



MidPoint Integrations: Partner Series

Keycloak as an Access Layer

Ján Marcin

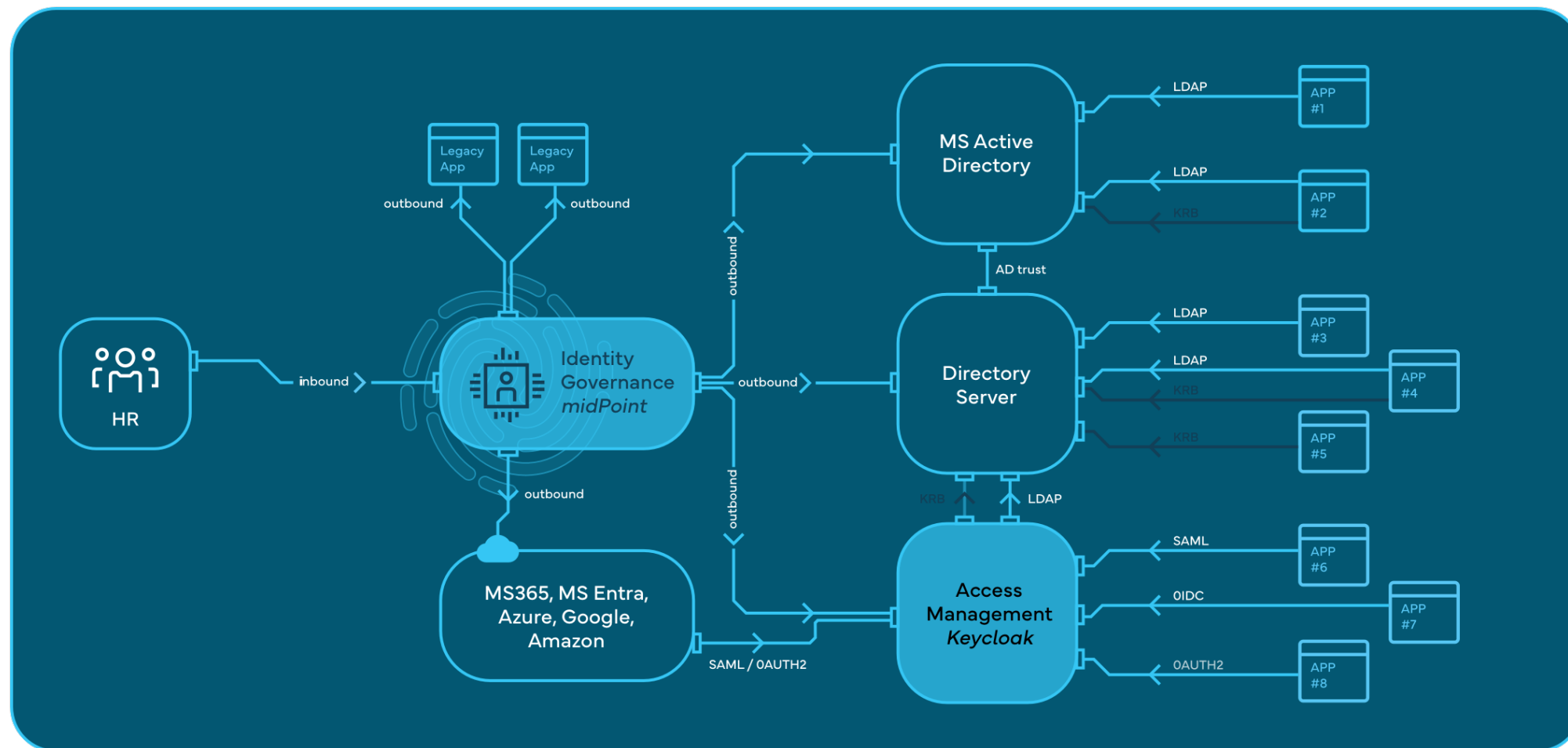
COO at Inalogy a.s.

