20.11.2024

Hy DOAG K&A 2024_
Single Sign-On –
One Login for All Your Needs

Timo Herwix, Senior Consultant

code of change

Hyand by GOD | MT

Who am I?

Timo Herwix

Timo Herwix
Senior Consultant

Oracle ACE Pro

- Senior Consultant at Hyand since 2019
- Previously worked as a Data Warehouse Developer
- Oracle APEX since 2016
- Oracle Databases since 2008
- Blog author, conference speaker
- Born in 1983, two children and living in Germany

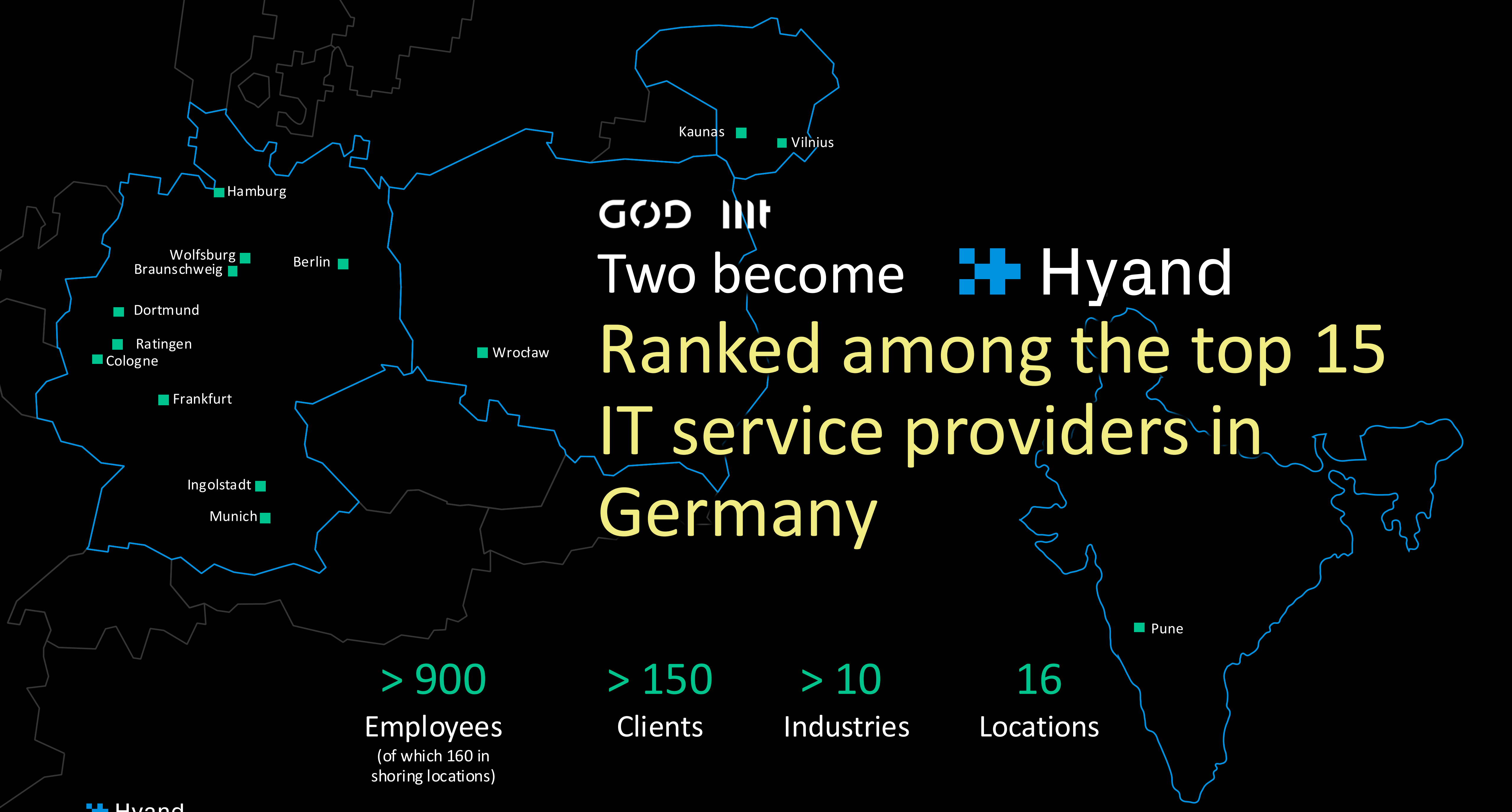
ORACLE Certified
Professional
Oracle Autonomous Database Cloud
2023

ORACLE Certified
Professional
Oracle APEX Cloud Developer

ORACLE Certified
Professional
Oracle Cloud Infrastructure Generative AI
2024

ORACLE Certified
Associate
Oracle Cloud Infrastructure Foundations
2023

ORACLE Certified
Associate
Oracle Cloud Infrastructure Architect
2023



Two become Hyand

Ranked among the top 15 IT service providers in Germany

> 900	> 150	> 10	16
Employees (of which 160 in shoring locations)	Clients	Industries	Locations

1

Introduction

2

Let´s dive deeper

3

Wrap-up

Single Sign-On
One Login for All Your Needs!

Source of truth for identities
Single Sign-On provides a single point of authentication

Developers

- Delegating a critical task like security to an expert in authentication is a smart move
- It removes the need to support or code a user management system within the APEX application
- This relieves the APEX developer from managing users and worrying about the security risks
- Not to mention the challenge of implementing Two-Factor Authentication and so on...

Users

- It improves User Experience by integrating with a suitable IdP, like using Entra ID for authentication in enterprises, allowing APEX login with the same credentials
- For public APEX apps, using IdPs like Google or Facebook simplifies user signup, avoiding the need for new account details

Authentication vs. Authorization.

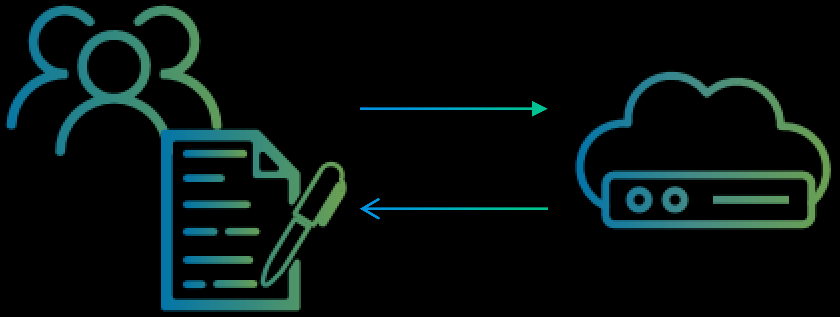
Authentication

Who are you?

401 Unauthorized

Authorization

What you can do?



403 Forbidden

Authentication.

- 👎 No Authentication (only for a public app ok, but be aware of DDoS)
- 👎 Open Door Credentials (only allowed in a dev/test environment)
- 👎 Custom (why reinvent the wheel and store passwords yourself?)
- 👎 LDAP-Directory (insecure)
- 👍 Database Accounts (only for legacy reasons)
- 👍 Oracle APEX Accounts (if no external Identity Provider is available)
- 👍 HTTP Header Variable (delegates authentication to external IdP)
- 👍 SAML Sign-In (delegates authentication to external IdP)
- 👍 Social Sign-In (delegates authentication to external IdP)

Hyand

OCI Demo App

DEMO

•••••••••••••

□ Remember username

Authentication Protocols - What should you go for?

SAML

XML-based framework for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP).

OAuth 2.0

OAuth 2.0 controls and delegates authorization to access a protected resource, like your web app, native app, or API service. It provides API security through scoped access tokens.

OpenID Connect

Extends OAuth 2.0 with user authentication and Single Sign-On (SSO) functionality. It enables you to retrieve and store authentication information about your end users. It also defines several OAuth 2.0 scopes to enable apps to access user profile information.

Kerberos

Uses tickets granted by a trusted third-party (Key Distribution Center - KDC) to authenticate users and services within a network.

Authentication Protocols - What should you go for?

SAML

Included as a Built-In Authentication since Version 21.2+ (Requires DB 19+)

Alternative: Use HTTP Header Variable as Authentication Scheme

Setup time: 2-4 hours.

OAuth 2.0

OpenID Connect

Better known as "Social Sign-In" Authentication.
Social Sign-In was introduced in APEX 18.1.

With Social Sign-In, you can easily authenticate using Google, Facebook, and other social networks that support OpenID Connect or OAuth2 standards.

It only takes about 1-2 hours to set up!

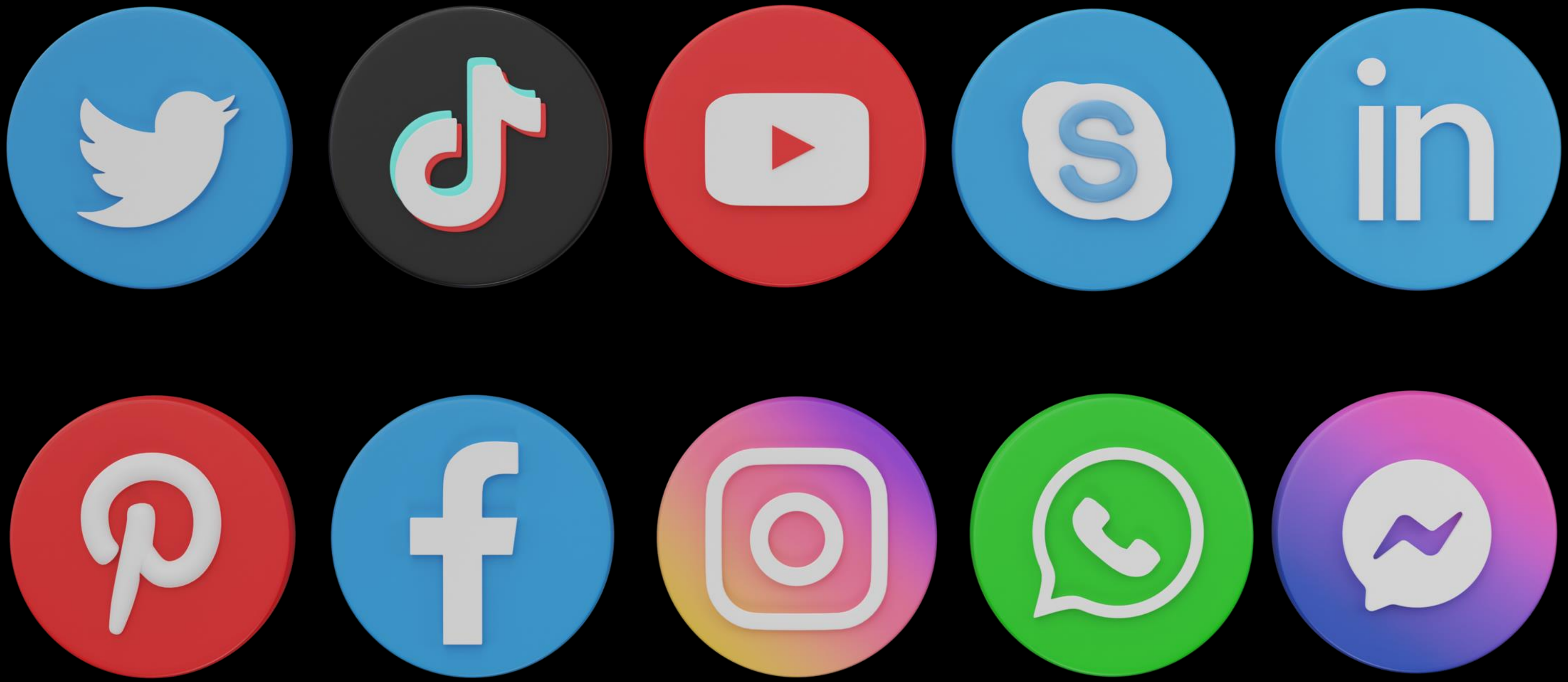
Kerberos

Kerberos is ideal for internal APEX environments, especially with Active Directory as the IdP.

