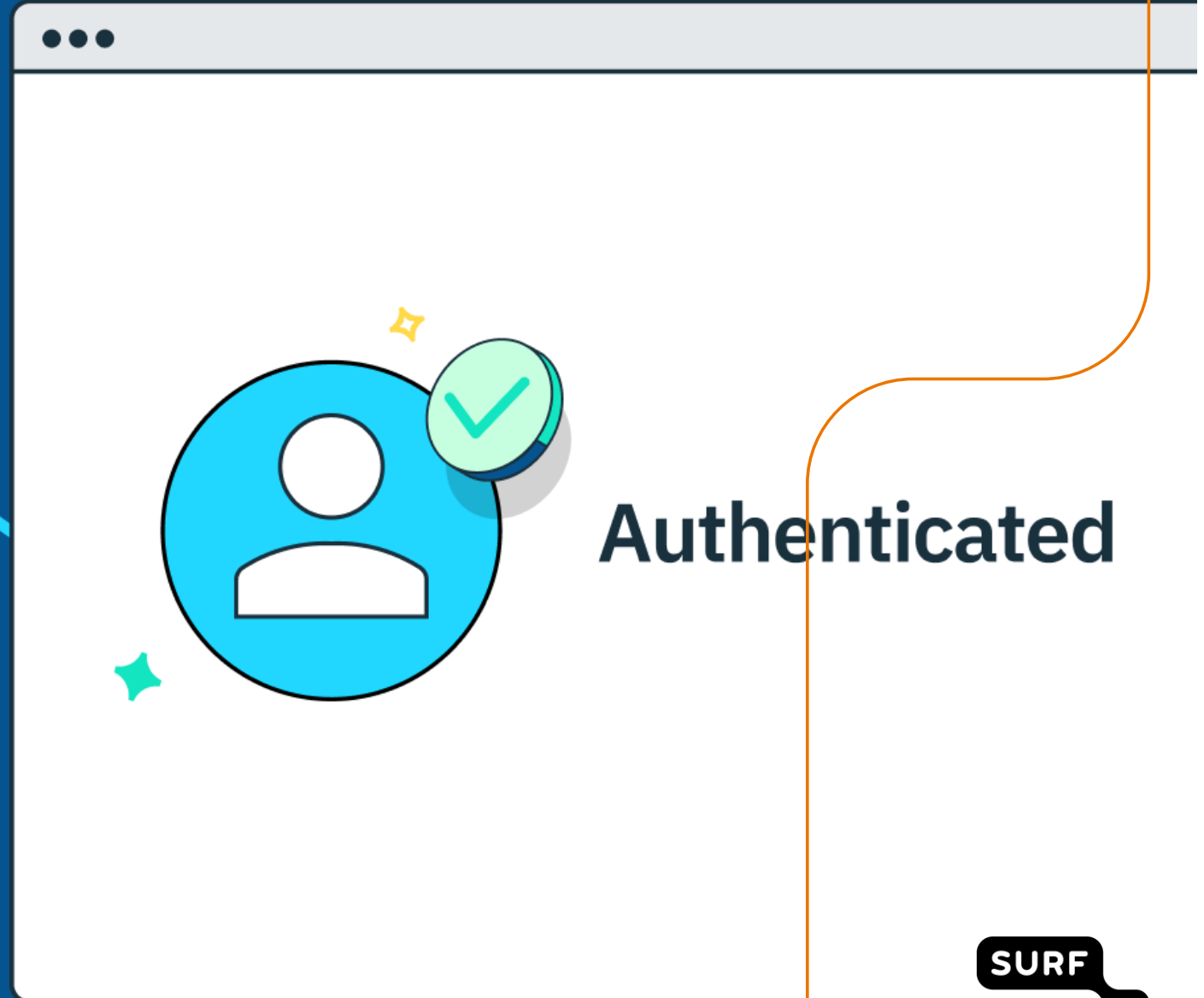


# OIDC

IT SEEMS TO BE  
HIP

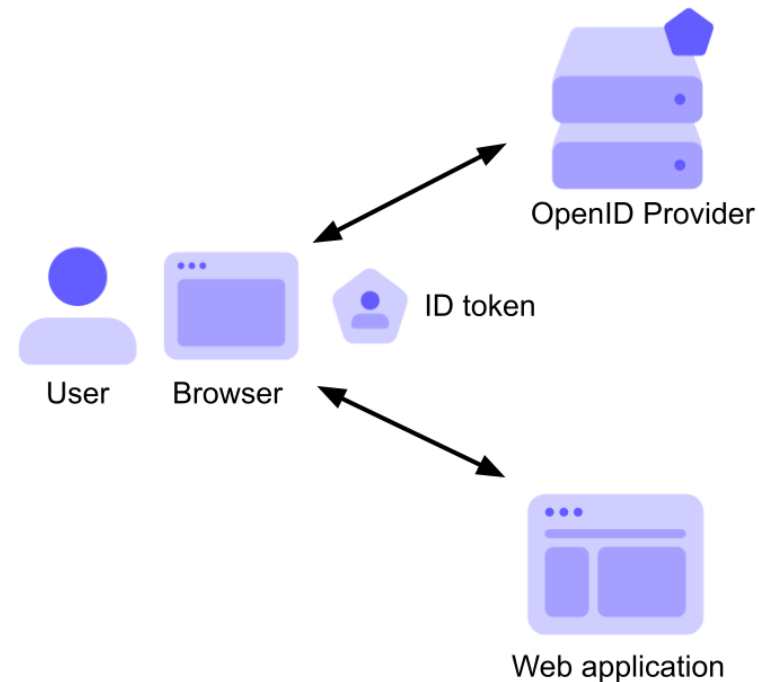


Authenticated