IAM, IDM, IGA, AM

- IDM - Identity Management is focusing on identity lifecycle management and data orchestration.
 - Identity lifecycle management
 - Password management
 - Management policies
 - Requesting access
 - Data synchronization
- IGA - Identity Governance and Administration expands on IDM by adding governance and compliance features.
 - Identity analysis
 - Recertification
 - Role governance
 - Segregation of duties
 - Audit and Compliance
- AM - Access Management specifically about controlling access, rather than managing identities.
 - Central authentication
 - Single Sign-On (SSO)
 - Clients and services management
 - Multifactor authentication (MFA)
 - Identity federation
- IAM - Identity and Access Management is an overarching concept that includes aspects of all the others.
 - IDM
 - IGA
 - AM



Inalogy IAM concept



Why there is a need for access layer

- To isolate the authentication layer
- Advanced safety mechanism
 - Brute force prevention
 - MFA
- Single Sign-On
- Delegated authentication
- Multiple options on the market
 - Keycloak
 - Microsoft Entra
 - Okta
 - CAS
 - Etc...

Why Keycloak

- Open-Source backed by [CNCF](#)
- Highly customizable UI
 - Themes
 - Localizations
- Supports customization of flows, processes, and screens via extension modules without impacting core code
- All standardized protocols
 - OAuth, OpenID Connect, SAML2.0
- Identity brokering via 3rd party IDPs
 - Microsoft, Google, Apple...
 - Custom IDPs supporting standard protocols
- MFA
 - OTP
 - Webauth
 - Certificates
 - Physical keys (Yubikey)
 - Passkeys
 - Push-notifications*

Mitigating security threats

- Defense mechanisms
 - Brute force detection
 - Lockout permanently
 - Lockout Temporarily
 - Lockout permanently after temporary lockout
 - Security Headers

The image shows two screenshots of a web application's configuration interface, specifically the 'Security defenses' section.

The top screenshot displays the 'Brute force detection' settings. The 'Brute Force Mode' is set to 'Lockout permanently after temporary lockout'. Other settings include 'Max login failures' (30), 'Maximum temporary lockouts' (1), 'Wait increment' (1 Minutes), 'Max wait' (15 Minutes), 'Failure reset time' (12 Hours), 'Quick login check milliseconds' (1000), and 'Minimum quick login wait' (1 Minutes).

The bottom screenshot displays the 'Security Headers' settings. The 'X-Frame-Options' is set to 'SAMEORIGIN'. The 'Content-Security-Policy' is set to 'frame-src 'self'; frame-ancestors 'self'; object-src 'none';'. The 'Content-Security-Policy-Report-Only' is empty. The 'X-Content-Type-Options' is set to 'nosniff'. The 'X-Robots-Tag' is set to 'none'. The 'X-XSS-Protection' is set to '1; mode=block'. The 'HTTP Strict Transport Security (HSTS)' is set to 'max-age=31536000; includeSubDomains'. The 'Referrer Policy' is set to 'no-referrer'.

midPoint OIDC configuration

Keycloak side

- Create midPoint client in Keycloak
 - General settings
 - Capability configuration
 - Login settings
- Secret is generated after client creation
- [Documentation link](#)

Create client

Clients are applications and services that can request authentication of a user.

1 General settings

2 Capability config

3 Login settings

Client type ⓘ

OpenID Connect

Client ID * ⓘ

midpoint

Name ⓘ

midpoint

Description ⓘ

This is OIDC client for midPoint

Always display in UI ⓘ

Off

Create client

Clients are applications and services that can request authentication of a user.

1 General settings

2 Capability config

3 Login settings

Client authentication ⓘ

On

Authorization ⓘ

Off

Authentication flow

☒ Standard flow ⓘ

☒ Direct access grants ⓘ

☐ Implicit flow ⓘ

☐ Service accounts roles ⓘ

☐ OAuth 2.0 Device Authorization Grant ⓘ

☐ OIDC CIBA Grant ⓘ

Create client

Clients are applications and services that can request authentication of a user.