It is well-known for use in Microsoft Windows networks, but it also works on macOS.

Setup time: 4-8 hours

Social Sign-In!



okta
ORACLE
Google Cloud IAM
Azure
KEYCLOAK

Why Oracle IAM/Entra ID?

- Both are a cloud-based platform
- Both IDPs are free, making it a great starting point for learning
- You can manage both - cloud and on-premise - Apps
- Oracle APEX integrates easily with both IDPs, requiring no to minimal coding and can be done in about 30 minutes
- Many customers use Entra ID, so it makes sense to take a closer look at it

1

Introduction

2

Let´s dive deeper

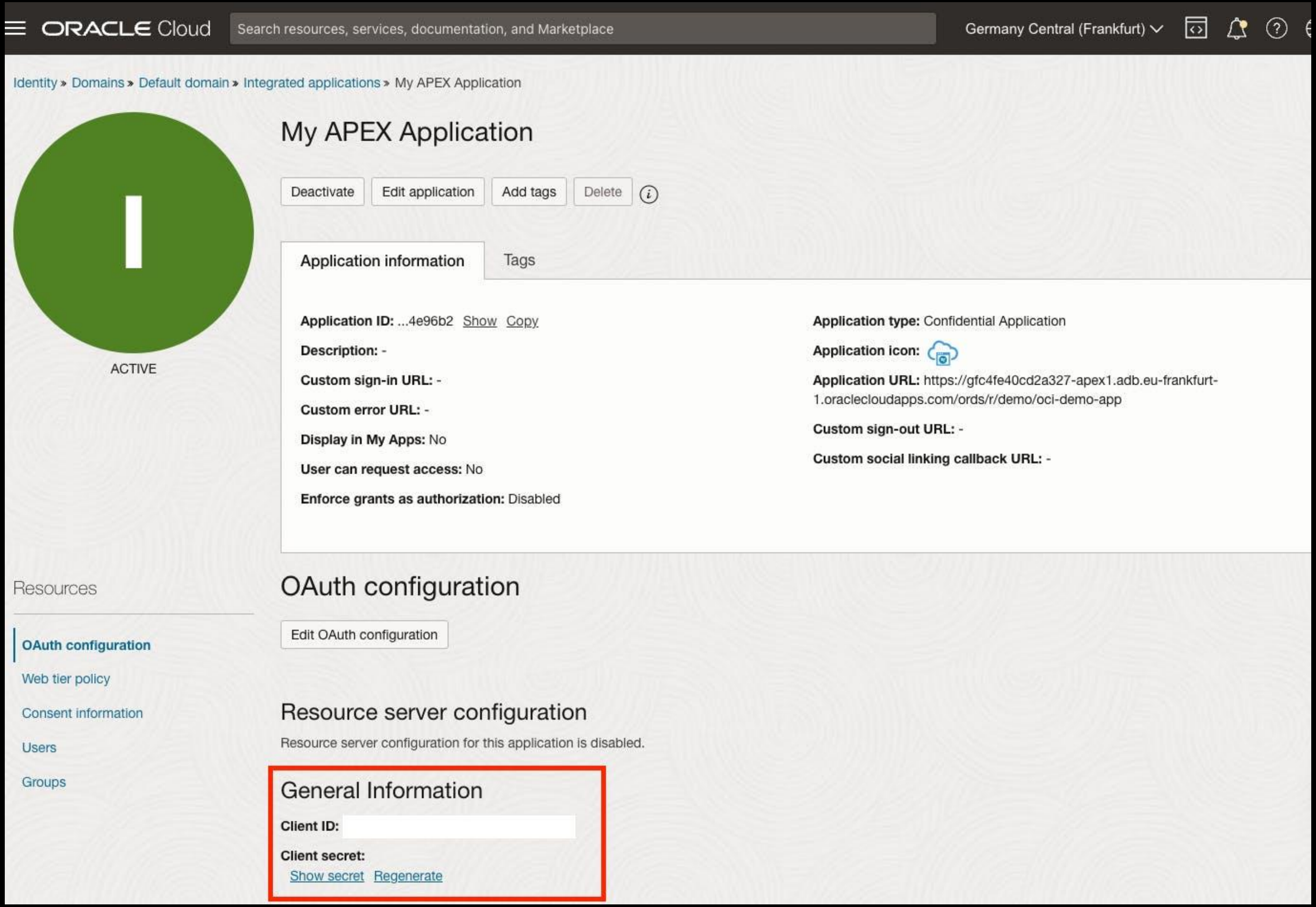
3

Wrap-up

Hyand

Implementing Social Sign-In in APEX.

OCI Configuration for Social Sign-In.



ORACLE Cloud
Search resources, services, documentation, and Marketplace
Germany Central (Frankfurt)
I
ACTIVE

Identity » Domains » Default domain » Integrated applications » My APEX Application

My APEX Application

Deactivate | Edit application | Add tags | Delete

Application information | Tags

Application ID: ...4e96b2 Show Copy

Description: -

Custom sign-in URL: -

Custom error URL: -

Display in My Apps: No

User can request access: No

Enforce grants as authorization: Disabled

Application type: Confidential Application

Application icon:

Application URL: https://gfc4fe40cd2a327-apex1.adb.eu-frankfurt-1.oraclecloudapps.com/ords/r/demo/oci-demo-app

Custom sign-out URL: -

Custom social linking callback URL: -

Resources

- OAuth configuration
- Web tier policy
- Consent information
- Users
- Groups

OAuth configuration

Edit OAuth configuration

Resource server configuration

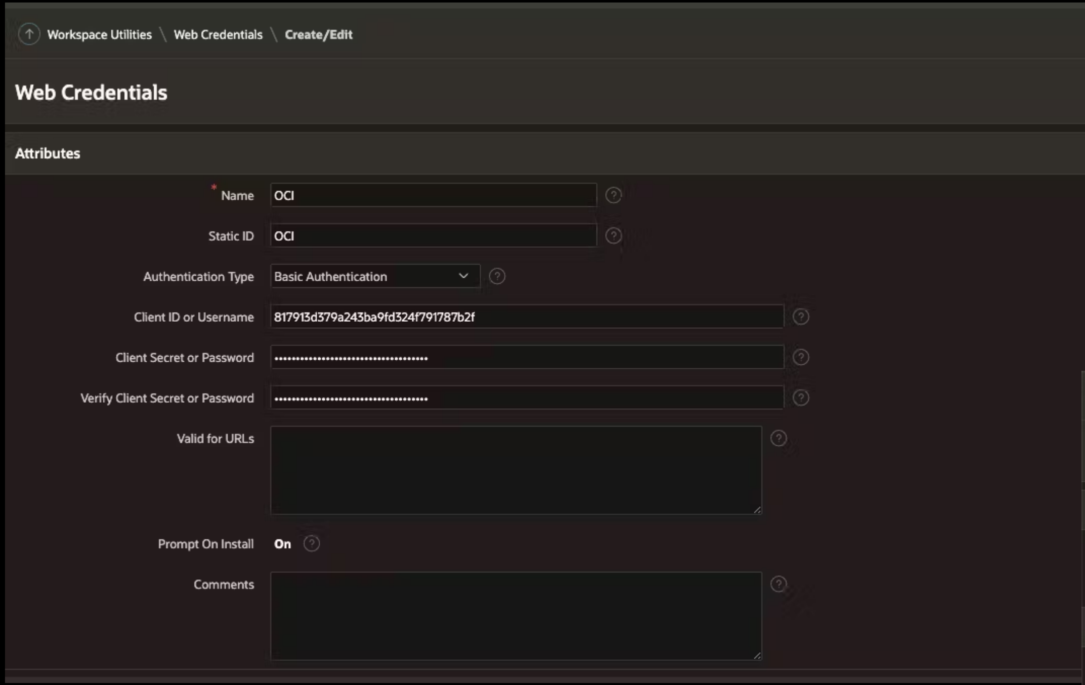
Resource server configuration for this application is disabled.

General Information

Client ID:

Client secret:
Show secret Regenerate

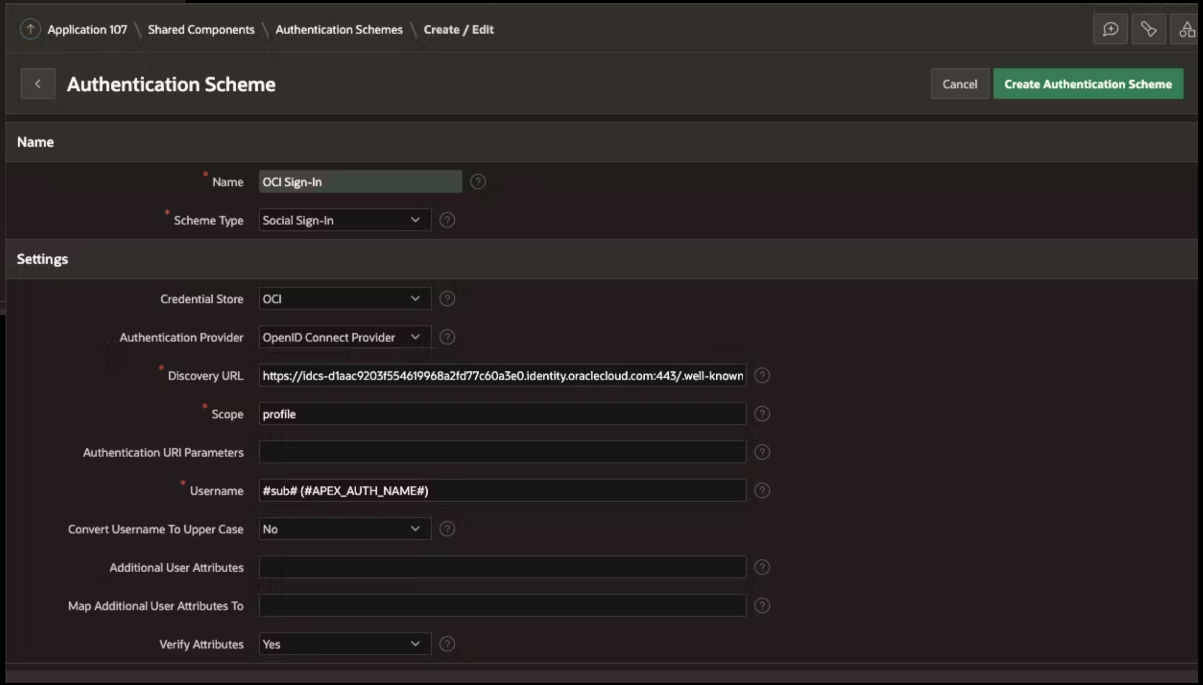
APEX Configuration for Social Sign-In.



