
- Support for basic auth for WebDAV purpose

What we compared

Keycloak absolute winner

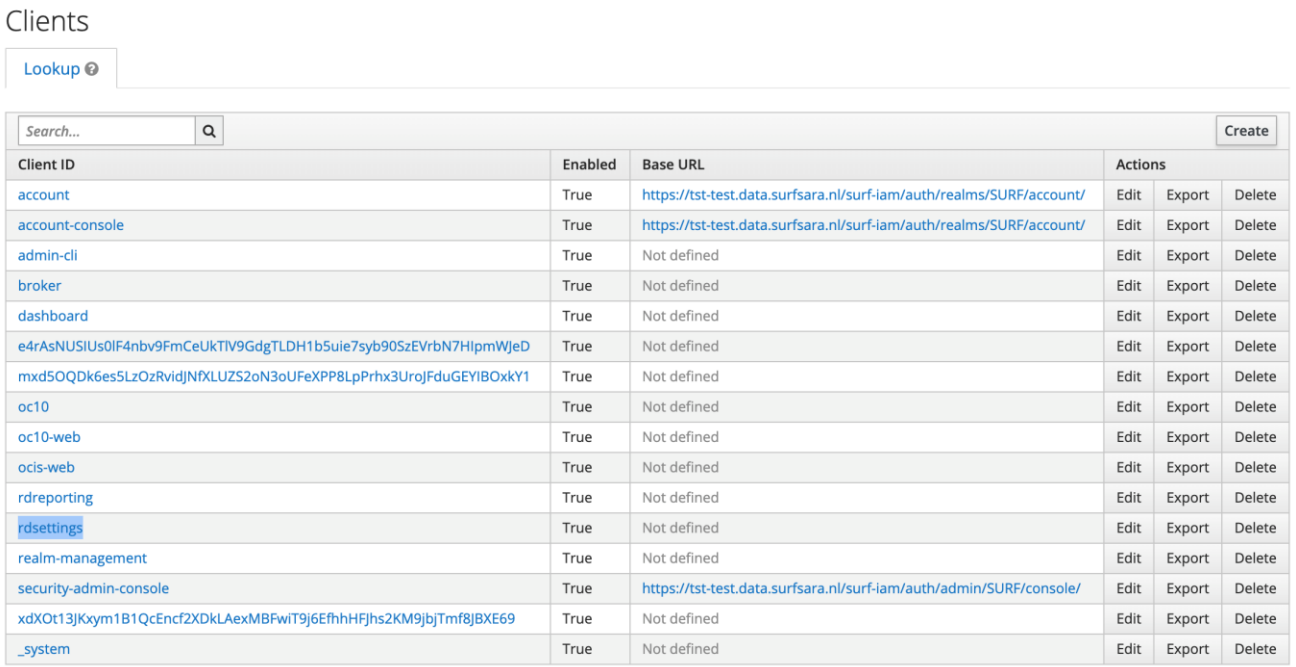
- Local user management
- Option to configure multiple MFA solutions
- Ability to connect external IdP for authentication and/or provisioning
- Ability to connect LDAP for read or read/write
- Possibility to make authentication flows
- Option to configure multiple applications for token usage
- API to do (user) management

Define the user flows



KeyCloak – OIDC Clients (Applications)

- List of client which is allowed to use the user session
  Each can have different config options;
  - Session lifetime
  - User attributes & roles