SURF

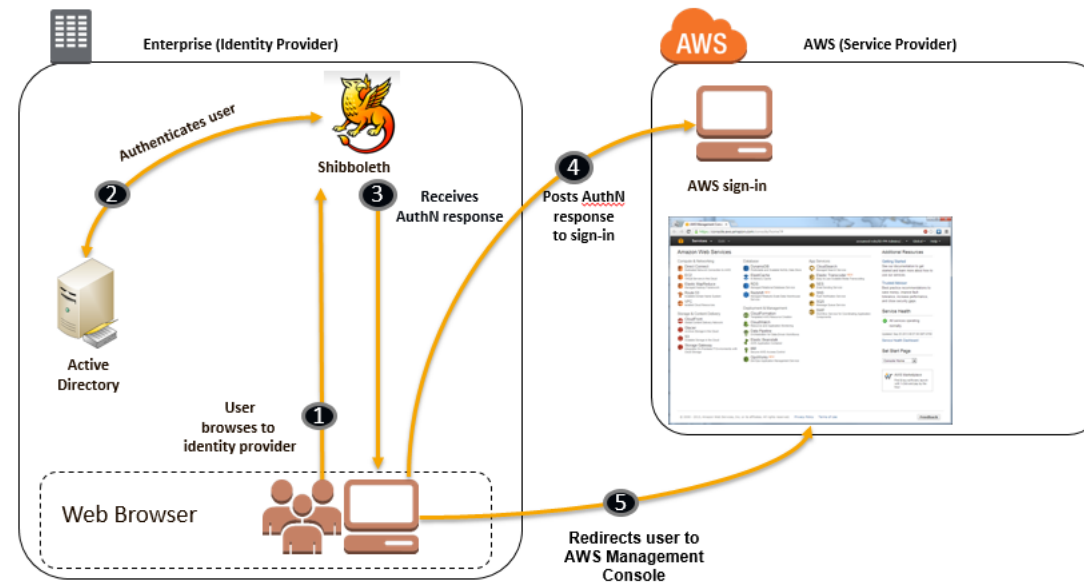
# What is OIDC

- 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?