Web Credentials

Attributes

* Name	OCI
Static ID	OCI
Authentication Type	Basic Authentication
Client ID or Username	817913d379a243ba9fd324f791787b2f
Client Secret or Password	••••••••••••••••••••••••••••••••••••
Verify Client Secret or Password	••••••••••••••••••••••••••••••••••••
Valid for URLs	
Prompt On Install	On
Comments	



Application 107 \ Shared Components \ Authentication Schemes \ Create / Edit
Cancel
Create Authentication Scheme

Authentication Scheme

Name

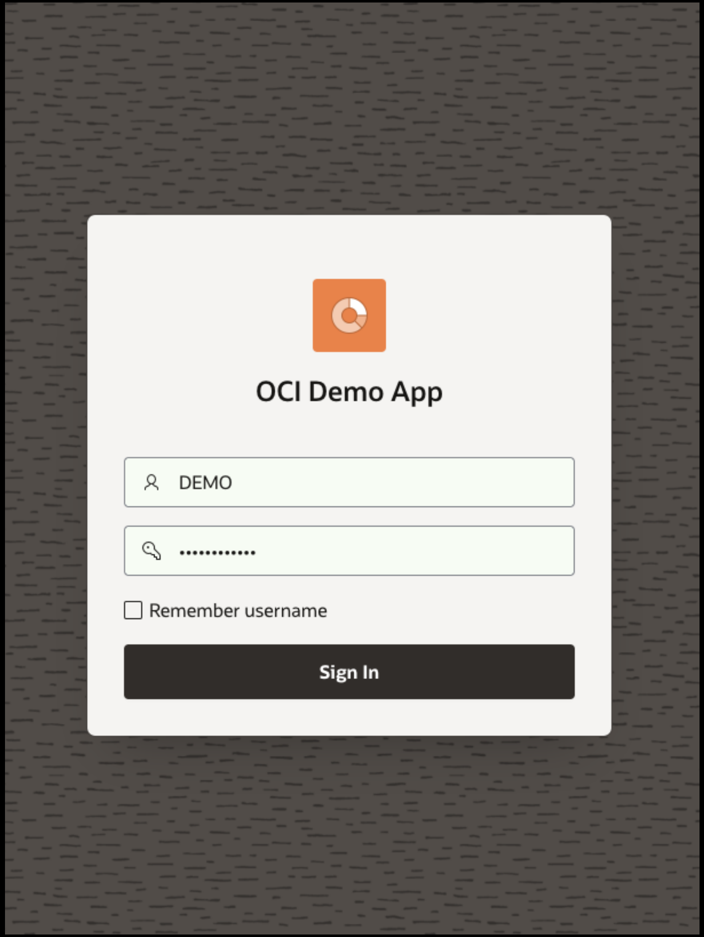
* Name	OCI Sign-In
* Scheme Type	Social Sign-In

Settings

Credential Store	OCI
Authentication Provider	OpenID Connect Provider
* Discovery URL	https://idcs-d1aac9203f554619968a2fd77c60a3e0.identity.oraclecloud.com:443/.well-known
* Scope	profile
Authentication URI Parameters	
* Username	#sub# (#APEX_AUTH_NAME#)
Convert Username To Upper Case	No
Additional User Attributes	
Map Additional User Attributes To	
Verify Attributes	Yes

Hyand

Social Sign-In!

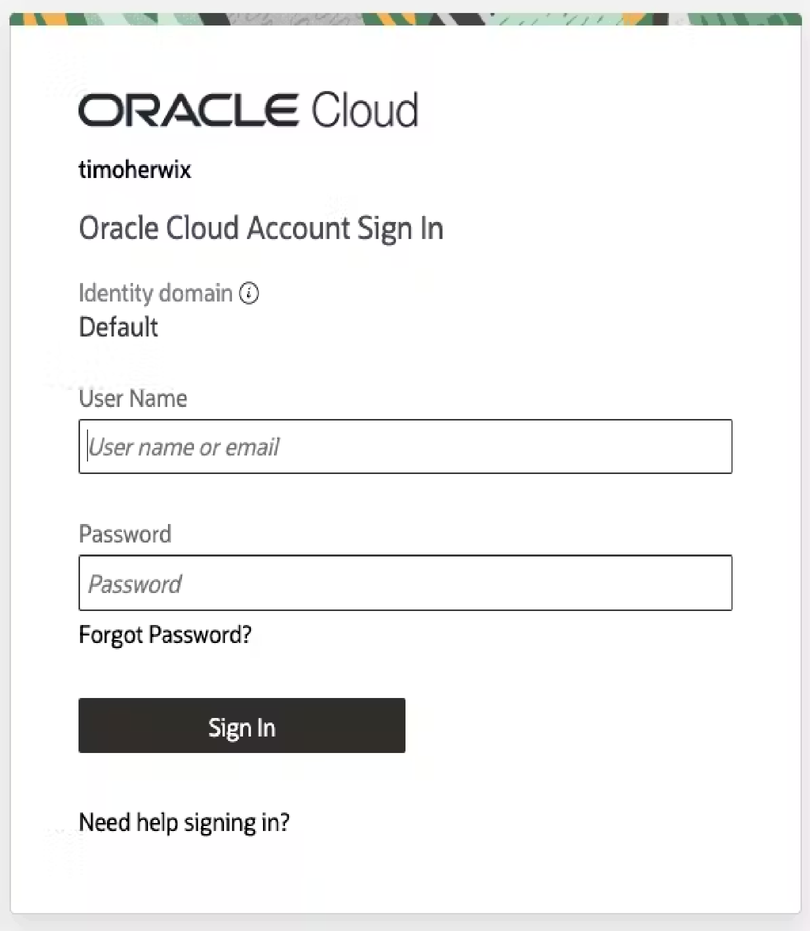


OCI Demo App

DEMO

••••••••••••

□ Remember username



ORACLE Cloud

timoherwix

Oracle Cloud Account Sign In

Identity domain ⓘ
Default

User Name
User name or email

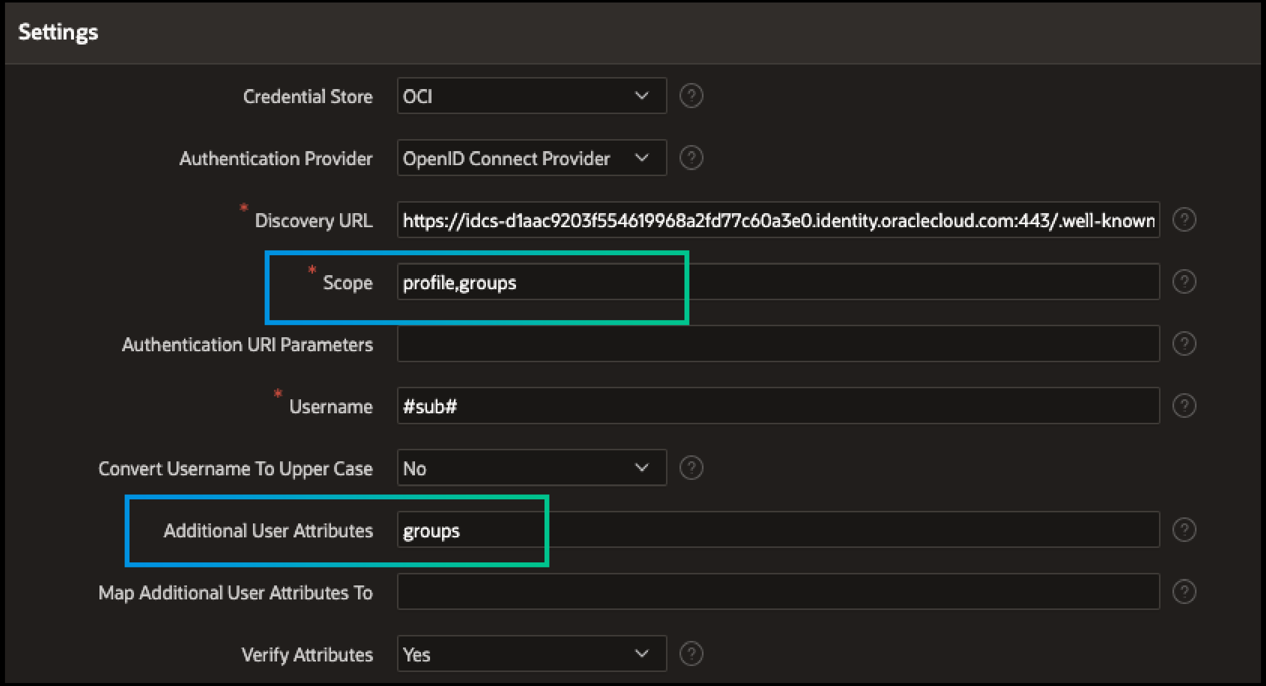
Password
Password

Forgot Password?

Need help signing in?