Clients

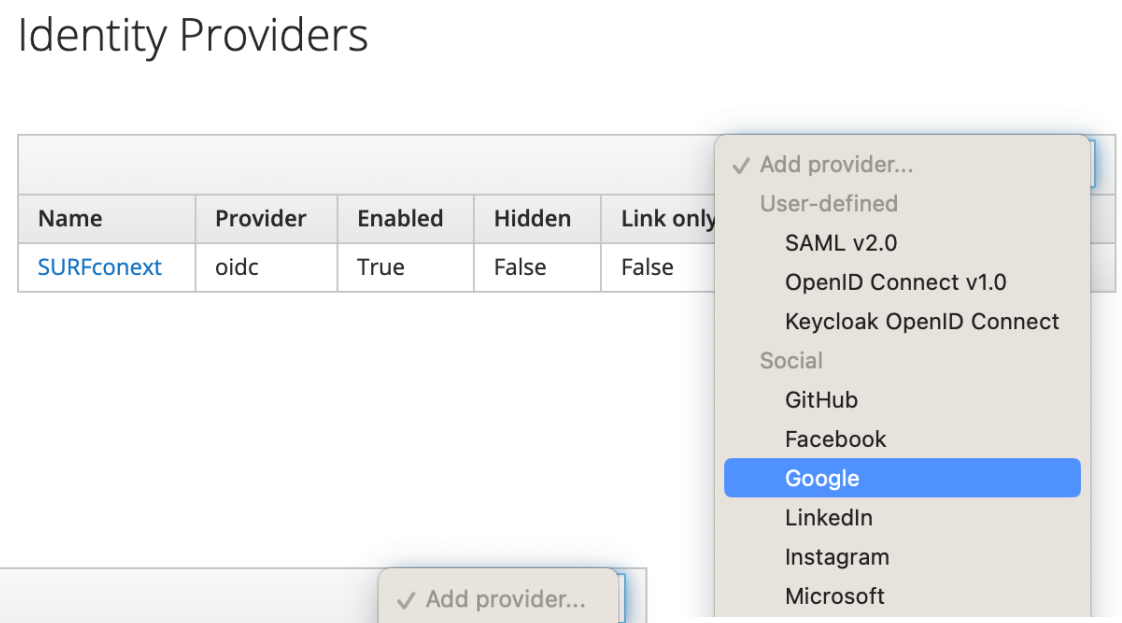
Lookup

Search... Create

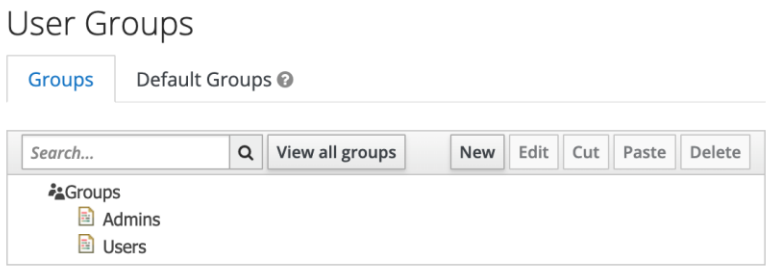
Client ID	Enabled	Base URL	Actions
account	True	https://tst-test.data.surfsara.nl/surf-iam/auth/realms/SURF/account/	Edit Export Delete
account-console	True	https://tst-test.data.surfsara.nl/surf-iam/auth/realms/SURF/account/	Edit Export Delete
admin-cli	True	Not defined	Edit Export Delete
broker	True	Not defined	Edit Export Delete
dashboard	True	Not defined	Edit Export Delete
e4rAsNUSlUs0lF4nbv9FmCeUkTlV9GdgTLDH1b5uie7syb90SzEVrbN7HlpmWJeD	True	Not defined	Edit Export Delete
mxd5OQDk6es5LzOzRvidJNfXLUZS2oN3oUFeXPP8LpPrhx3UroJFduGEYIBOxkY1	True	Not defined	Edit Export Delete
oc10	True	Not defined	Edit Export Delete
oc10-web	True	Not defined	Edit Export Delete
ocis-web	True	Not defined	Edit Export Delete
rdreporting	True	Not defined	Edit Export Delete
rdsettings	True	Not defined	Edit Export Delete
realm-management	True	Not defined	Edit Export Delete
security-admin-console	True	https://tst-test.data.surfsara.nl/surf-iam/auth/admin/SURF/console/	Edit Export Delete
xdXOt13JKxym1B1QcEncf2XDkLAexMBFwiT9j6EfhhHFJhs2KM9jbjTmf8JBXE69	True	Not defined	Edit Export Delete
_system	True	Not defined	Edit Export Delete

