



Muse Identity Manager

May 2, 2023

Document Version 1.4
Muse Identity Manager
2.3.0.3



Notice

No part of this publication may be reproduced stored in a retrieval system, or transmitted, in any form or by any means, without the prior written permission of MuseGlobal Inc.

Disclaimer

MUSEGLOBAL, INC. MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE CONTENTS HEREOF AND SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OR MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE.

Trademarks

MUSE IS A REGISTERED TRADEMARK OF MUSEGLOBAL, INC. OTHER PRODUCT NAMES AND SERVICE NAMES ARE THE TRADEMARKS OR REGISTERED TRADEMARKS OF THEIR RESPECTIVE OWNERS AND ARE USED FOR IDENTIFICATION ONLY.

museknowledge.com







Table of Contents

1.0 Overview	5
2.0 Features	7
2.1 General Features	9
2.2 Supported Authentication Protocols	10
2.3 End-User Related Features	10
2.4 Administration Console	11
2.5 Password Management	12
2.6 Security	12
2.7 Web Interface	12
2.8 Payment Registration Workflow	13





1.0

Overview

Muse Identity Manager (Muse IDM) is a web application with processes for identifying, authenticating and authorizing individuals or groups of people to access configured applications by associating user rights and restrictions with established identities.

Muse IDM offers support for user registration using preconfigured workflows (with email validation, with or without administrator approval, etc.) and an administration interface for centralized users management with many features like user searching and filtering, bulk updates, sending emails, export as CSV, import from CSV file, login history and user statistics.





2.0

Features

Muse Identity Manager offers features for provisioning identities, role-based access management and enables you to manage access to configured applications and resources securely.

Some screenshots are presented below:

End-user pages

MuseKnowledge™ Users Identity Manager

Please enter your email address and password in the form below to authenticate to the MuseKnowledge™ Users Identity Manager. You can register for an account if you do not have one already, reset the password if you do not remember it anymore, or access your account information.

Email

Password

Remember me

Login

[Register New Account](#) | [Reset Lost Password](#) | [Manage Account](#)

Figure 1. Login Page



Register New Account

Fill in this form to register with this site. The first step is to verify your email address. Enter your institutional email address where to receive the validation link needed for completing the registration.

Full name*


Email*

Confirm email*

Password*

Use 8 or more characters with a mix of letters, numbers and symbols.

Confirm password*

I'm not a robot 

Register

Figure 2. Registration Page

Administrator Pages

MuseKnowledge™ Users Identity Manager Home Users Statistics OAuth2 Users Theme English idm

User Accounts

Showing the list of users registered in this organization. Here you can filter, add, edit, delete, approve, reject registered users.

Search

Search Term:

Per Page: Sort Direction: Sort By:

Bulk Actions

Showing 1 to 3 of 3 entries

<input type="checkbox"/>	Email	Full Name	Affiliation	Status	Enabled	Locked	Created at	Expire at	Last Login	Attributes	Roles	Action
<input type="checkbox"/>	aurelian.popescu@edulib.ro	Aurelian Popescu	EDULIB S.R.L.	REGISTERED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2021-02-05	2022-02-05	2021-02-05T17:53:07	-	USER	<input type="button" value="edit"/> <input type="button" value="delete"/> <input type="button" value="approve"/> <input type="button" value="reject"/>
<input type="checkbox"/>	aurelian.popescu@museglobal.ro	Aurelian Popescu	MuseGlobal SA	REGISTERED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2021-02-05	2022-02-05	2021-02-05T14:49:01	-	USER ADMIN	<input type="button" value="edit"/> <input type="button" value="delete"/> <input type="button" value="approve"/> <input type="button" value="reject"/>
<input type="checkbox"/>	auras@museglobal.ro	Aurelian Popescu		REGISTERED	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2021-02-05	2022-02-05	2021-02-05T17:54:26	-	USER	<input type="button" value="edit"/> <input type="button" value="delete"/> <input type="button" value="approve"/> <input type="button" value="reject"/>