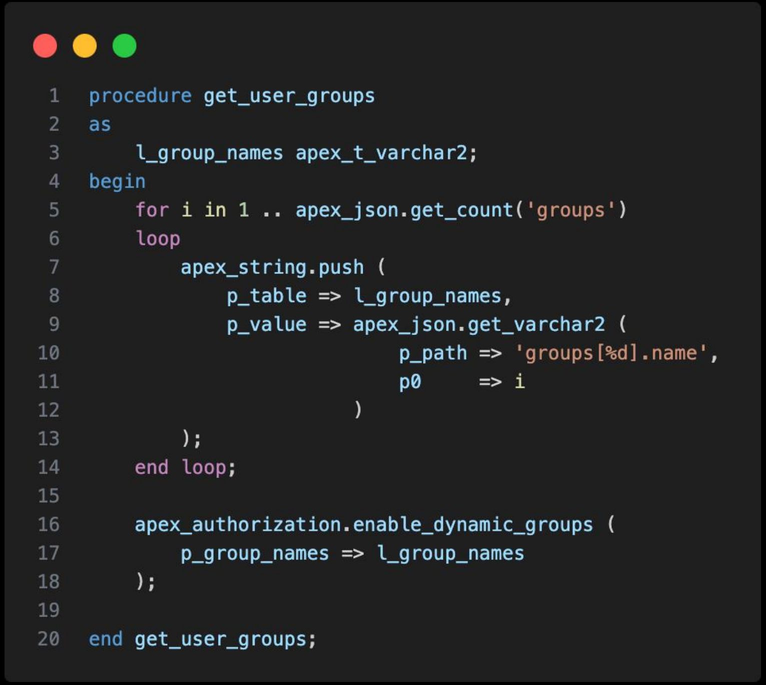
Manage User rights in APEX using Oracle IAM Groups!

Manage User rights in APEX using Oracle IAM Groups!



Settings

Credential Store	OCI
Authentication Provider	OpenID Connect Provider
* Discovery URL	https://idcs-d1aac9203f554619968a2fd77c60a3e0.identity.oraclecloud.com:443/.well-known
* Scope	profile,groups
Authentication URI Parameters	
* Username	#sub#
Convert Username To Upper Case	No
Additional User Attributes	groups
Map Additional User Attributes To	
Verify Attributes	Yes

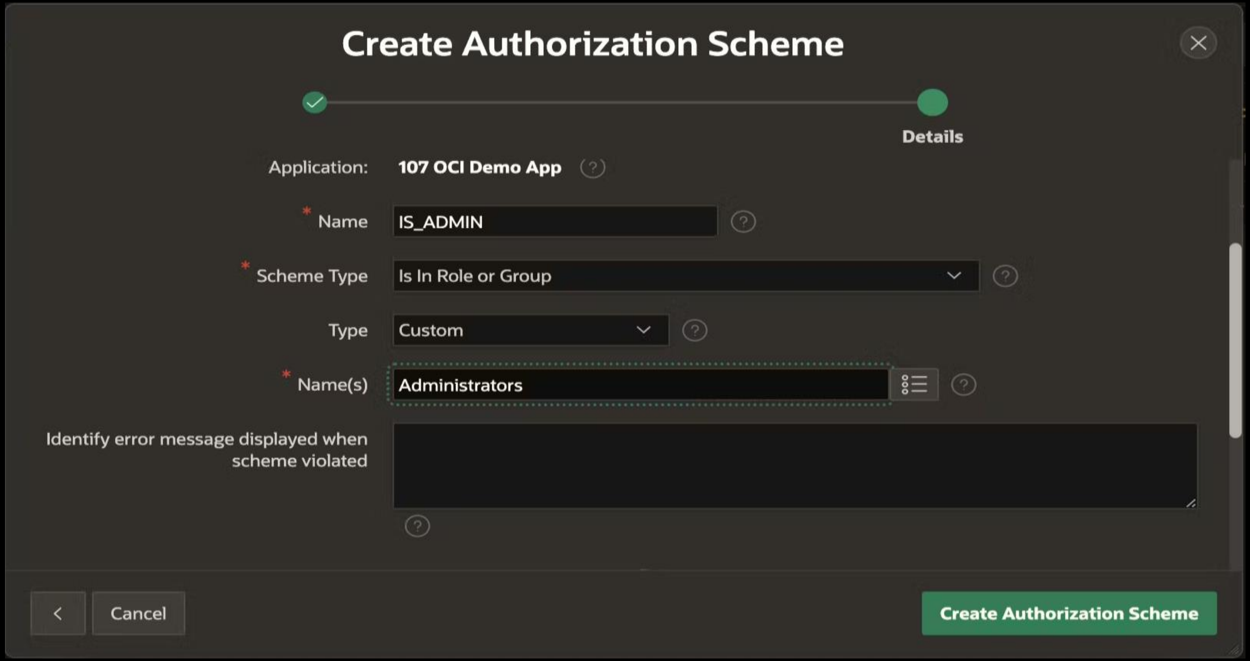


```
procedure get_user_groups
as
    l_group_names apex_t_varchar2;
begin
    for i in 1 .. apex_json.get_count('groups')
    loop
        apex_string.push (
            p_table => l_group_names,
            p_value => apex_json.get_varchar2 (
                           p_path => 'groups[%d].name',
                           p0     => i
                       )
        );
    end loop;

    apex_authorization.enable_dynamic_groups (
        p_group_names => l_group_names
    );

end get_user_groups;
```

Manage User rights in APEX using Oracle IAM Groups!



Create Authorization Scheme

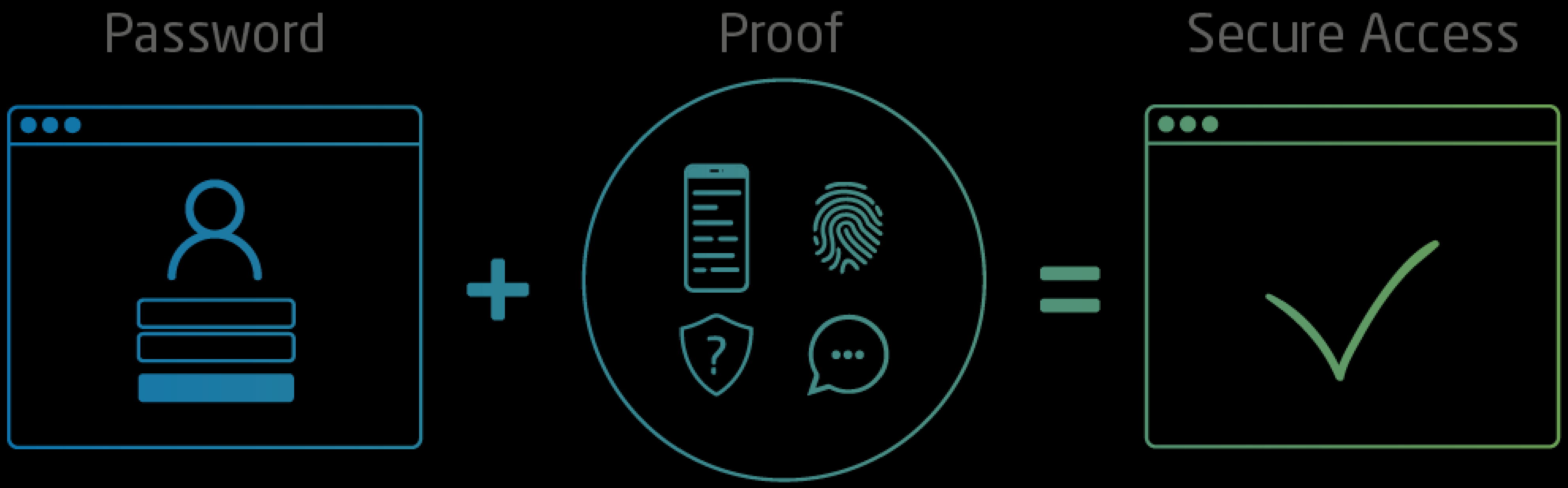
Application:	107 OCI Demo App
* Name	IS_ADMIN
* Scheme Type	Is In Role or Group
Type	Custom
* Name(s)	Administrators
Identify error message displayed when scheme violated	

Controlling Access to...

- Applications
- Pages
- Page Components

Multi-Factor Authentication!

By adding an extra barrier and layer of security, MFA can stop more than 99.9 percent of attempts to hack into accounts!

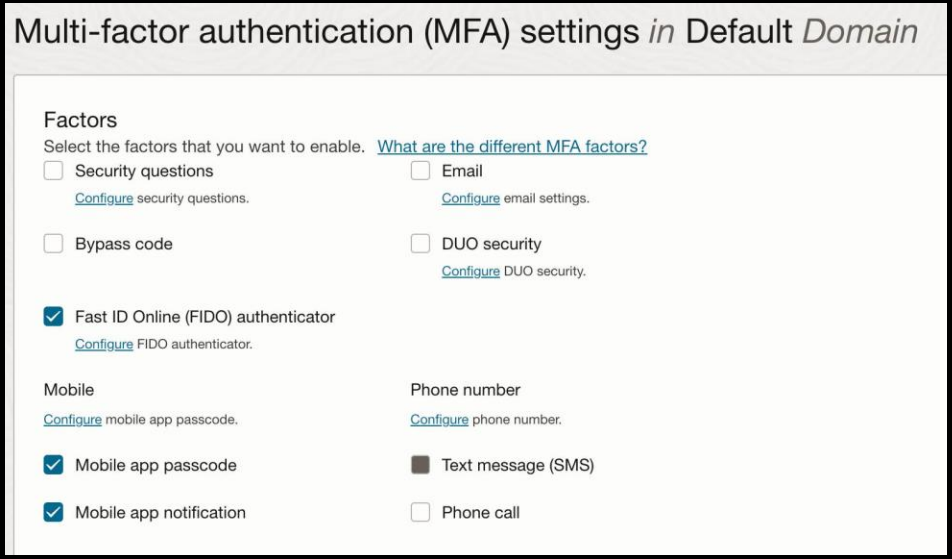


Authentication Factors!

- Security Questions: Users verify their identity by answering a set number of questions after entering their username and password.
- Email: OCI sends a one-time passcode to the user's primary email for second verification.
- Duo Security: Enable Duo Security for MFA, allowing users to authenticate via the Duo App or other factors.
- Fast ID Online (FIDO): Configure FIDO authentication for users to utilize external devices like YubiKey or internal devices like Windows Hello or Mac Touch ID for identity domain authentication.
- Mobile App Passcode: Use an authenticator app like Oracle Mobile Authenticator or Google Authenticator for generating OTPs.
- Mobile App Notification: Send a push notification with an approval request for login attempts. After entering credentials, a request is sent to the user's phone app, and they tap Allow to authenticate.
- Text Message (SMS) or Phone Call: Users receive a passcode via text or call for use as a second verification method after entering their username and password.

Multi-Factor Authentication (MFA) in OCI.

Enabling Multi-Factor Authentication



Multi-factor authentication (MFA) settings *in* Default *Domain*

Factors

Select the factors that you want to enable. What are the different MFA factors?