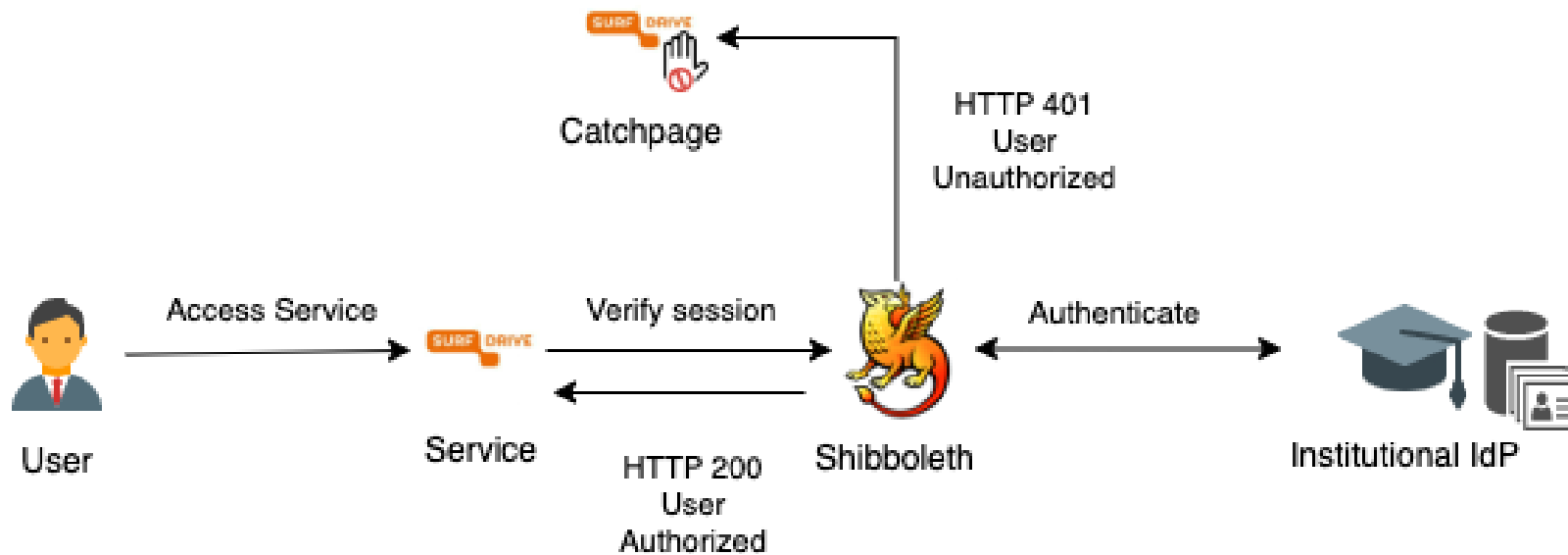
- Shibboleth – SAML authentication protocol for ownCloud
- SimpleSAMLphp for SURFdrive management application
- oAuth2 to authenticate applications for user session



# Why change, when it works ?

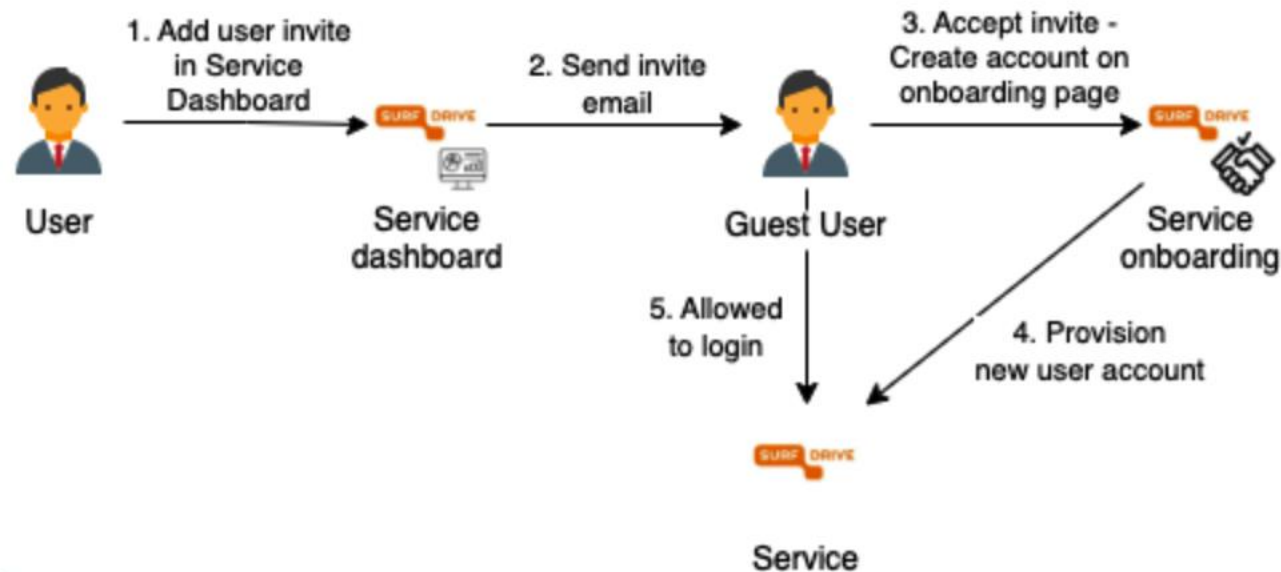
- Shibboleth is somewhat unstable
  - ***Healthcheck which kicks shibboleth when it crashed***
- Remove dependency on application support
- Ability to define user authentication flows
- Discouple application user from idp user
  - Quite hard when a username is changed these days.
- Session token on Session 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 decouple application account from IdP user
- Support for basic auth for WebDAV purpose

