
Authentification d'entreprise avec OPENID CONNECT

Description

Question : Comment je peux authentifier les utilisateurs de la plateforme Diver avec mon fournisseur d'identité corporate (IdP) ?

Par exemple :

Microsoft Entra ID (Azure Active Directory)

Google Workplace

Ping Identity

Auth0

Okta

Keycloak

... toute IdP implémentant OpenID Connect (basé sur OAuth 2.0)

La réponse est la suivante :

Utilisation du protocole OpenID Connect (OIDC)

Question : Pourquoi devrais-je authentifier les utilisateurs Diver Platform avec mon fournisseur d'identité corporate (IdP) ?

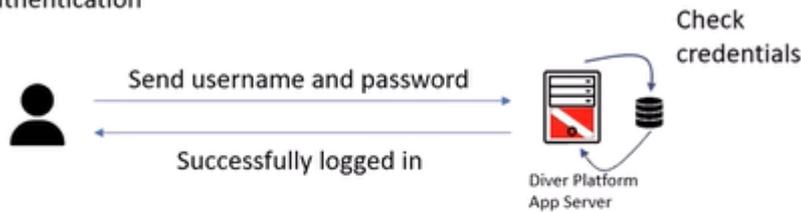
Réponse : Améliorer la sécurité et l'expérience utilisateur.

Les bénéfices du connecteur OpenID :

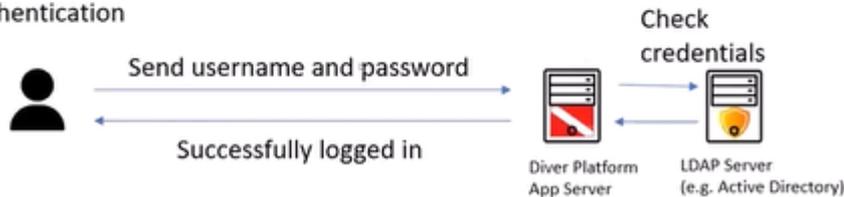
- Gestion de l'utilisateur centralisée
 - De plus en plus populaire car les compagnies recherchent des Active Directory sur site
- Les clients définissent des politiques dans toute l'organisation
 - Complexité des mots de passe
 - Authentification multi-facteurs
- SSO possible
 - IdP peut être configuré pour partager des sessions de cookies et rafraichir des tokens

Flux de connexion classiques - expérience utilisateur :

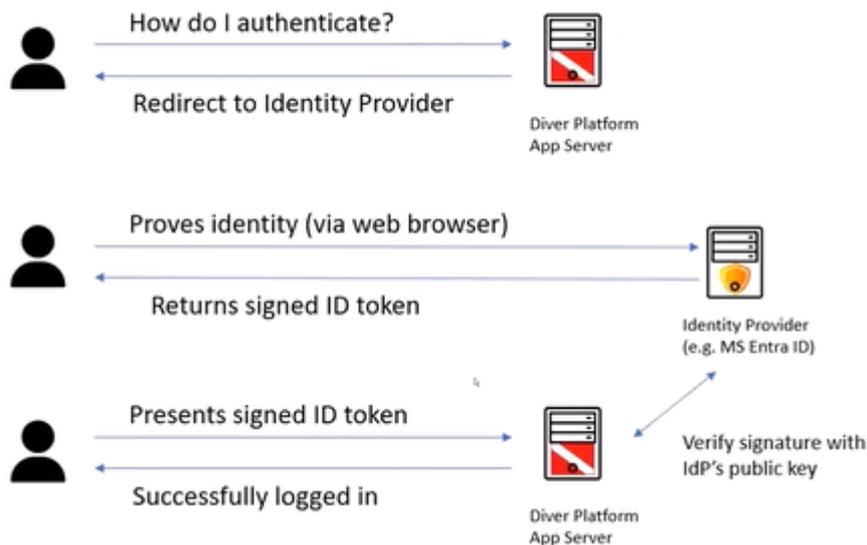
"Own" Authentication



LDAP Authentication



Flux de connexion OpenID - expérience utilisateur :



Les étapes de configuration

Sur le fournisseur d'identité :

- déclarer une nouvelle application
- spécifier les URLs de redirection

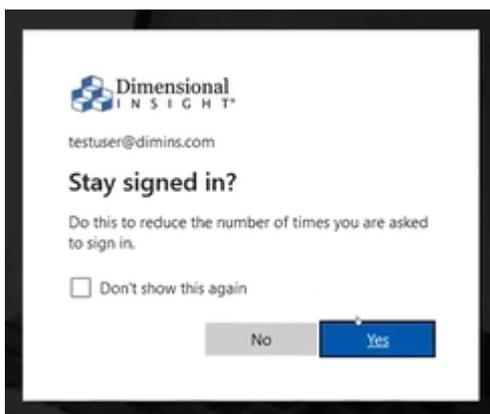
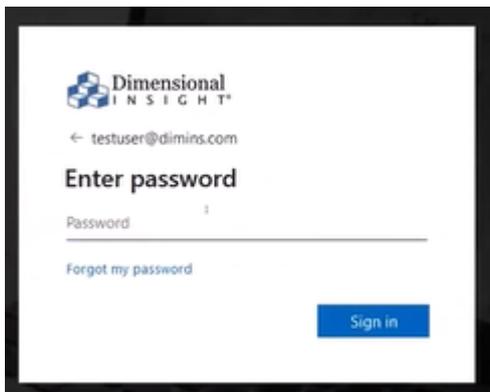
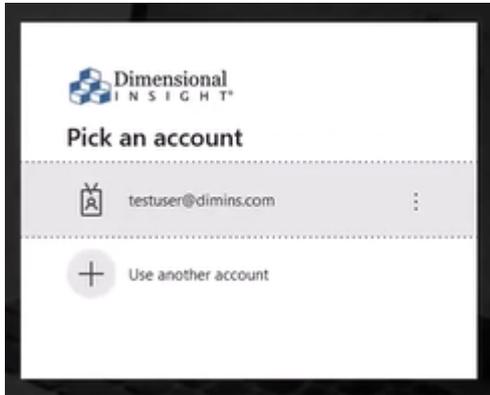
Dans Workbench :

1. ajouter un nouveau fournisseur OIDC
2. spécifier l'URL de l'émetteur et l'ID client lors de l'enregistrement
3. définir un schéma d'authentification globalement ou pour certains utilisateurs

Mixer les connexions OpenID avec les autres schémas d'authentification

- certains utilisateurs utilisent OIDC, les autres utilisent OWN/LDAP/System
 - et/ou plusieurs fournisseurs d'identité OIDC
- approches
 - diriger tous les utilisateurs vers OIDC IdP sauf si l'invite du nom d'utilisateur est forcée
 - ajouter ou se connecter à des URL ou à un nom de serveur
 - demander le nom de l'utilisateur, ensuite envoyer à l'IdP ou demander un mot de passe

Exemple de capture d'écran DivePort :



Vous trouverez plus d'informations sur le lien suivant :

<https://dimins.com/help/oidc>

Tags

1. Workbench