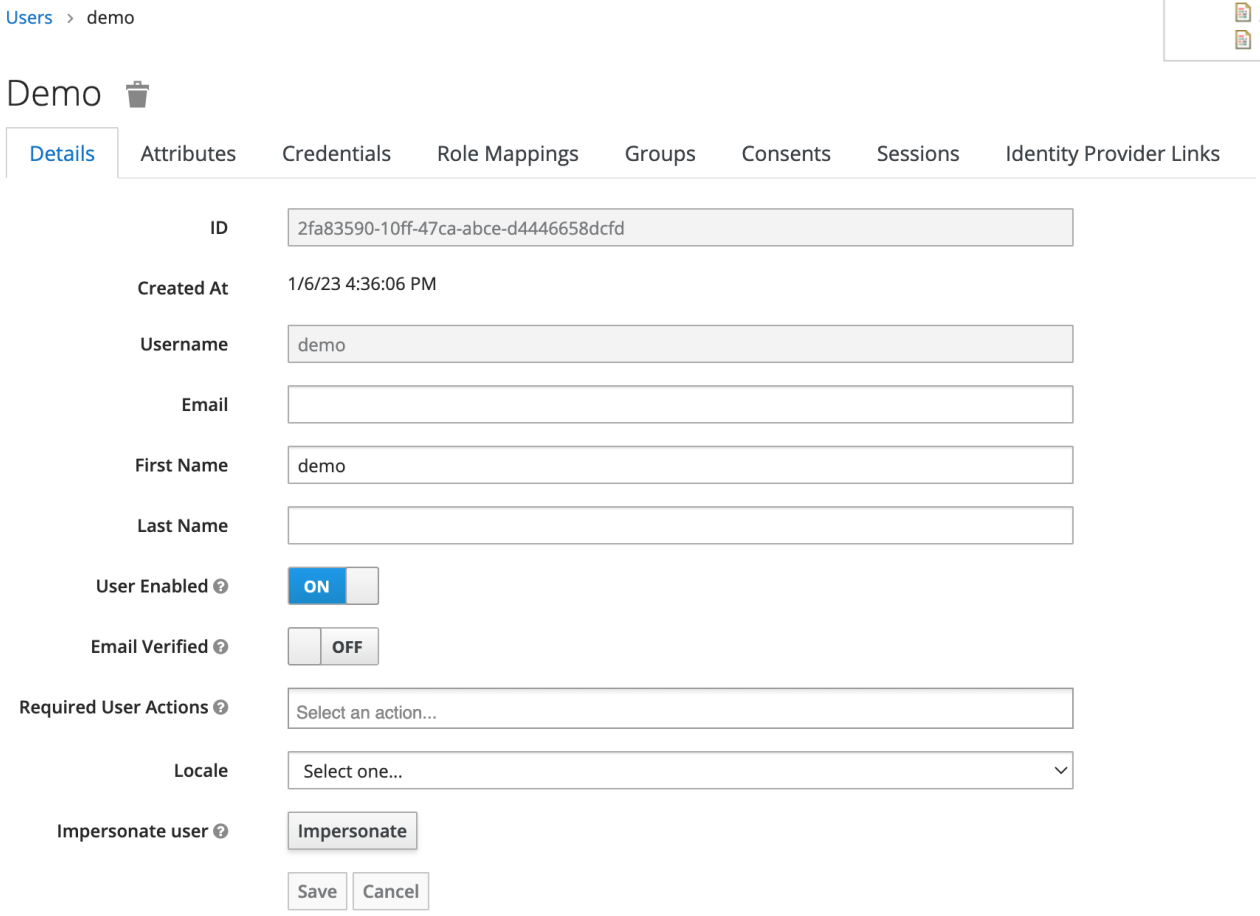
KeyCloak – Federation

- Authenticate or only provision account via external Identity provider
- Read or Read/Write user accounts to external federation for example a LDAP