1 General settings

2 Capability config

3 Login settings

Root URL ⓘ

https://demo.inalogy.com/midpoint

Home URL ⓘ

https://demo.inalogy.com/midpoint

Valid redirect URIs ⓘ

https://demo.inalogy.com/midpoint/*

+ Add valid redirect URIs

Valid post logout redirect URIs ⓘ

+ Add valid post logout redirect URIs

Web origins ⓘ

+ Add web origins

midPoint OIDC configuration

midPoint side

- Security policy
- Flexible authentication
- OIDC module
- Authentication via ClientID and Secret
- [Documentation link](#)

- ❶ To allow logging in for users that have no accounts in Keycloak (e.g., default midPoint administrator). Not strictly necessary.
- ❷ OpenID Connect login for ordinary users.
- ❸ Technical information that may be basically anything legal for inclusion into URI.
- ❹ ID of the client as registered in Keycloak.
- ❺ Secret of the client as generated by Keycloak (or provided manually).
- ❻ URL at which Keycloak runs.

```
<securityPolicy>
  <authentication>
    <modules>
      ...
      <loginForm> ❶
        <identifier>loginForm</identifier>
      </loginForm>
      ...
      <oidc> ❷
        <identifier>gui-oidc</identifier>
        <client>
          <registrationId>oidc-registration</registrationId> ❸
          <clientId>midpoint</clientId> ❹
          <clientSecret>
            <t:clearValue>RwdBxRh0ggkDCr321SzyGwkEVvRHd7g1</t:clearValue> ❺
          </clientSecret>
          <clientAuthenticationMethod>clientSecretBasic</clientAuthenticationMethod>
          <nameOfUsernameAttribute>preferred_username</nameOfUsernameAttribute>
          <openIdProvider>
            <issuerUri>http://192.168.4.100:8080/realms/master</issuerUri> ❻
          </openIdProvider>
        </client>
      </oidc>
      ...
    </modules>
    ...
    <sequence> ❷
      <identifier>gui-oidc</identifier>
      <channel>
        <channelId>http://midpoint.evolveum.com/xml/ns/public/common/channels-3#user</channelId>
        <default>true</default>
        <urlSuffix>gui-oidc</urlSuffix>
      </channel>
      <module>
        <identifier>gui-oidc</identifier>
      </module>
    </sequence>
    ...
    <sequence> ❶
      <identifier>gui-login-form</identifier>
      <channel>
        <channelId>http://midpoint.evolveum.com/xml/ns/public/common/channels-3#user</channelId>
        <urlSuffix>gui-login-form</urlSuffix>
      </channel>
      <module>
        <identifier>loginForm</identifier>
      </module>
    </sequence>
    ...
  </authentication>
</securityPolicy>
```


