Alfresco TTL #141

HANDOUT

Alfresco™ | Now a part of Hyland

Hyland | DevCon

International technical event
for developers, architects
and DevOps teams

Meliá Costa del Sol, Málaga
(Torremolinos), Spain
January 24–26, 2023

Hyland | DevCon

The conference program will be available soon:

- Connect with Hyland experts and leadership
- Hackathon
- Technical training
- Deep-dive presentations
- Lightning Tech Talks
- Q&A panels
- Registration now open!

Call for Paper is open

- Don't wait to submit talks
- Open to Alfresco and Nuxeo
- Deadline November 15

Hyland™ | DevCon

All information:

https://web.cvent.com/event/c03ce216-9281-4a36-9c57-fb896e67abc1/

Call for Paper:

https://survey.alchemer.com/s3/6839578/Hyland-DevCon-2023-Call-for-Speakers

ACS 7.3 GENERAL AVAILABILITY

- Release scheduled **November 14th**

- Highlights

  - First version built with **Java 17** (despite *Java 11* is still supported)

  - First version supporting **Angular 14** for ADF

  - New REST API endpoints related to *Actions*

  - 20+ Bugs fixed

  - 2 Security patches

  - (Enterprise) Support for Elasticsearch **and** OpenSearch

  - (Enterprise) Activiti Web Console has been removed

- Stay tuned at Alfresco Hub and Alfresco website for release note and download

Service	Version
Alfresco Content Services	7.3.0
Alfresco Share	7.3.0
Alfresco Transform	2.6.0
Alfresco Office Services	1.5.0
Alfresco Content Application	3.1.0
Alfresco Search Services	2.0.5
ActiveMQ	5.17.1
Postgres	14.4
Maven SDK	4.5
Java SDK	5.2

LET'S TALK ABOUT SOFTWARE UPGRADES

- Please take this 1-2 minute survey to help us understand and improve the software upgrade experience all together at Hyland.

- See also on the Hub

https://survey3.medallia.com/?51fMJi-LTAUpgrades

RESOURCES FROM THE COMMUNITY

From the Hub

- How many PATHs remain to be indexed?
  https://hub.alfresco.com/t5/alfresco-content-services-blog/how-many-paths-remain-to-be-indexed/ba-p/314158

- Using AWS OpenSearch with Alfresco Search Enterprise 3.1
  https://hub.alfresco.com/t5/alfresco-content-services-blog/using-aws-opensearch-with-alfresco-search-enterprise-3-1/ba-p/313526

- Alfresco Login Issues & How To Solve Them
  https://hub.alfresco.com/t5/alfresco-content-services-blog/alfresco-login-issues-amp-how-to-solve-them/ba-p/313602

- Control indexing in Alfresco with Alfresco Search Services, by *Abhinav Mishra*
  https://hub.alfresco.com/t5/alfresco-content-services-blog/control-indexing-in-alfresco-with-alfresco-search-services/ba-p/314038

TTL SPEAKERS WANTED!

Topics

- Open source projects

- Showcase of your best work

- Tips and tricks

- Discussions on best practices

- Technical talk and demos only!

- About Alfresco & Nuxeo or associated technologies

- And more! Just pitch it to the team

Benefits for Speakers

- Visibility in the ecosystem

- Goodies

- And other advantages

Enterprise Role Maintenance with ACS & APS

- **Brian Long**
  - Process Specialist
  - Inteligr8
  - Former Alfresco Engineer

Agenda

- ACS & AIS Features & Pain Points
- APS & AIS Features & Pain Points
- ACS & AIS with Acosix Modules
- APS & AIS with Inteligr8 Extension
- Demostration