Accounts: [Export](#) [About to export \(0\) items](#)

Figure 3. User Accounts

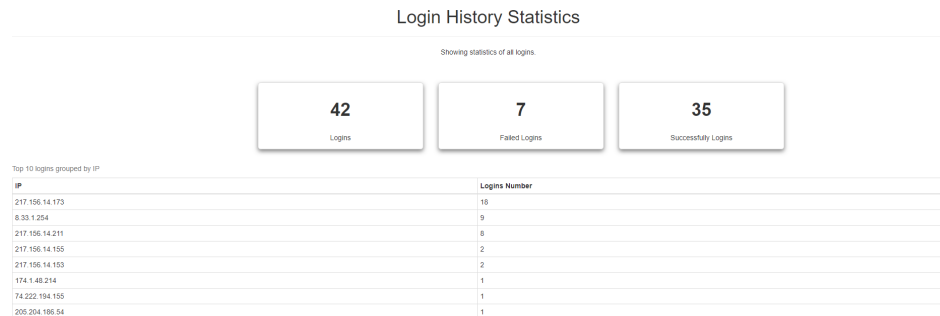


Figure 4. Login History Statistics

Most important features of Muse IDM are detailed in the following sections.

2.1 General Features

The Muse IDM platform is a lightweight application, easy to deploy in any Servlet Container, to integrate with any software needing individual user accounts with self registration and authentication.

General features are presented below:

- Muse IDM allows a high degree of customizations in terms of look and feel, a list with predefined themes from where to choose is available: Amelia (ID `amelia`), Brown (ID `brown`), Dark (ID `dark`), Dark Blue (ID `darkblue`), Gray (ID `gray`), Purple (ID `purple`), White (ID `white`). The theme can be set/changed by passing the theme identifier as value for the `&theme` parameter in the requests.
- Custom fields can be defined for the users registration form. Each custom field defined can have predefined values and validation rules. For example, validation rules can be specified for a Telephone number custom field, to allow phone numbers from a specific country/operator. Mandatory custom fields can be specified.
- Various registration workflows can be configured for user registration: allow direct registration with or without email validation, allow registration only from specific predefined domains, allow registration after email validation and administrator approval.
- Forms protection with Google reCAPTCHA2 security. All application forms like the registration page, login page and password reset page can be protected with Google reCAPTCHA2.



- ✎ Administration console is available for user management, configurations and statistical information. Any user with administrative role can access the administration and configuration items, like users management and statistics.

2.2 Supported Authentication Protocols

- ✎ Muse IDM supports SAML 2.0 as Identity Provider. SAML integrations come with the following features: SAML 2.0 based Single Logout (SLO), metadata profile and SAML attributes filtering.
- ✎ OAuth 2.0 is supported. Muse IDM can be configured as Authorization Server and offers support to manage OAuth2 clients through the Administrator Console. This feature was successfully tested with Muse Proxy, miniOrange(an OAuth2 client for WordPress) and Moodle version 3.7.1.
- ✎ HMAC integration support is available in Muse IDM. Integrations out of the box are available with MuseKnowledge Search and Muse Proxy applications.
- ✎ TOTP (Time-based One Time Password). The user authentication process can be secured with a 2-factor authentication by using TOTP codes generated by mobile applications such as Authy, Google Authenticator and TOTP Authenticator. The TOTP authentication can be enforced, thus all users have to use it, or not, the users can enable it at will.

2.3 End-User Related Features

- ✎ The users can manage their profile details, they can view and edit their own custom attributes values.
- ✎ User roles. The Muse IDM users can have administrator or regular users role. The users with administrative role have access to administrative and configuration features.
- ✎ User status. Users have associated status values to describe their current status: Registered, Pending, Confirmed, Rejected, Expired, Pending Administrator Review, Reset Password, Archived, Await Email Validation, Requires Password Update.
- ✎ Account expiration date is set when a user registers or is added by an administrator. The expiration date is a general property of the system configured in the main configuration file (`application.properties`), for the users added manually by the administrator a custom



expiration date can be set.