□ Security questions
Configure security questions.

□ Email
Configure email settings.

□ Bypass code

□ DUO security
Configure DUO security.

☑ Fast ID Online (FIDO) authenticator
Configure FIDO authenticator.

Mobile
Configure mobile app passcode.

☑ Mobile app passcode

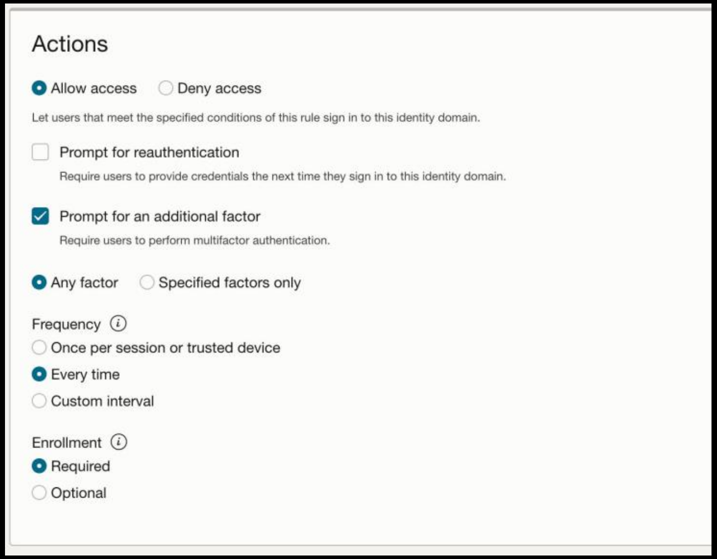
☑ Mobile app notification

Phone number
Configure phone number.

■ Text message (SMS)

□ Phone call

Creating a Sign-On Policy to activate MFA



Actions

● Allow access ○ Deny access

Let users that meet the specified conditions of this rule sign in to this identity domain.

□ Prompt for reauthentication
Require users to provide credentials the next time they sign in to this identity domain.

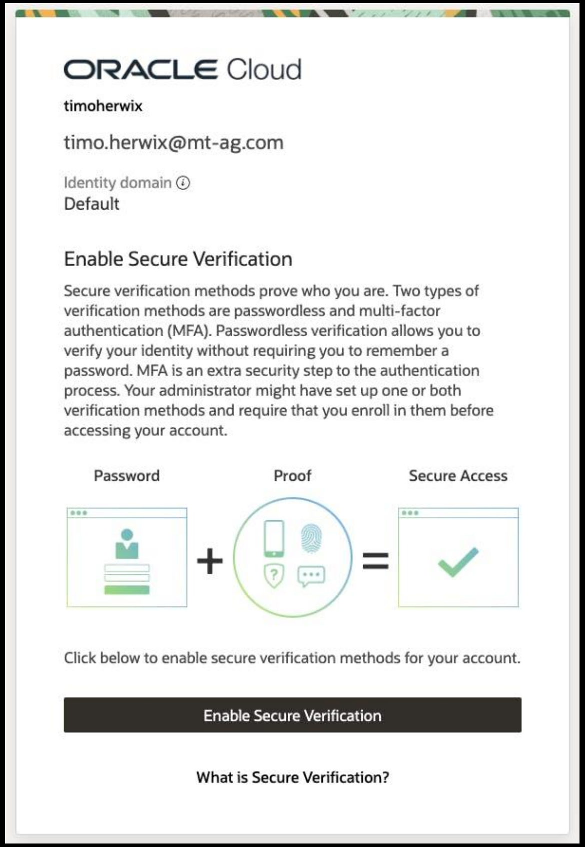
☑ Prompt for an additional factor
Require users to perform multifactor authentication.

● Any factor ○ Specified factors only

Frequency ⓘ
○ Once per session or trusted device
● Every time
○ Custom interval

Enrollment ⓘ
● Required
○ Optional

Multi-Factor Authentication!



ORACLE Cloud

timoherwix

timo.herwix@mt-ag.com

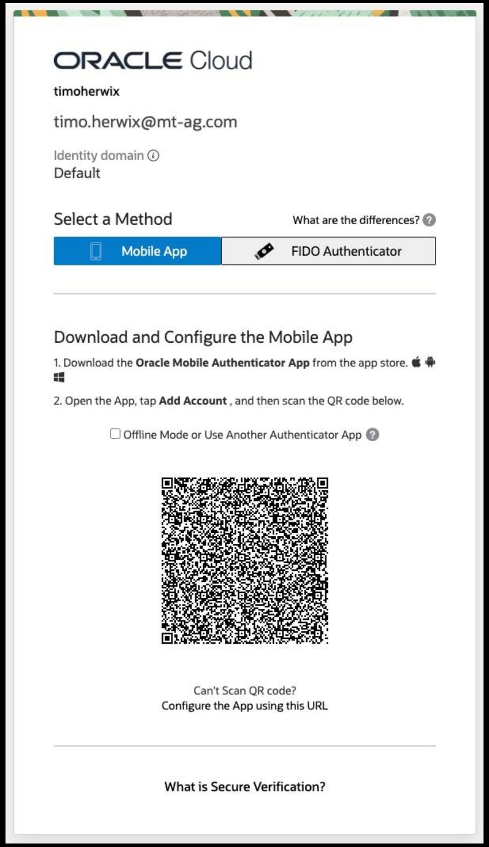
Identity domain ⓘ
Default

Enable Secure Verification

Secure verification methods prove who you are. Two types of verification methods are passwordless and multi-factor authentication (MFA). Passwordless verification allows you to verify your identity without requiring you to remember a password. MFA is an extra security step to the authentication process. Your administrator might have set up one or both verification methods and require that you enroll in them before accessing your account.

Click below to enable secure verification methods for your account.

What is Secure Verification?



ORACLE Cloud

timoherwix

timo.herwix@mt-ag.com

Identity domain ⓘ
Default

Select a Method

Download and Configure the Mobile App

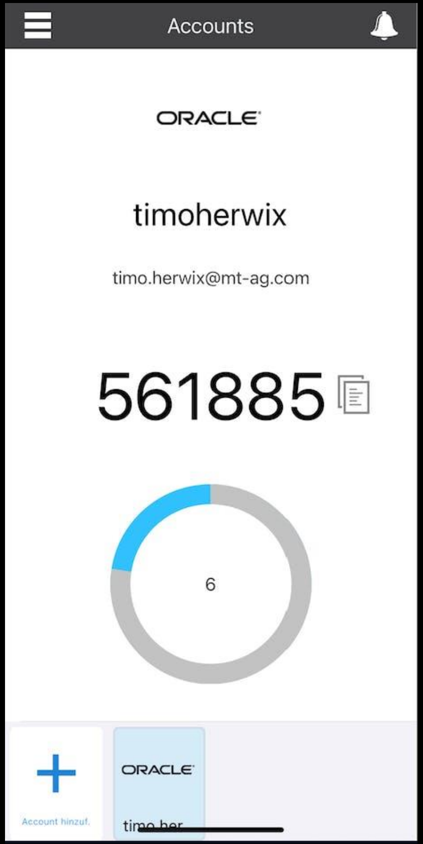
1. Download the **Oracle Mobile Authenticator App** from the app store.

2. Open the App, tap **Add Account** , and then scan the QR code below.

☐ Offline Mode or Use Another Authenticator App

Can't Scan QR code?
Configure the App using this URL

What is Secure Verification?



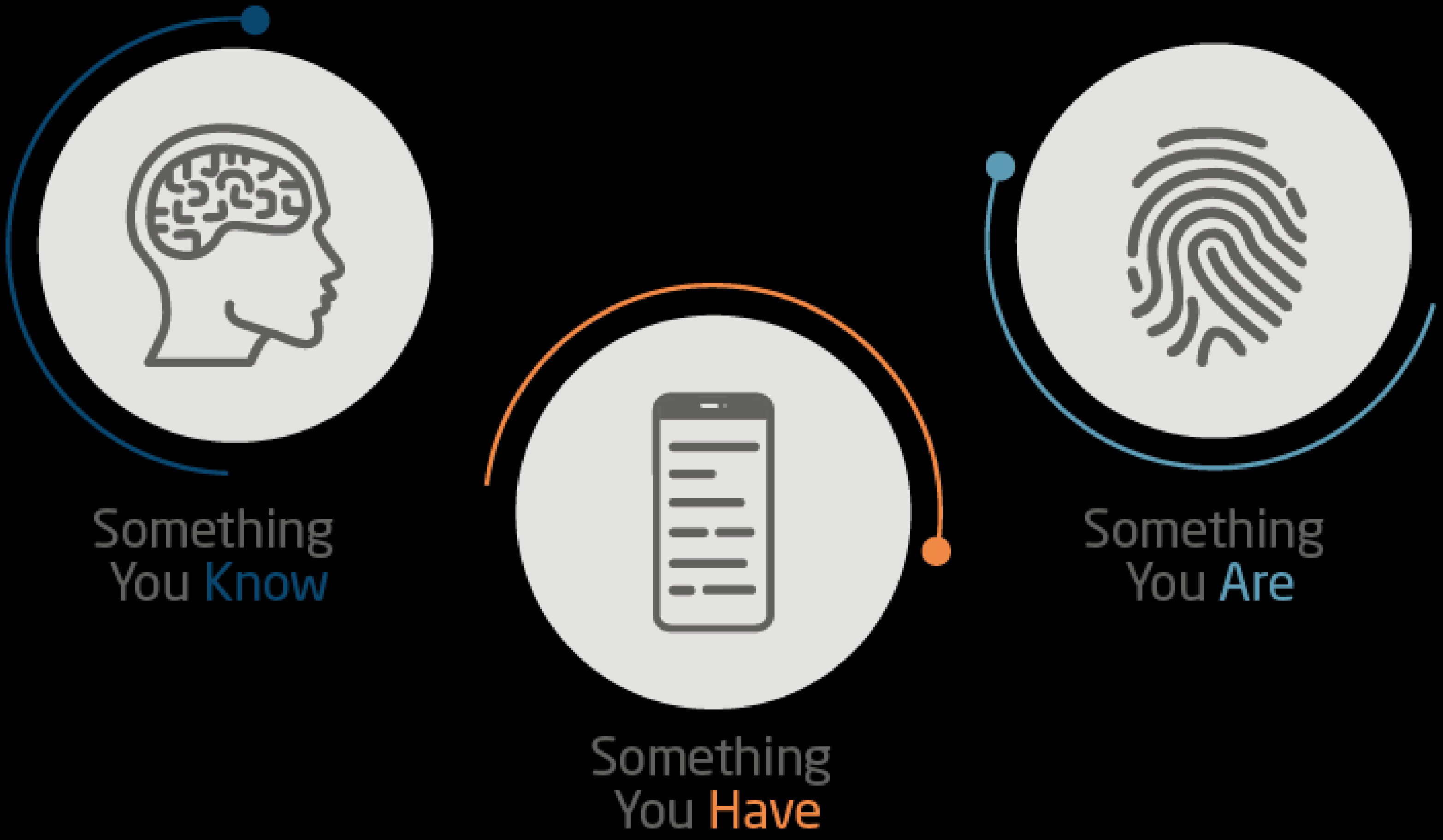
timoherwix

timo.herwix@mt-ag.com

561885

Passwordless Authentication!