# What we compared

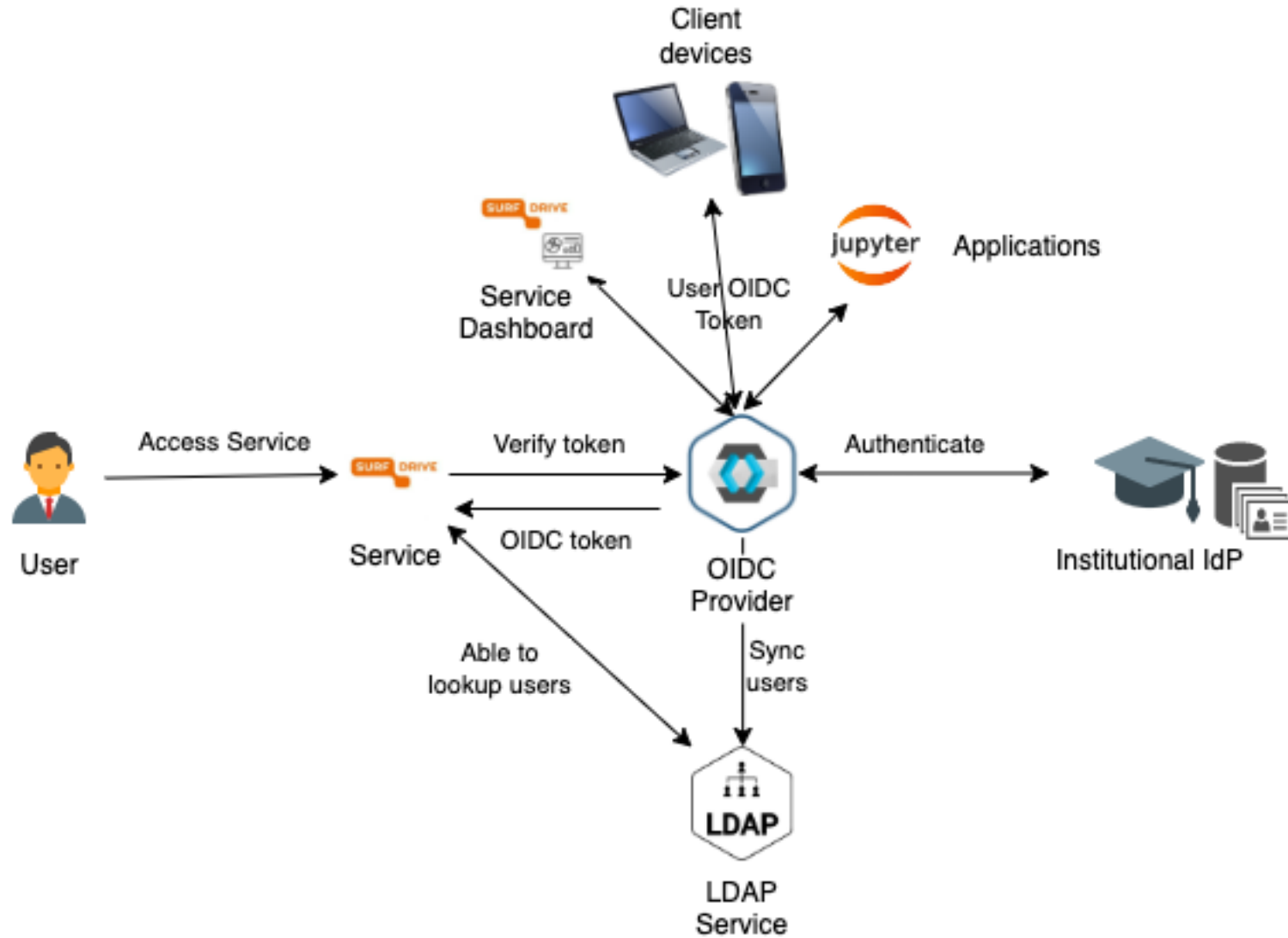




# Keycloak absolute winner

- 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...

Client ID	Enabled	Base URL	Actions		
account	True	<a href="https://tst-test.data.surfsara.nl/surf-iam/auth/realms/SURF/account/">https://tst-test.data.surfsara.nl/surf-iam/auth/realms/SURF/account/</a>	Edit	Export	Delete
account-console	True	<a href="https://tst-test.data.surfsara.nl/surf-iam/auth/realms/SURF/account/">https://tst-test.data.surfsara.nl/surf-iam/auth/realms/SURF/account/</a>	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
e4rAsNUSIU0lF4nbv9FmCeUkTV9GdgTLDH1b5uie7syb90S2zEVrbN7HlpmWJeD	True	Not defined	Edit	Export	Delete
mxd5OQDk6es5LzOzRvidjNfXLUZS2oN3oUFeXPP8LpPrhx3UrojFduGEYIB0xkY1	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	<a href="https://tst-test.data.surfsara.nl/surf-iam/auth/admin/SURF/console/">https://tst-test.data.surfsara.nl/surf-iam/auth/admin/SURF/console/</a>	Edit	Export	Delete
xdXOt13Jkxym1B1QcEncf2XDKLAexMBFwIT9j6EfhHFFjhs2KM9jbjTmf8JBXE69	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

## Identity Providers

Name	Provider	Enabled	Hidden	Link only
