SYSTEMATIC

Interface Specification
FBS-14789

External authorization in Cicero

Table of Contents

1 Introduction 3
1.1 References 3

2 Authentication 3

3 Authorization 3
3.1 Configuration of roles 3
3.2 Configuration of branch access 4

Interface Specification

Project: FBS-14789
Revision: $Revision: 1.5$ $Date: 13 Feb 2023$
Document: $SSE/14789/IFS/0027

1 Introduction

This document describes the integrations of external authentication and authorization providers for Cicero LMS. The document covers where and when the integration is used.

The target group for this document is system administrators of Cicero LMS.

1.1 References

Reference	Link
[Cicero LMS system administration]	https://ciceroconnect.zendesk.com/hc/da/articles/360010183817

2 Authentication

Authentication against LMS is possible by external providers that provide access through either SAML or OAuth.

External authentication is made against existing users in LMS, and the username provided by the external authenticator must match the username of a registered user in Cicero LMS exactly. Note that usernames are case sensitive.

See [Cicero LMS system administration] for information about how to create users in Cicero.

3 Authorization

Authorization is based on meta-data returned by the external authorization server. For SAML-based providers, the data resides in SAML attributes. For OAuth-based providers, the data resides in Claims within a JWT token.

Authorization is based on two data types: roles (determining the user's access to functionality in Cicero) and branch ISIL codes (determining the user's access to patron data).

3.1 Configuration of roles

Roles are defined in Cicero LMS, defining the user's access to functionality in Cicero. Roles must be configured in Cicero LMS before they can be resolved through external authorization.

See [Cicero LMS system administration] for information about how to create roles in Cicero.

When an external authorization mechanism is used, it must provide a list of roles in meta-data, and these role names need to match the roles that are configured in LMS. Note that role names are case-sensitive.

The external configuration of roles on users is added to the configuration made in Cicero. That is, if a user has roles "R1" and "R2" assigned in Cicero, and a role "R3" is externally provided, the user effectively has the roles "R1", "R2" and "R3".

3.2 Configuration of branch access

BranchISIL numbers are defined on branches in Cicero, and it is possible to define which branches a user can access. If a user does not have access to a particular branch, that user cannot look up data for patrons with pickup branch on that branch.

See [Cicero LMS system administration] for information about how to set branch access in Cicero.

An external authorization mechanism can provide a list of BranchISIL numbers in meta data. These must be provided as a singular value (in the example of SAML, as a single SAML attribute) with commas separating each ISIL code.

The external configuration of branch access is added to the configuration made in Cicero. That is, if a user has been granted access to patron data on branches "DK-761500" and "DK-761501" in Cicero, and access to the branch "DK-761502" is provided externally, the user effectively has access to patron data on the branches "DK-761500", "DK-761501" and "DK-761502".

SYSTEMATIC

Denmark - HQ
Aarhus
Copenhagen

Australia
Canberra
Brisbane

Canada
Ottawa

Finland
Tampere

Germany
Cologne

New Zealand
Wellington

Romania
Bucharest

Sweden
Stockholm

United Arab Emirates
Abu Dhabi

United Kingdom
Farnborough

United States of America
Centreville

To find more specific office details please scan the QR code below