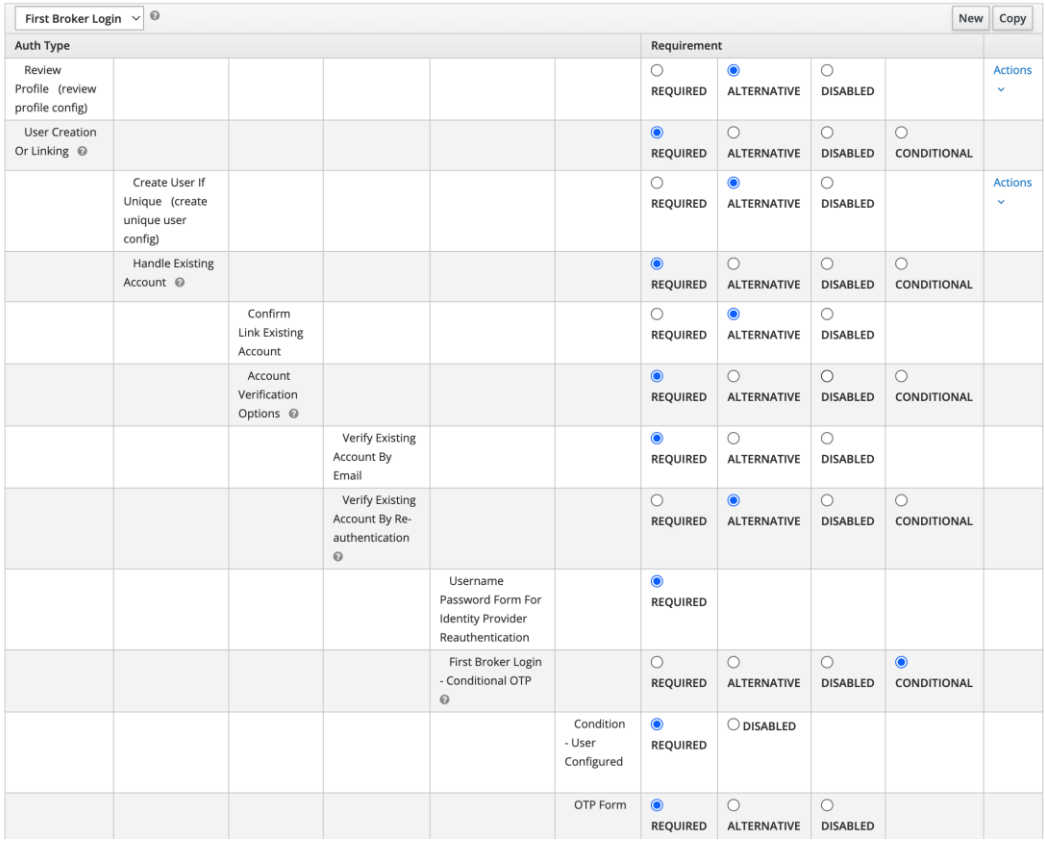
KeyCloak – Users & Groups





KeyCloak – Define the flows

- Multiple flows possible
  - Based on token client
  - Used authentication method
  - User settings (like MFA)