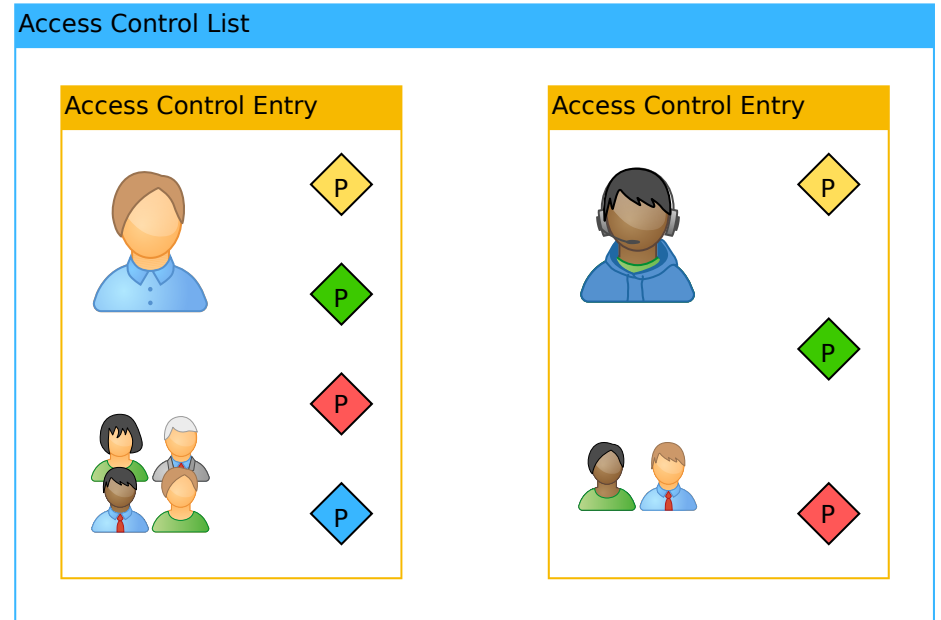# Identity in Alfresco Content Services

ACS Users & User Groups

- Authentication Subsystems
  - Internal Storage: `alfrescoNtlm`
  - LDAP: `ldap/ldap-ad`
  - AIS/Keycloak: `ais`
- Synchronization Subsystem
 - LDAP: `ldap/ldap-ad`

ACS Security

- Users & User Groups
  - Both are "Authority"
- Access Control Entry
  - Authority & Permission
- Access Control List
  - ACEs
- Nodes
  - ACLs
  - Inherited ACLs

ACS with Alfresco Identity Service

- User Authentication
  - Supported
  - ACS Trusts AIS & Validates
    - OAuth Access Token
- User Information
  - Supported
  - ACS Requests User Info
    - Open ID Connect

OAuth

OAuth Token

OIDC User Info

Alfresco
Identity Service

Alfresco
Content Service
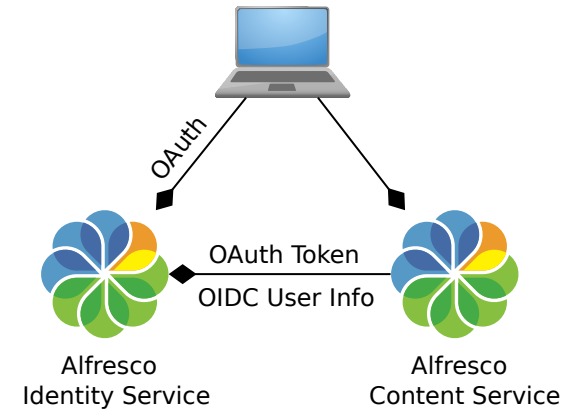
ACS with Alfresco Identity Service

- User Roles
  - Supported by AIS
  - Not Supported by ACS
    - May Use LDAP Synchronization (Lag)
- Share UI
  - Limited Support

Identity in Alfresco Process Services

APS Users & Groups

- Spring Framework Identity Service
  - Internal Storage (default)
  - LDAP
  - AIS/Keycloak
- Synchronization Subsystem
  - LDAP

APS vs Activiti

- Identity Services
  - Open Source Activiti
  - Proprietary APS
- API Confusion
  - If you are using APS, do NOT use Activiti Identity Service API
- APS Group Types
  - Capability
  - Organization

APS with Alfresco Identity Service

- User Authentication
  - Supported
  - APS Trusts AIS & Validates
    - OAuth Access Token
  - APS Rejects Unsynchronized Users