MidPoint Keycloak integration

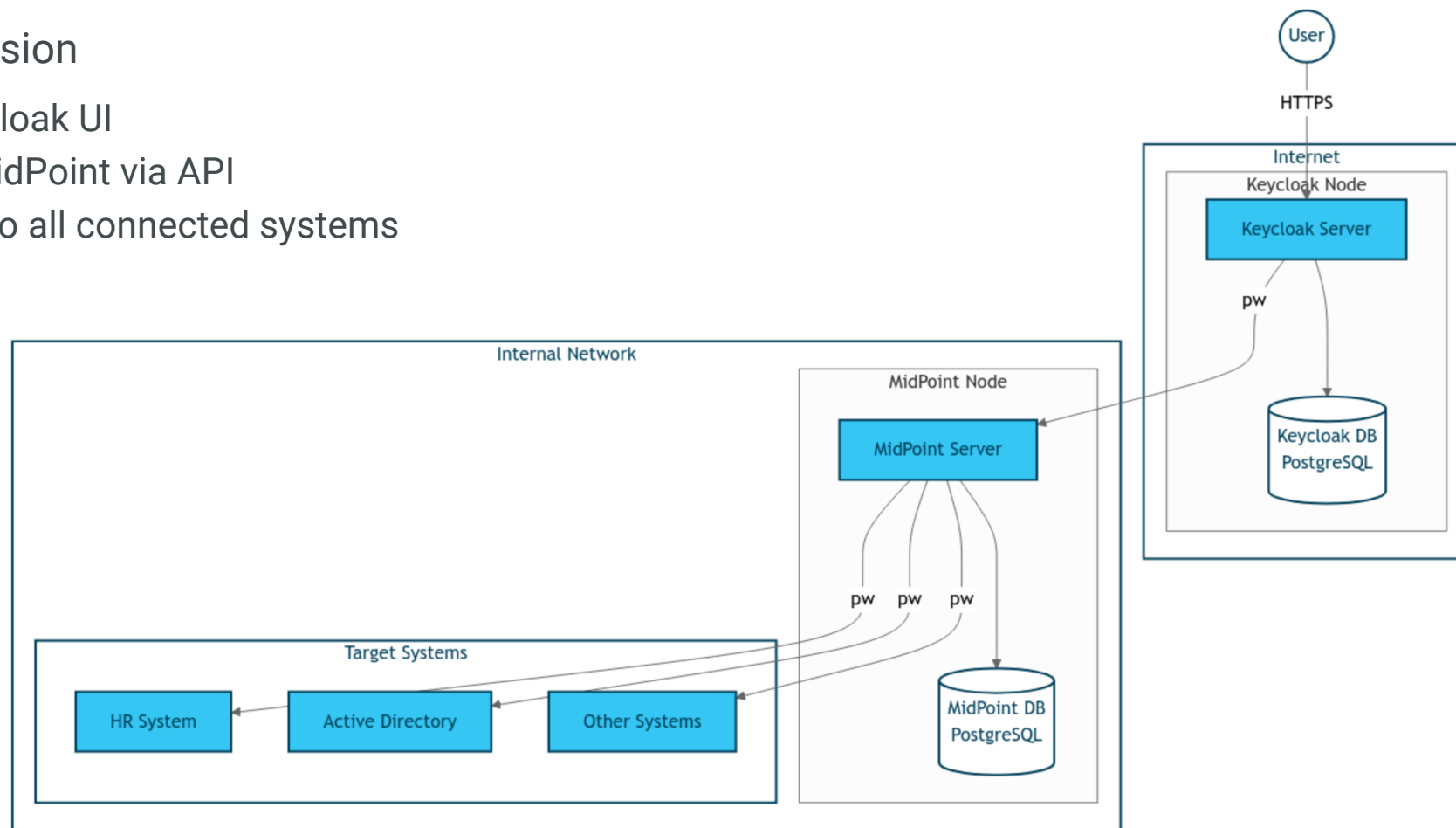
Outbound

- Keycloak connector by NRI
 - <https://docs.evolveum.com/connectors/connectors/jp.openstandia.connector.keycloak.KeycloakConnector/>
 - Assigning KC roles directly
- Native LDAP federation
 - Assigning KC roles via LDAP groups
- 3rd Party Identity providers like EntraID
 - Assigning KC roles via AD groups

MidPoint Keycloak integration

Inbound

- Password provisioning extension
 - Manage password via Keycloak UI
 - Send a new password to midPoint via API
 - Distribute new passwords to all connected systems
- Use cases
 - Password change
 - Forgotten password
 - Account recovery



Keycloak customization

- Authentication flows
 - Login
 - Register
 - Password reset
- Themes
 - Templates (Apache FreeMarker)
 - Custom CSS
 - Custom e-mail templates
- Extensions

LOGIN

Welcome back, Scout! Login to your scout.org account below.



[FORGOT PASSWORD?](#)

[NOT A MEMBER YET?](#)

[REGISTER](#)

LOGIN

Or use social login

 Apple

 Google

 Microsoft

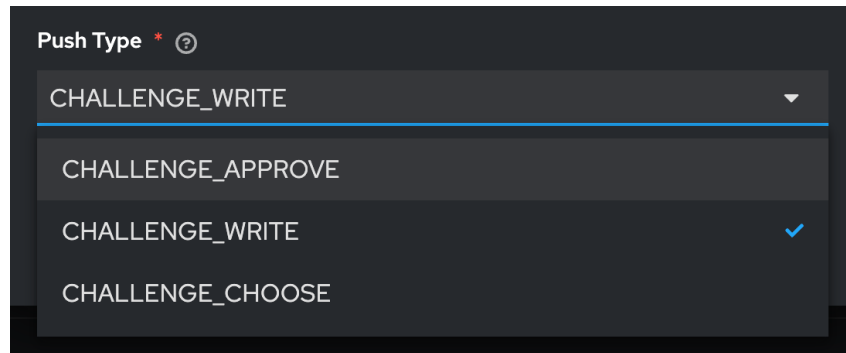
 Facebook

WHY LOGIN?