Passwordless Authentication!

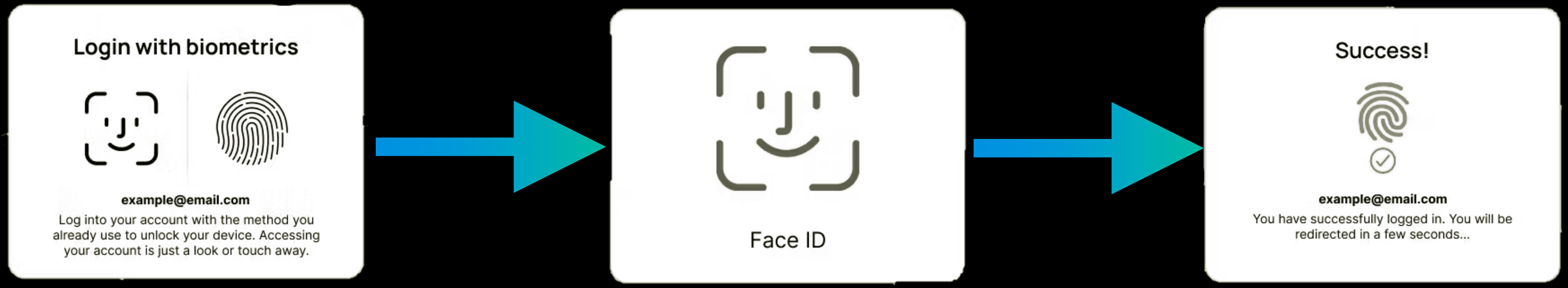


Something You Know

Something You Have

Something You Are

Passwordless Authentication!



Login with biometrics

example@email.com

Log into your account with the method you already use to unlock your device. Accessing your account is just a look or touch away.

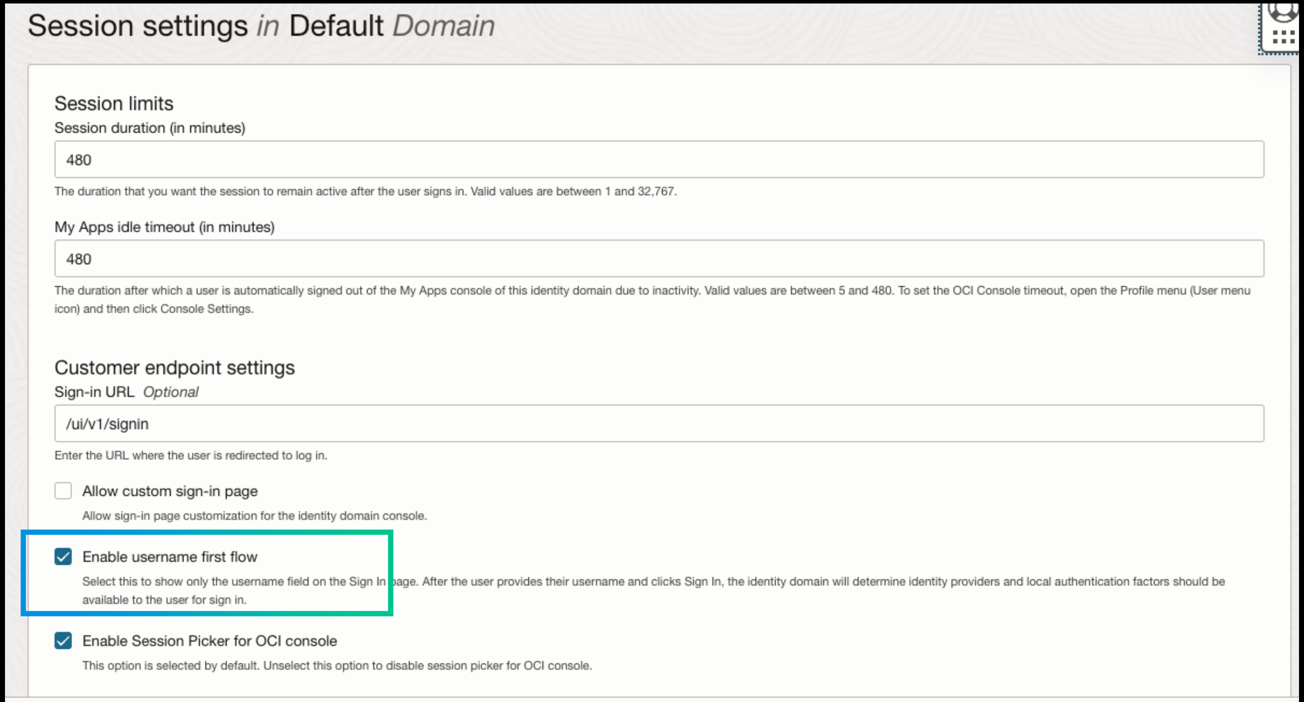
Face ID

Success!

example@email.com

You have successfully logged in. You will be redirected in a few seconds...

Setting up Username only Sign-In!



Session settings *in* Default *Domain*

Session limits

Session duration (in minutes)

480

The duration that you want the session to remain active after the user signs in. Valid values are between 1 and 32,767.

My Apps idle timeout (in minutes)

480

The duration after which a user is automatically signed out of the My Apps console of this identity domain due to inactivity. Valid values are between 5 and 480. To set the OCI Console timeout, open the Profile menu (User menu icon) and then click Console Settings.

Customer endpoint settings

Sign-in URL *Optional*

/ui/v1/signin

Enter the URL where the user is redirected to log in.

☐ Allow custom sign-in page

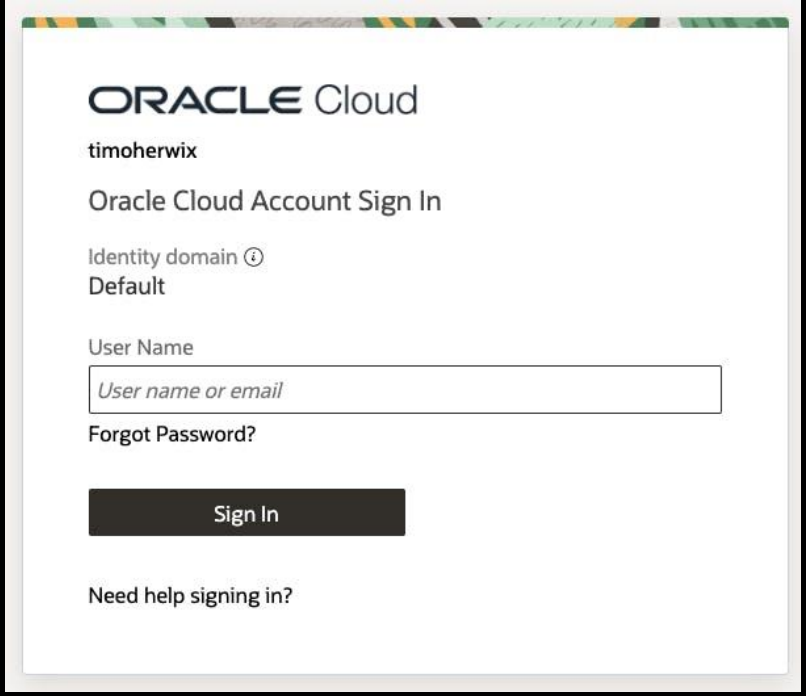
Allow sign-in page customization for the identity domain console.

☑ Enable username first flow

Select this to show only the username field on the Sign In page. After the user provides their username and clicks Sign In, the identity domain will determine identity providers and local authentication factors should be available to the user for sign in.

☑ Enable Session Picker for OCI console

This option is selected by default. Unselect this option to disable session picker for OCI console.



ORACLE Cloud

timoherwix

Oracle Cloud Account Sign In

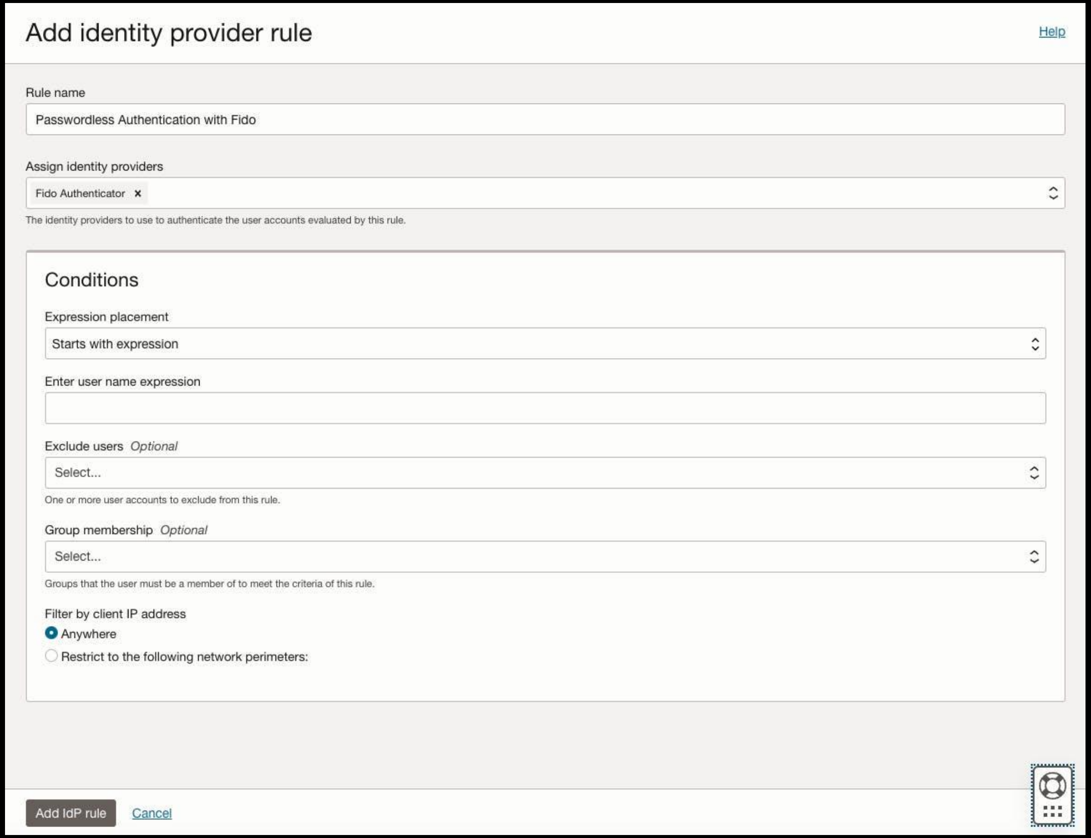
Identity domain ⓘ

Default

User Name

User name or email

Setting up the Identity Provider Policy!