<a href="#">SURFconext</a>	oidc	True	False	False

✓ Add provider...

User-defined

- SAML v2.0
- OpenID Connect v1.0
- Keycloak OpenID Connect

Social

- GitHub
- Facebook
- Google**
- LinkedIn
- Instagram
- Microsoft

## User Federation

ID	Enabled	Provider Name	Priority	Act
<a href="#">openldap</a>	true	Ldap	0	...

✓ Add provider...





- kerberos
- ldap**

# KeyCloak – Users & Groups

[Users](#) > demo

Demo 

**Details** | [Attributes](#) | [Credentials](#) | [Role Mappings](#) | [Groups](#) | [Consents](#) | [Sessions](#) | [Identity Provider Links](#)

ID	<input type="text" value="2fa83590-10ff-47ca-abce-d4446658dcfd"/>
Created At	1/6/23 4:36:06 PM
Username	<input type="text" value="demo"/>
Email	<input type="text"/>
First Name	<input type="text" value="demo"/>
Last Name	<input type="text"/>
User Enabled 	<input checked="" type="checkbox"/> ON <input type="checkbox"/>
Email Verified 	<input type="checkbox"/> OFF <input type="checkbox"/>
Required User Actions 	<input type="text" value="Select an action..."/>
Locale	<input type="text" value="Select one..."/>
Impersonate user 	<input type="button" value="Impersonate"/>
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