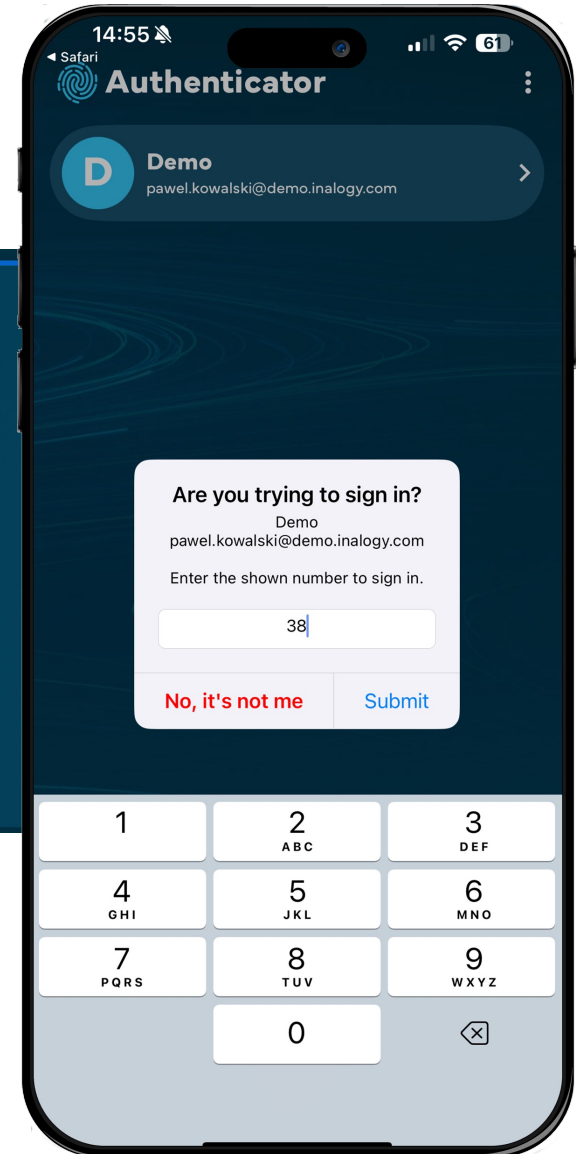
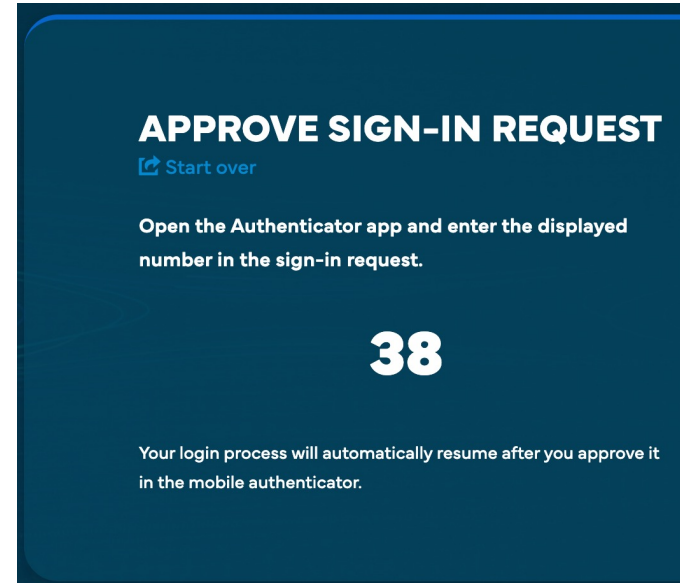
Logging in to your scout.org account allows you to access all of your World Scouting platforms.