Add identity provider rule

Rule name: Passwordless Authentication with Fido

Assign identity providers: Fido Authenticator ×

The identity providers to use to authenticate the user accounts evaluated by this rule.

Conditions

Expression placement: Starts with expression

Enter user name expression:

Exclude users *Optional*: Select...

One or more user accounts to exclude from this rule.

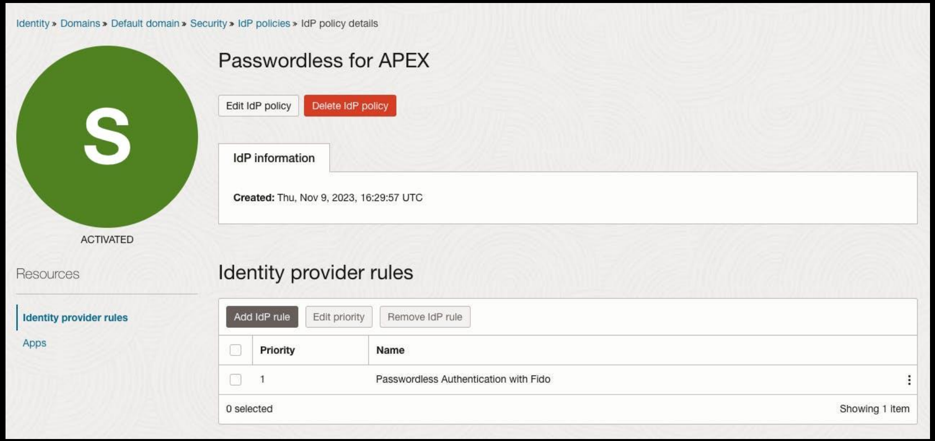
Group membership *Optional*: Select...

Groups that the user must be a member of to meet the criteria of this rule.

Filter by client IP address

● Anywhere

○ Restrict to the following network perimeters:



Identity » Domains » Default domain » Security » IdP policies » IdP policy details

Passwordless for APEX

Created: Thu, Nov 9, 2023, 16:29:57 UTC

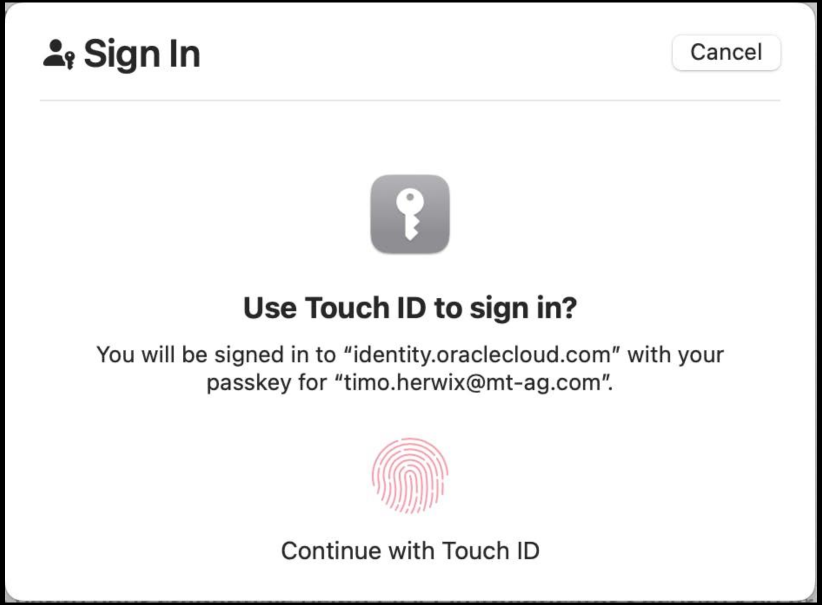
Identity provider rules

□	Priority	Name
□	1	Passwordless Authentication with Fido

0 selected — Showing 1 item

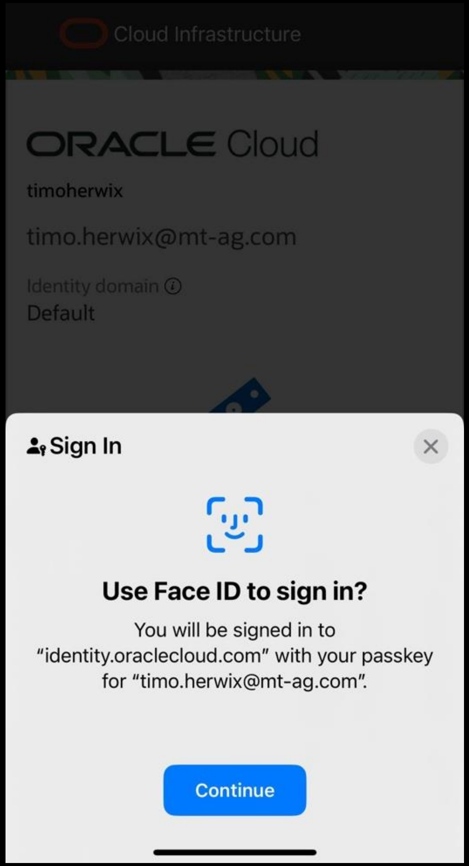
Hyand

Passwordless Authentication!



Use Touch ID to sign in?

You will be signed in to "identity.oraclecloud.com" with your passkey for "timo.herwix@mt-ag.com".



timoherwix

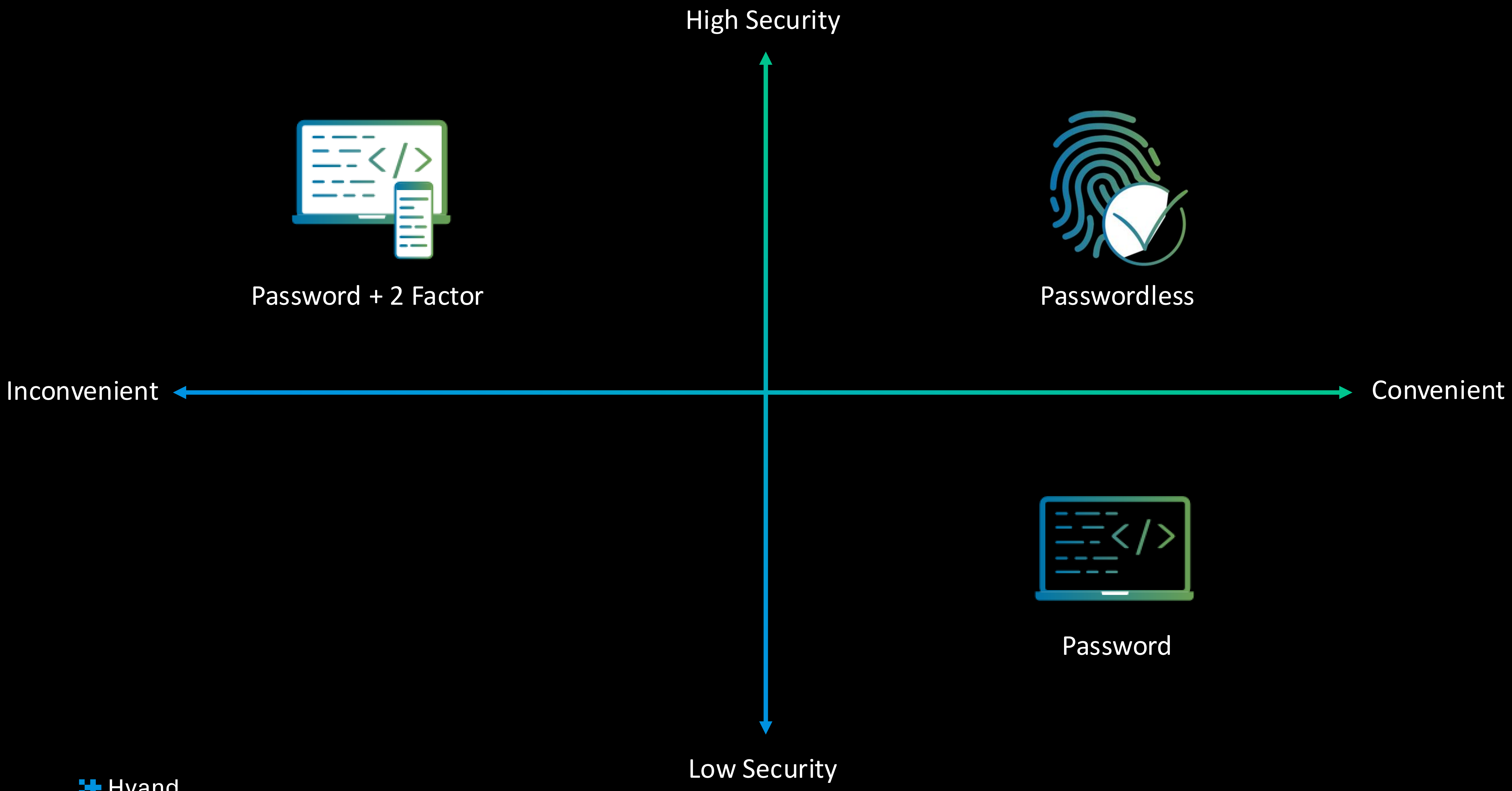
timo.herwix@mt-ag.com

Identity domain: Default

Use Face ID to sign in?

You will be signed in to "identity.oraclecloud.com" with your passkey for "timo.herwix@mt-ag.com".

Conclusion!