## User Groups

**Groups** | [Default Groups](#) 

-  Groups
-  Admins
-  Users

# KeyCloak – Define the flows

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

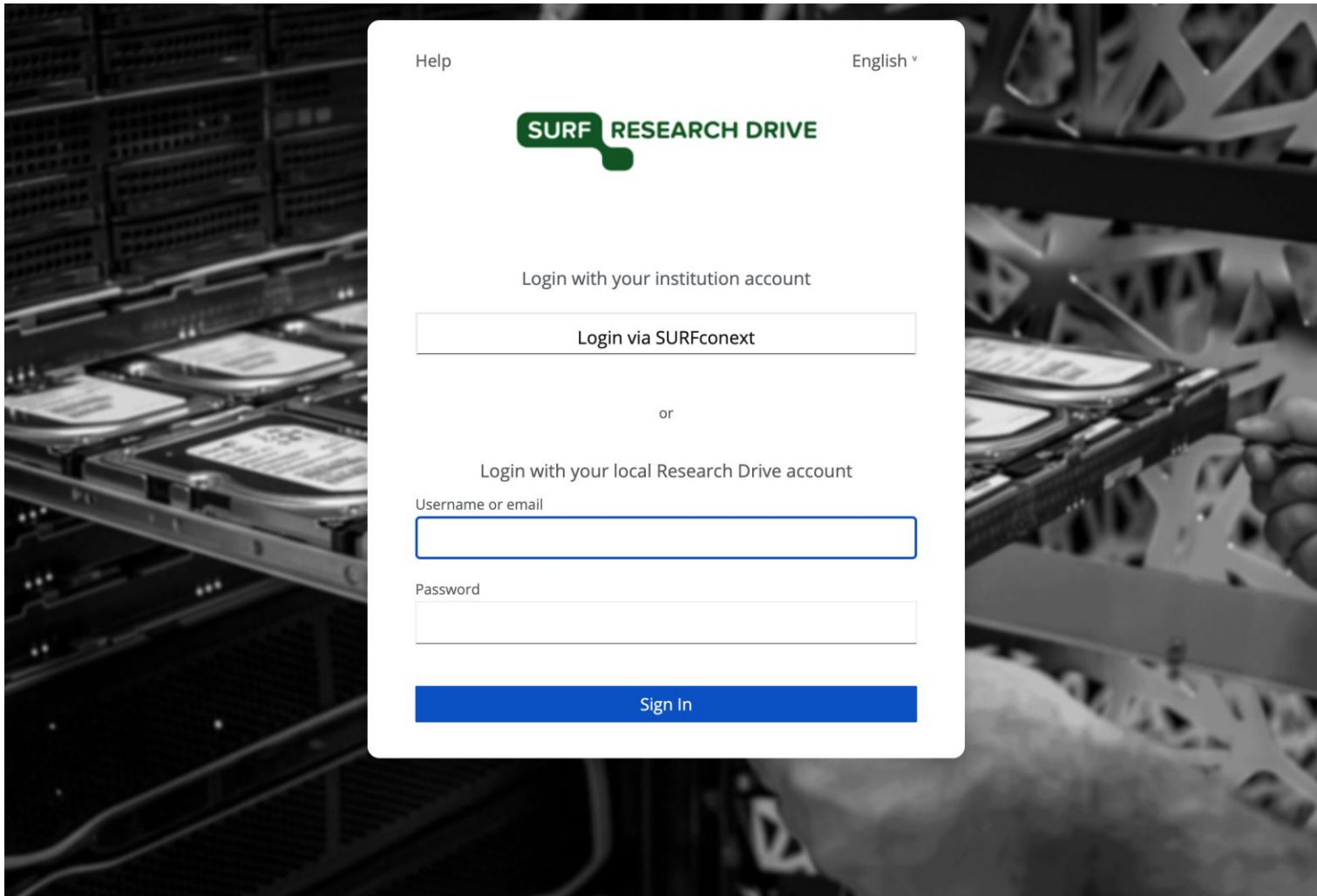
First Broker Login					Requirement				New	Copy
Auth Type										
Review Profile (review profile config)					<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED			Actions
User Creation Or Linking					<input checked="" type="radio"/> REQUIRED	<input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