- User Information
  - Supported
  - APS Requests User Info
    - Open ID Connect
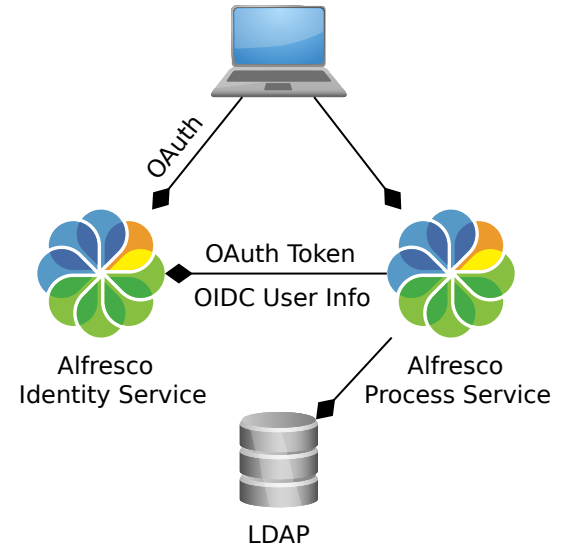
APS with Alfresco Identity Service

- User Roles
  - Supported by AIS
  - Not Supported by APS
    - May Use LDAP Synchronization (Lag)

Alfresco Content Services
w/ Acosix Keycloak Modules

Acosix Keycloak Modules

- Axel Faust
- Project: https://github.com/Acosix/alfresco-keycloak
- Organization: https://acosix.de/
- Platform Module
  - Expands support and configurability for Keycloak (AIS).
- Share Module
  - Better support for Keycloak (AIS).

Acosix Keycloak & Roles for ACS

- Role Recognition Support
  - Immediate: On Authentication
  - Routine: On Token Refresh
- LDAP Not Needed/Used
- Shorter Authorization Security Hole (from lag)

Acosix Keycloak & Roles for ACS

- AIS Roles <=> ACS User Groups
  - ACS User Groups are hierarchical for inheritance
    - Parent for application uses (like folder ACLs)
    - Child for AIS synchronization
  - Sync'd ACS User Groups are created on-demand
    - May be created manually if needed
- Identity/authorization administration for ACS admins:
  - Add/remove sync'd ACS User Groups as subgroups to system or business ACS User Groups