- ✎ Account locking for failed login attempts, the user account is locked for a configured period of time if the user tries to authenticate multiple times with invalid credentials.
- ✎ Account locking for invalid captcha attempts, the user is locked for a configured period of time if the reCaptcha security check fails.
- ✎ Account locking when the maximum number of concurrent sessions is exceeded. The maximum number of concurrent sessions per user is a system property configured in the main configuration file (`application.properties`), for the users added manually by the administrator a custom value for the maximum number of concurrent sessions can be set.

2.4 Administration Console

- ✎ A centralized user administration console that embeds features for users management, system configuration and statistical information, is available for the users with administrative role.
- ✎ The users management features include:
 - ✎ Create, View, Edit, Delete users;
 - ✎ Search functionality for users is available, with multiple filtering options. The search is done in all user fields, filtering can be done based on Role, Status values, Expiry details, etc.;
 - ✎ Bulk actions: Edit users, Send Email, Export as CSV, Delete;
 - ✎ Import users from CSV file.
 - ✎ Manage the 2FA Authentication with TOTP.
- ✎ View and add OAuth2 clients;
- ✎ Statistics
 - ✎ Users Login History;
 - ✎ Overall Statistics: Expired Accounts, Accounts About to Expire, Locked Accounts, Disabled Accounts, Number of Administrator Accounts, Number of Users Never Logged in.
 - ✎ Session Statistics;
 - ✎ User Sessions Management: view, filter, search and logout;



- ✎ TOTP Statistics: TOTP Enabled Accounts, TOTP Disabled Accounts or TOTP Pending Accounts.

2.5 Password Management

- ✎ Configurable password policies are available. Supported password complexity requirements include: minimum and maximum length, strength between levels 1 and 5, validation for password to be different than the user email.
- ✎ Passwords expiry. User passwords can be configured to expire after a specific amount of time. At the first login the user is forced to change the password.
- ✎ Password history validation. The user cannot set the same password he used for the last 3 times.
- ✎ Administrator forced password reset. The administrator can force the users to set another password by changing the user' status to `REQUIRES_PASSWORD_UPDATE`.

2.6 Security

- ✎ Authentication and role based authorization take place to ensure proper security. The authentication process can be secured with reCaptcha checks and a 2 Factor Authentication with TOTP.
- ✎ User passwords are stored safely using the most secure hashing algorithms.
- ✎ Server side field validation is performed to increase security.

2.7 Web Interface

The application's web interface is based on the Bootstrap 3 CSS library, thus the user experience is seamless across all devices. The features regarding the interface are presented below.

- ✎ The interface look and feel can be changed by selecting the desired theme from the available ones. The application's default theme is set by the administrator through configuration. Also by con



figuration the **Theme** menu item can be enabled or disabled, thus the user can set the desired theme during his session.

- ✎ Localization (i18n) to be independent from a specific language or limiting character set. An Arabic translation is available, however adding new language translations can be easily made, more details can be found in the **Muse Identity Manager Install** manual, chapter **Internationalization support**.
- ✎ HTML support for email templates is available through the FreeMarker Template Engine. Application properties and user attributes can be accessed dynamically and used in the email templates. The emails templates support internationalization.

2.8 Payment Registration Workflow

- ✎ In the user registration workflow a payment feature can be integrated. Thus a new user creating an account in Muse IDM, after the configured validation steps are fulfilled, on his first login, he is redirected to the configured Payment Platform page to pay the configured subscription plan. All subscription plans are managed on the Payment Platform, Muse IDM is not storing any payment related items.

This feature was successfully tested with [Stripe](#), [Paystack](#) and [Verifone](#) Payment Platforms.