# KeyCloak – Define the flows

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

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

# KeyCloak – User facing



Help English ▾

**SURF RESEARCH DRIVE**

Login with your institution account

Login via SURFconext

or

Login with your local Research Drive account

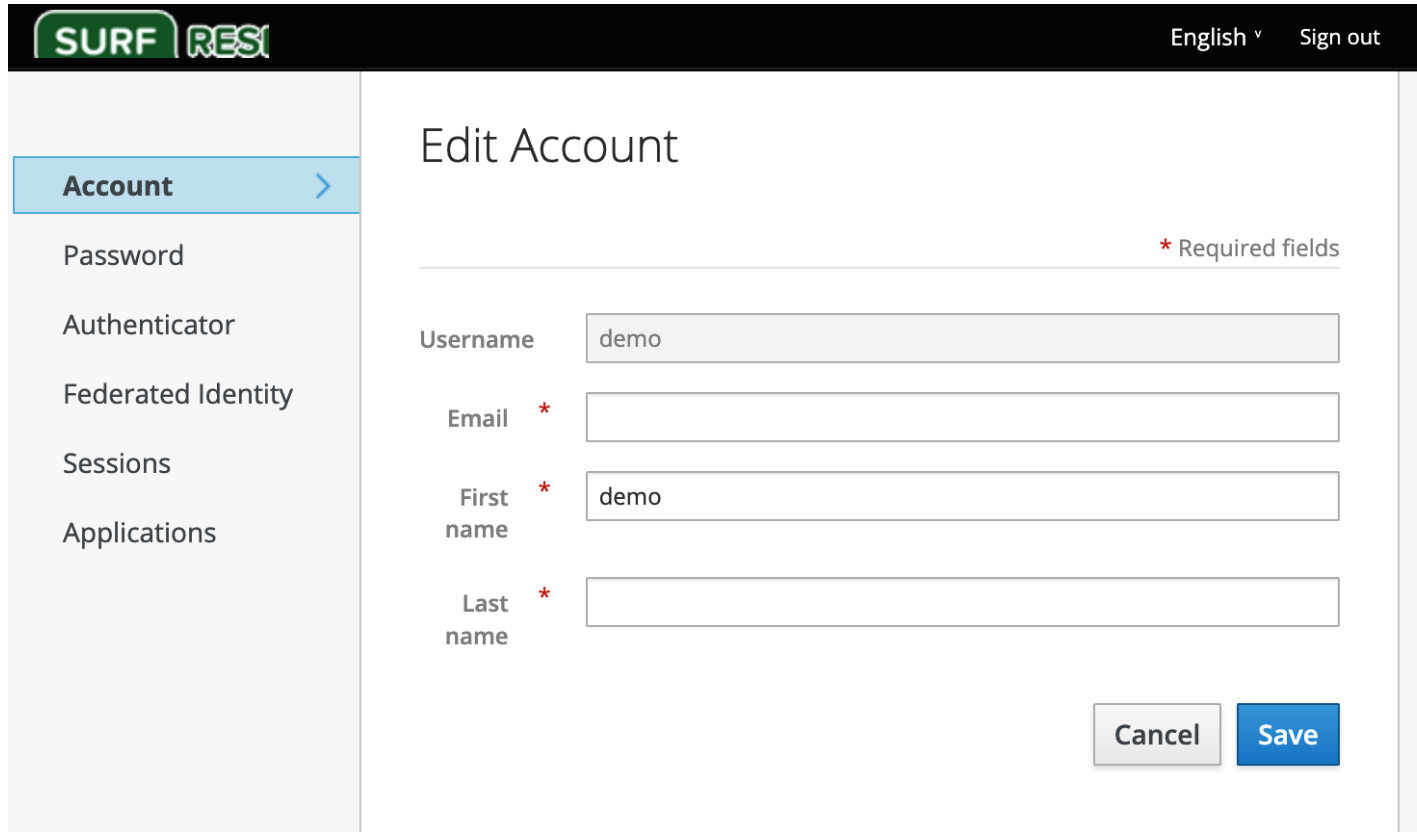
Username or email

Password

Sign In



# KeyCloak – User facing



The screenshot shows the 'Edit Account' page in the Keycloak user interface. At the top left is the SURF RES logo. At the top right, there is a language dropdown set to 'English' and a 'Sign out' link. A left-hand navigation menu is visible, with 'Account' selected and highlighted in blue. The main content area is titled 'Edit Account' and contains a form with the following fields: 'Username' (containing 'demo'), 'Email' (marked with a red asterisk), 'First name' (containing 'demo' and marked with a red asterisk), and 'Last name' (marked with a red asterisk). A legend indicates that red asterisks denote required fields. At the bottom right of the form are 'Cancel' and 'Save' buttons.

# Thanks!

Example;

[https://github.com/T0mWz/ocis\\_individual\\_services](https://github.com/T0mWz/ocis_individual_services)

Tom Wezepoel  
tom.wezepoel@surf.nl

**SURF**