AIS & ACS Role Mappings
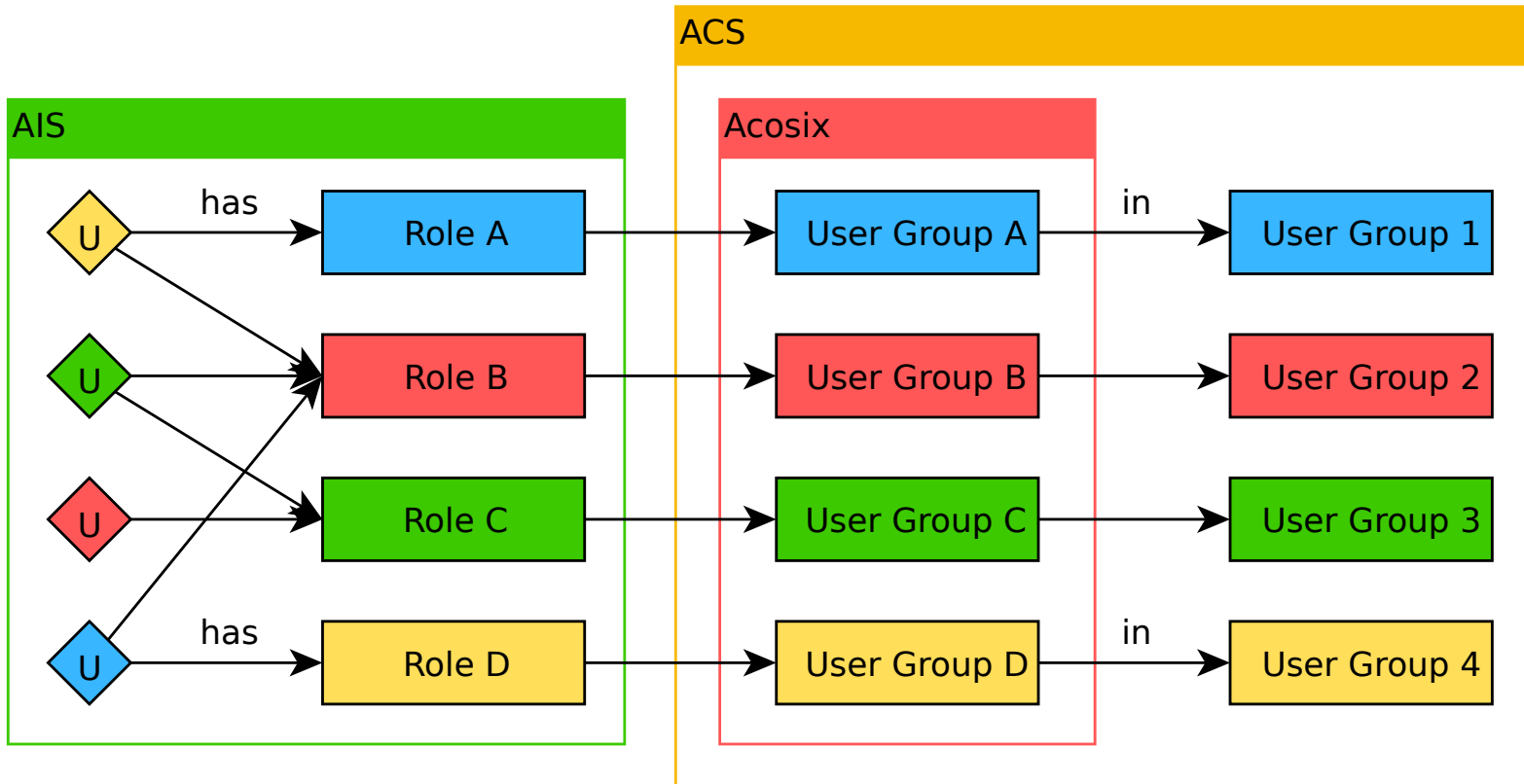
Alfresco Process Services
w/ Inteligr8 Keycloak Extension

Inteligr8 Keycloak Activiti App Extension

- Brian Long
- Project: https://bitbucket.org/inteligr8/keycloak-activiti-app-ext
- Organization: https://inteligr8.com
- The Extension
  - Adds support for create missing users
  - Adds support for role recognition

Inteligr8 Keycloak & Roles for APS

- Role Recognition Support
  - Immediate: On Authentication
  - Routine: On Token Refresh
- LDAP Not Needed/Used
- Shorter Authorization Security Hole (from lag)

Inteligr8 Keycloak & Roles for APS

- AIS Roles map to APS Organizations
  - Configurable to map some to APS Capabilities
  - APS Organizations are hierarchical for inheritance
    - Parent for application uses (like Activity candidate groups)
    - Child for AIS synchronization
  - Sync'd APS Organizations are created on-demand
- Identity/authorization administration for APS admins:
  - Add/remove sync'd APS Organizations as subgroups to system or business APS Organizations/Capabilities