Push Notifications for on-prem AM

- Push notifications for on-prem AM
- Multiple security options

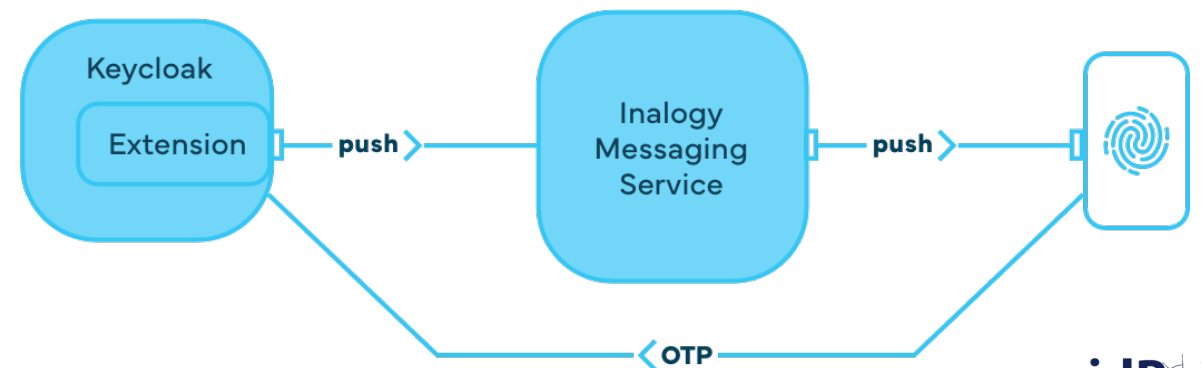
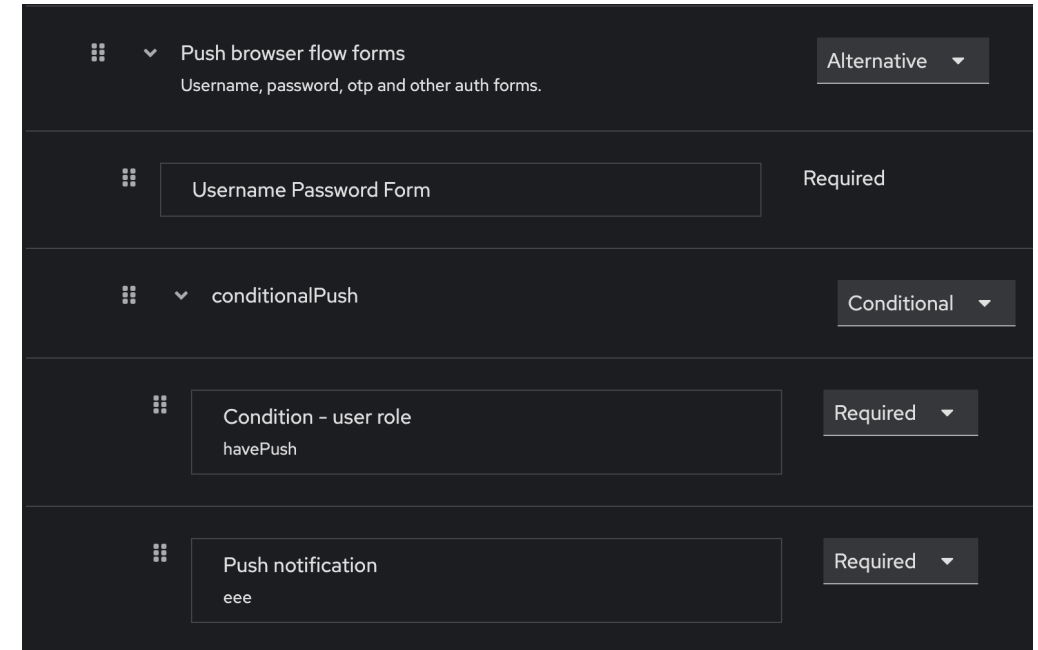


- Inalogy Authenticator available for free



Under the hood

- Keycloak extension
 - Configurable directly in Keycloak auth flow wizard
- IMS
 - Cloud messaging service providing a bridge between Keycloak instances and Mobile Authenticators
 - Communicates with Keycloak non-admin API
- Inalogy authenticator
 - Native iOS application
 - Native Android application



Demo

- demo.inalogy.com
 - Password change
 - Role driven MFA
 - MFA via push notification



Thank you for your attention

Inalogy Authenticator



midPoint

MidPoint Integrations: Partner Series
2024