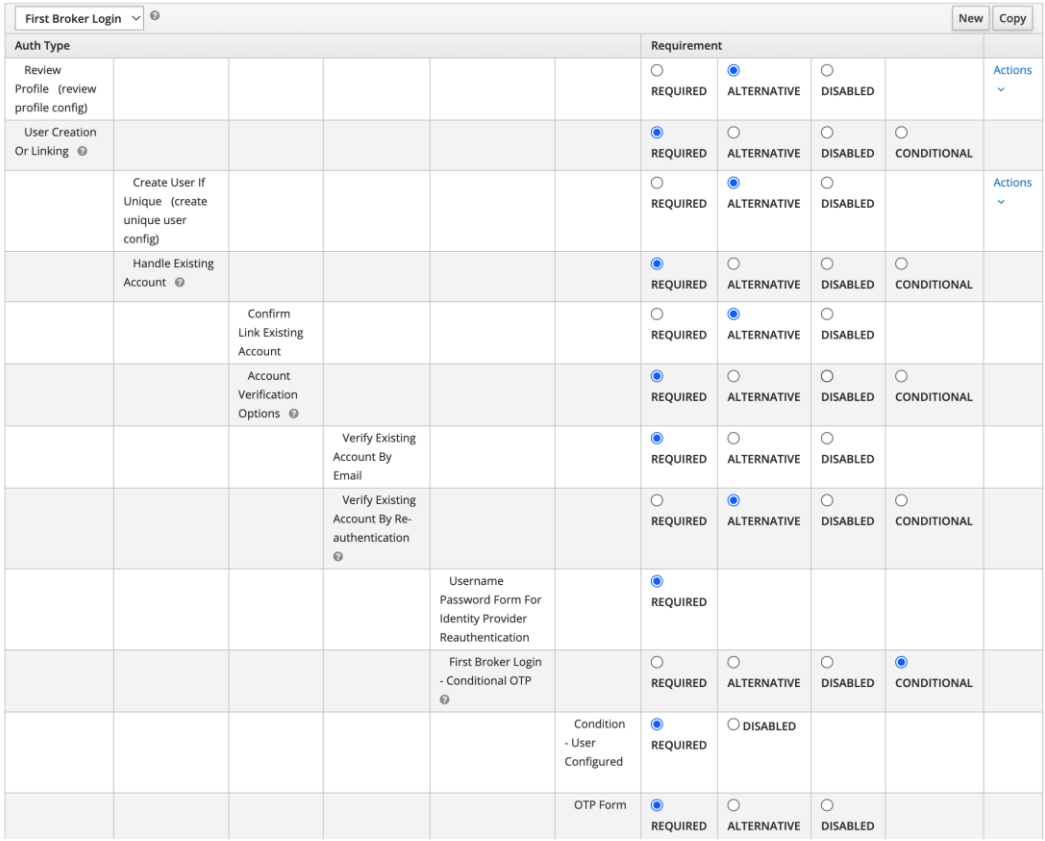


First Broker Login | New | Copy

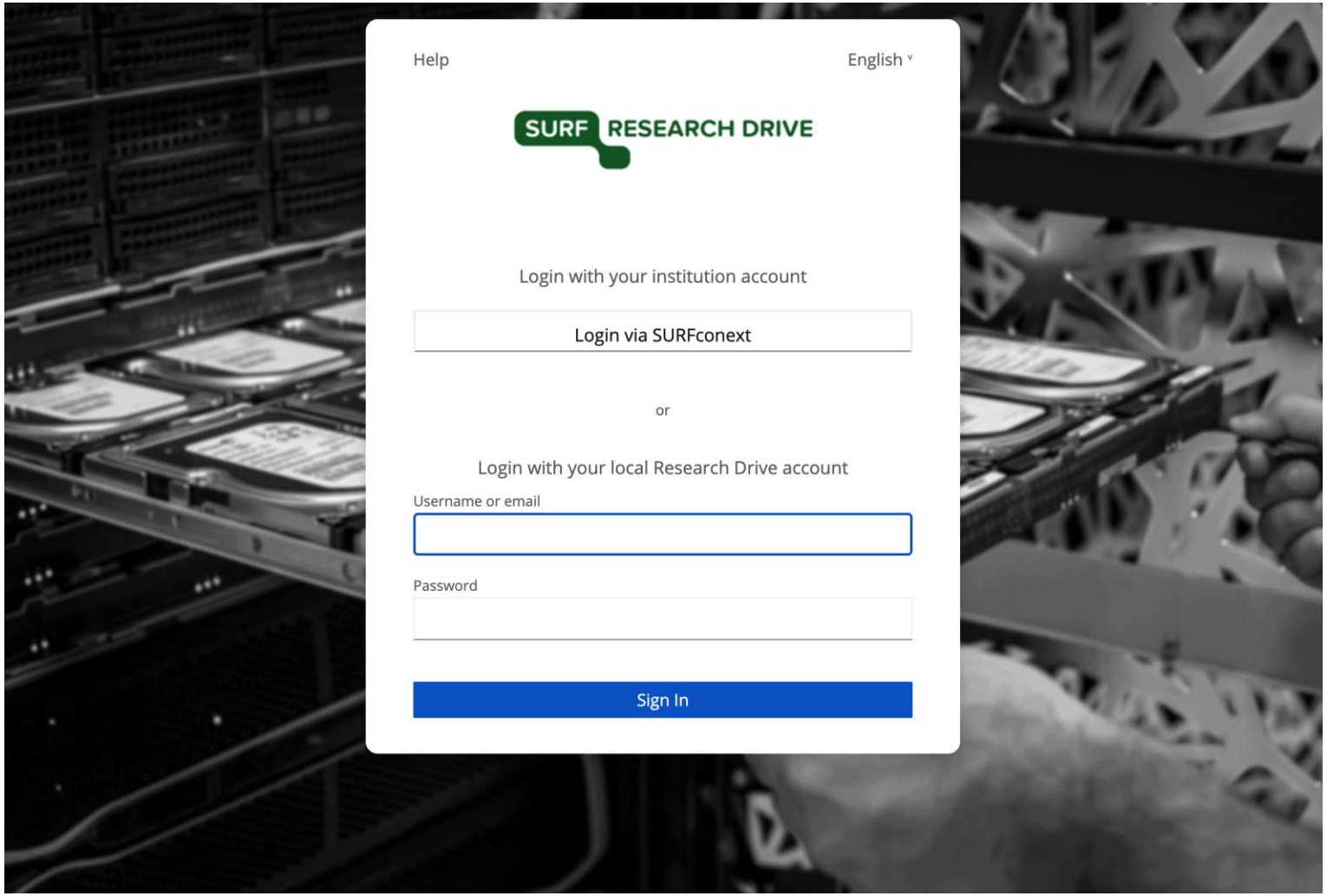
Auth Type						Requirement				
Review Profile (review profile config)						REQUIRED	ALTERNATIVE	DISABLED		Actions
User Creation Or Linking						REQUIRED	ALTERNATIVE	DISABLED	CONDITIONAL	
	Create User If Unique (create unique user config)					REQUIRED	ALTERNATIVE	DISABLED		Actions
	Handle Existing Account					REQUIRED	ALTERNATIVE	DISABLED	CONDITIONAL	
		Confirm Link Existing Account				REQUIRED	ALTERNATIVE	DISABLED		
		Account Verification Options				REQUIRED	ALTERNATIVE	DISABLED	CONDITIONAL	
			Verify Existing Account By Email			REQUIRED	ALTERNATIVE	DISABLED		
			Verify Existing Account By Re-authentication			REQUIRED	ALTERNATIVE	DISABLED	CONDITIONAL	
				Username Password Form For Identity Provider Reauthentication		REQUIRED				
				First Broker Login - Conditional OTP		REQUIRED	ALTERNATIVE	DISABLED	CONDITIONAL	
					Condition - User Configured	REQUIRED	DISABLED			
					OTP Form	REQUIRED	ALTERNATIVE	DISABLED		