AIS & APS Role Mappings
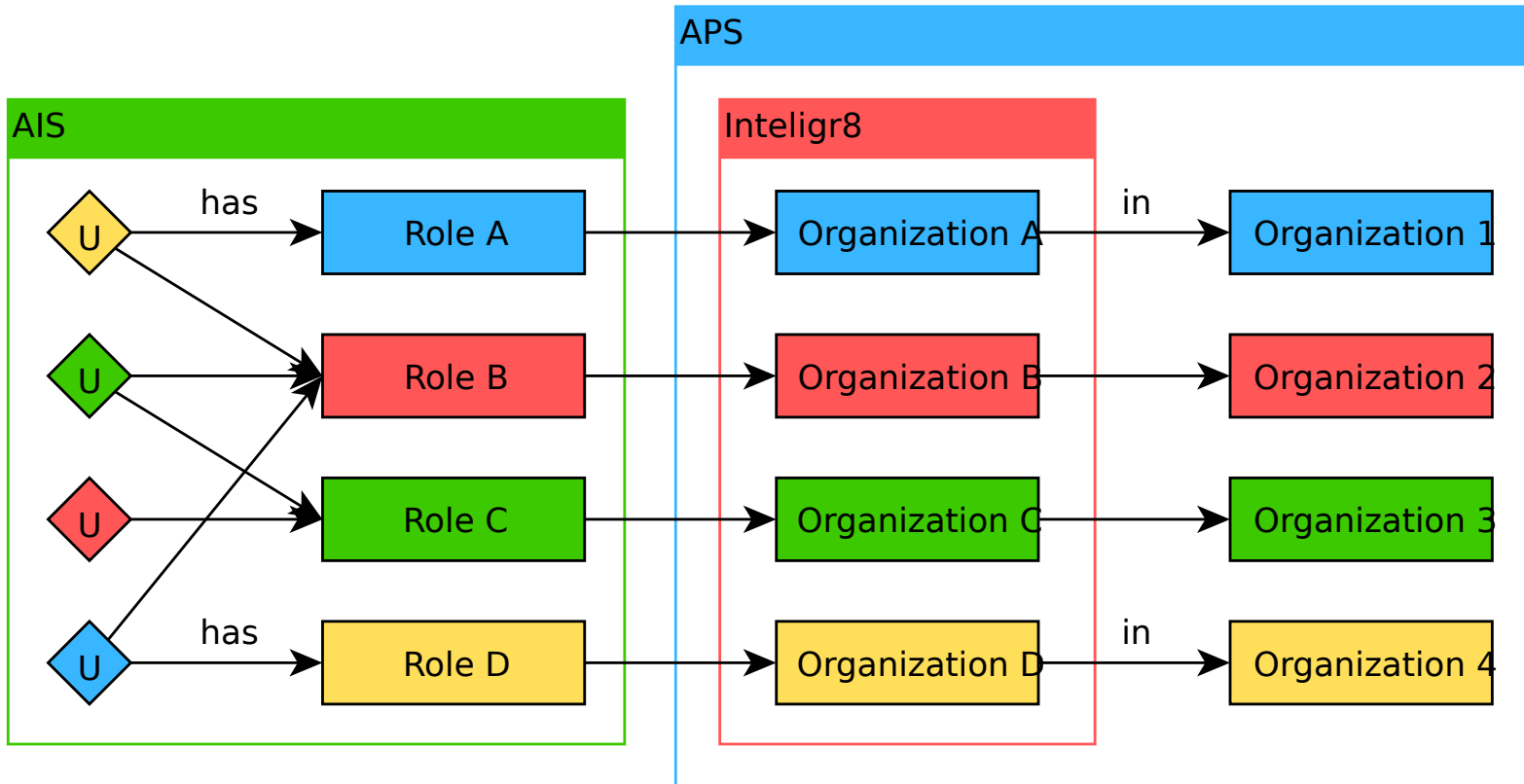
Alfresco Digital Business Platform w/ Acosix & Inteligr8

Inteligr8

Alfresco Digital Business Platform

- Users & Roles & User/Role Mappings
  - Managed by
    - AIS admins
    - Brokered Identity Provider teams
- Roles are determined by the business requirements
- Never managed by ACS or APS admin

Alfresco Digital Business Platform

- Role/ACS User Group Mappings
  - Managed by ACS admins
- Role/APS Organization Mappings
  - Managed as APS admins
- Role/AIS Role Mappings (optional)
  - Managed by AIS admins
  - Only needed if the text should be translated
    - Like IdP role 'content-administrator' to AIS role 'acs-admin'
  - Avoid as it is just additional maintenance
- Supports both AIS Realm & Client Roles

Demonstration

Resources

- ACS Keycloak Module:
  https://github.com/Acosix/alfresco-keycloak
- APS Keycloak Extension:
  https://bitbucket.org/inteligr8/keycloak-activiti-app-ext