High Security

Password + 2 Factor

Passwordless

Inconvenient

Convenient

Password

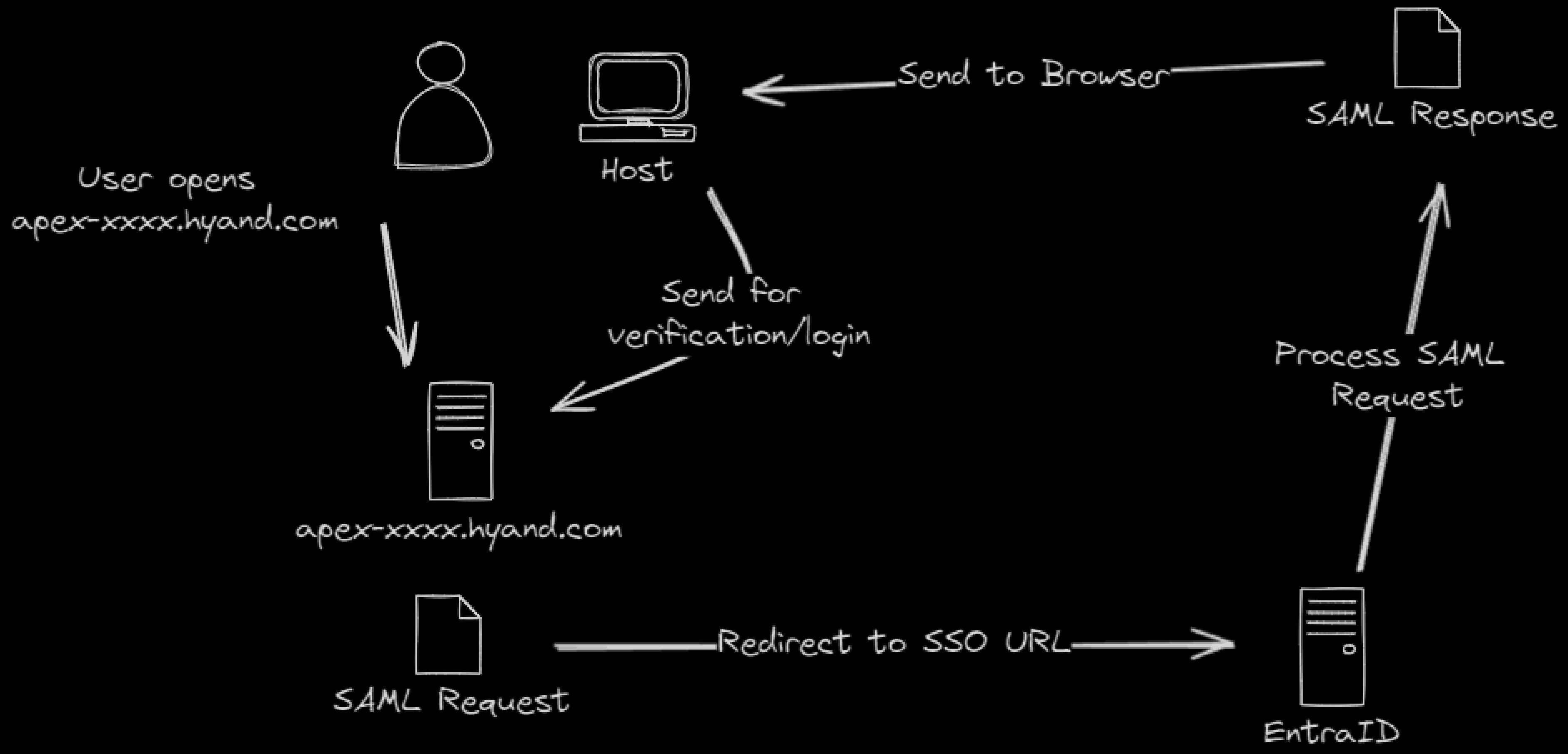
Low Security

RIP passwords - the future is passwordless!

Single Sign-On between OCI and Azure!

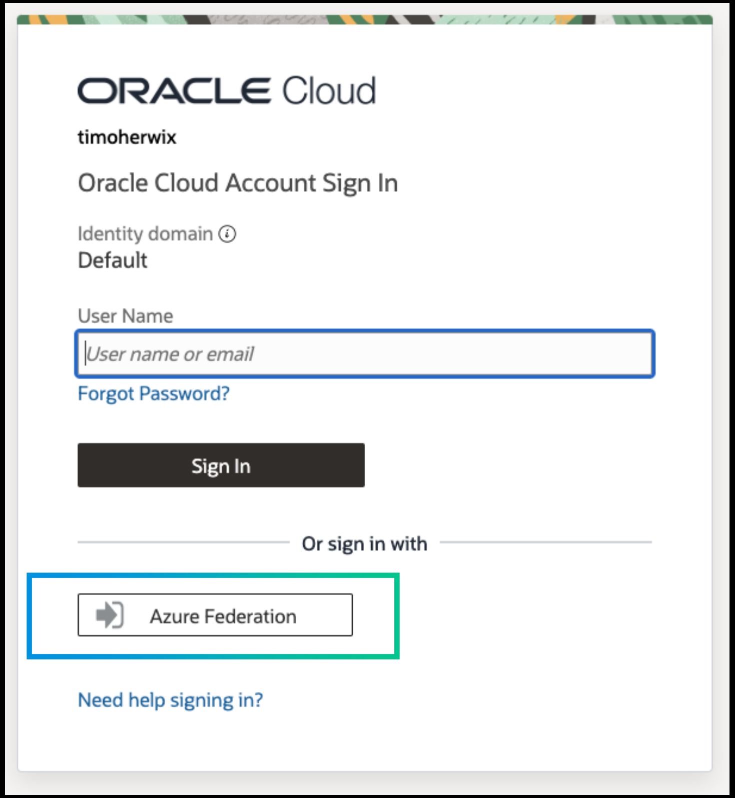
By setting up a federation between Azure and OCI IAM, you allow users to access services and applications in OCI using their Entra-ID Credentials.

SAML Authentication Flow



Hyand

Single Sign-On between OCI and Azure!



ORACLE Cloud

timoherwix

Oracle Cloud Account Sign In

Identity domain ⓘ
Default

User Name
User name or email

Forgot Password?

Sign In

Or sign in with

Azure Federation

Need help signing in?

To make this work, the user you're using for Single Sign-On needs to be in both OCI IAM and Entra-ID!

From now on, both identity access managers can be used. In this case OCI and Azure.

1

Introduction

2

Let´s dive deeper

3

Wrap-up

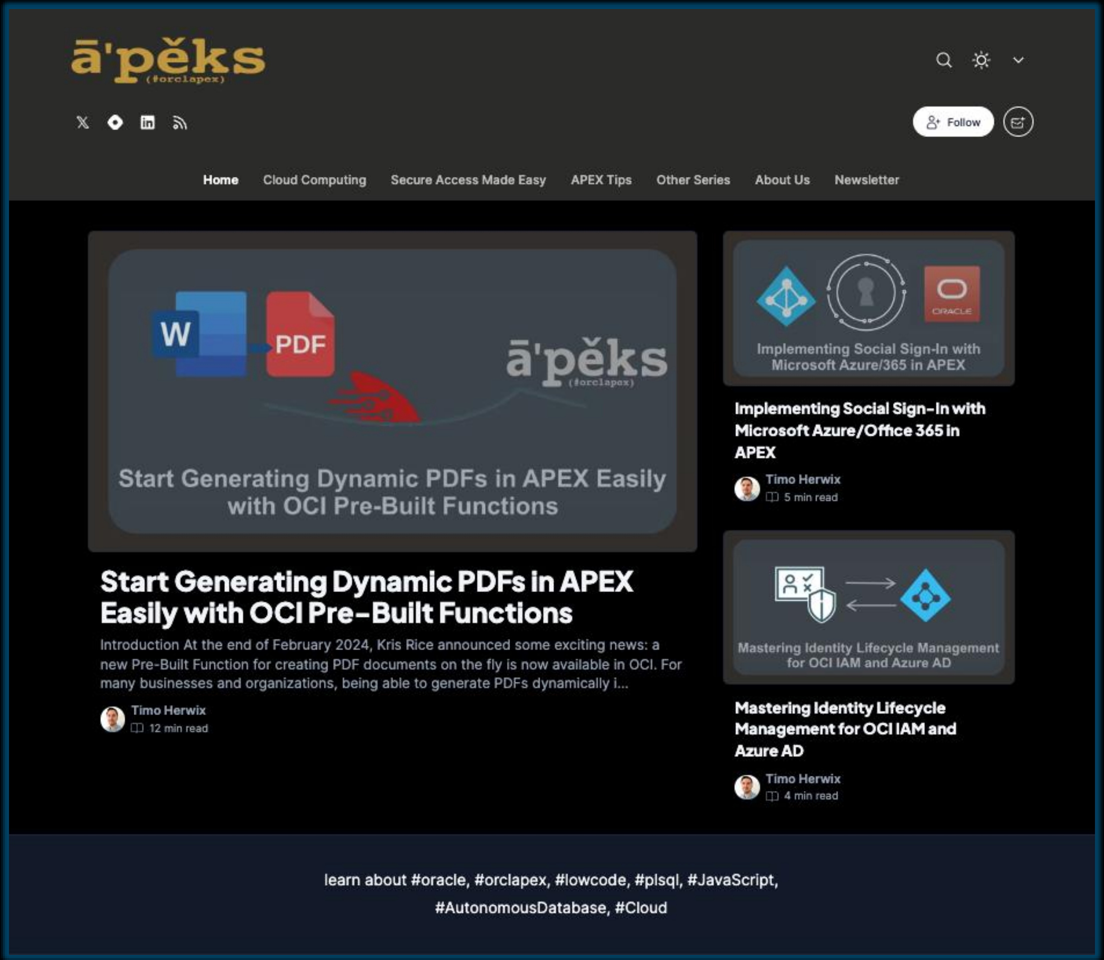
Top five.

- Super easy to set up
- Makes things smoother for users (like with Single Sign-On)
- Boosts security (think MFA)
- Helps everyone get more done
- Opens the door to sign in without a password

5

Blog

Scan me!



ā'pěks
(#orclapex)
Follow

Home · Cloud Computing · Secure Access Made Easy · APEX Tips · Other Series · About Us · Newsletter

Start Generating Dynamic PDFs in APEX Easily with OCI Pre-Built Functions

Introduction At the end of February 2024, Kris Rice announced some exciting news: a new Pre-Built Function for creating PDF documents on the fly is now available in OCI. For many businesses and organizations, being able to generate PDFs dynamically i...

Timo Herwix
12 min read

Implementing Social Sign-In with Microsoft Azure/365 in APEX

Implementing Social Sign-In with Microsoft Azure/Office 365 in APEX

Timo Herwix
5 min read

Mastering Identity Lifecycle Management for OCI IAM and Azure AD

Timo Herwix
4 min read

learn about #oracle, #orclapex, #lowcode, #plsql, #JavaScript, #AutonomousDatabase, #Cloud

Are you interested?

Timo Herwix
Senior Consultant

Telefon: +49 2102 30 961-0
Mobil: +49 176 20185455
Mail: timo.herwix@hyand.com

Timo Herwix

@Therwix

tm-apex.hashnode.dev