KeyCloak – Define the flows

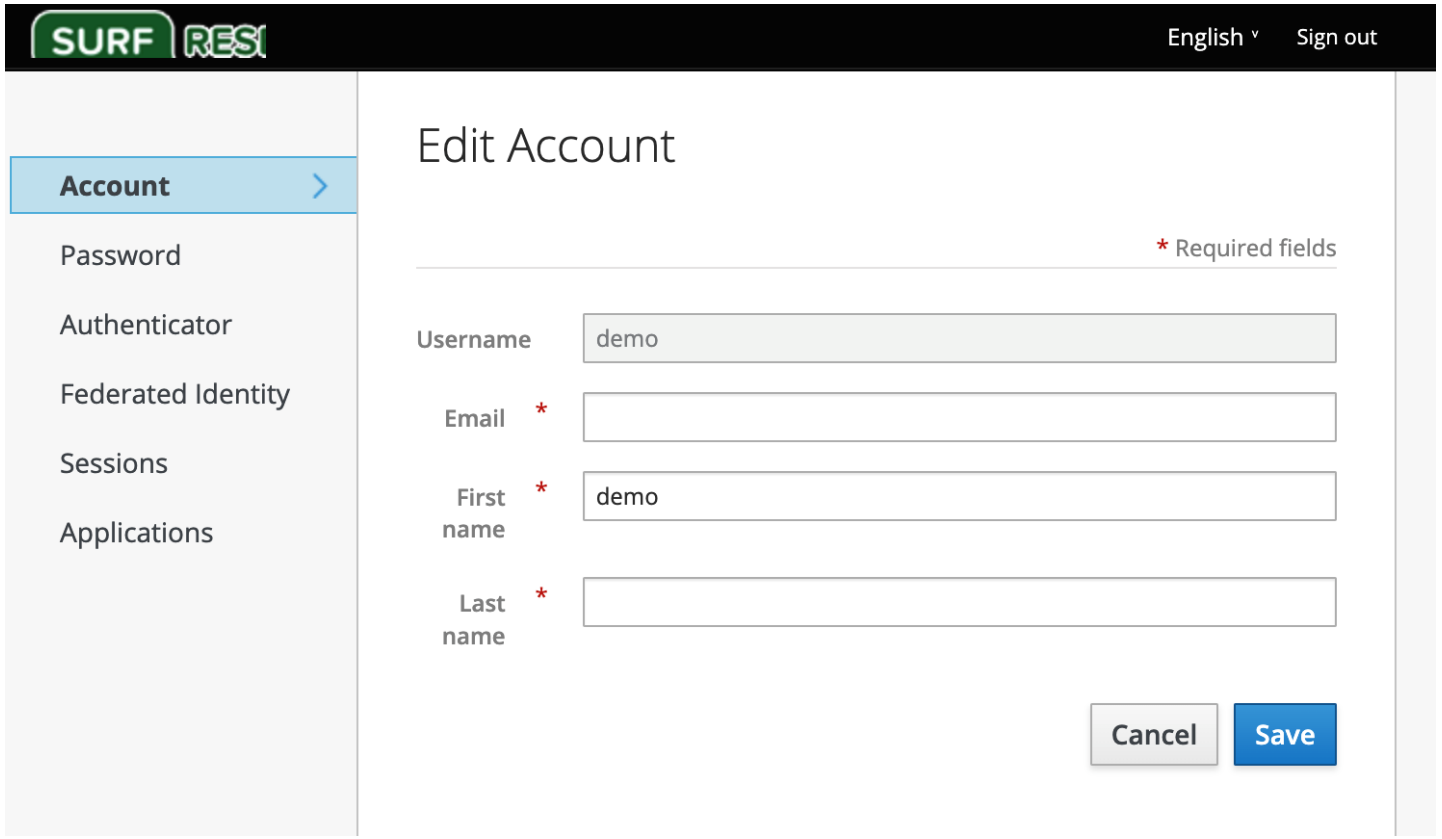
- Multiple flows possible
  - Based on token client
  - Used authentication method
  - User settings (like MFA)



KeyCloak – User facing



KeyCloak – User facing



Thanks!

Example;
https://github.com/T0mWz/ocis_individual_services

Tom Wezepoel
tom.wezepoel@surf.nl